Sisekaitseakadeemia

Politsei- ja Piirivalvekolledž

Kerly Palm

DIGITAALSED TÕENDID JA NENDE TALLETAMINE PÕHJA PREFEKTUURI NÄITEL

Lõputöö

Juhendaja:

Janar Kummits

Kaasjuhendaja:

Uno Traat

Tallinn 2013

ANNOTATSIOON

SISEKAITSEAKADEEMIA

Kolledž: Politsei- ja Piirivalvekolledž Kuu ja aasta: Mai 2013
Töö pealkiri eesti keeles: „Digitaalsed tõendid ja nende talletamine Põhja Prefektuuri näitel“
Töö pealkiri võõrkeeles: „Digital evidence and their storing by example of Northern Prefecture“
Töö autor: Kerly Palm Olen nõus oma lõputöö kättesaadavaks tegemisega elektroonilises keskkonnas. Allkiri:
Lühikokkuvõte: Lõputöö maht on 42 lehekülge, millele on lisatud kolm lisa kogumahuga 6 lehekülge. Töö kirjutamisel on kasutatud 17 allikat. Töö on kirjutatud eesti keeles. Käesoleva lõputöö eesmärgiks on Põhja Prefektuuri politseiametnike sündmuskohal talletamisega seonduvate probleemide olemasolu ja nendega seonduvate asjaolude väljaselgitamine. Lõputöö eesmärgi saavutamiseks on püstitatud järgmised uurimisküsimused: 1) kes on sündmuskohal peamised digitaalsete tõendite talletajad? 2) kas sündmuskohal digitaalseid tõendeid talletavad ametnikud on piisavalt pädevad või mitte? 3) kas talletamise osas esineb puudusi/probleeme? kui siis milliseid? 4) milliseid muudatusi oleks vaja sisse viia, et digitaalseid tõendeid paremini talletada? Lähtudes püstitatud uurimisküsimustest, valiti uurimismeetodiks kvalitatiivse uurimusena intervjuude läbiviimine. Intervjuud viidi läbi 9 Põhja Prefektuuri kriminalistide, 10 Põhja Ringkonna prokuröride ja prokuröride abide ning 3 Põhja Prefektuuri uurijate hulgas. Uurimuse tulemusena selgus, et peamiste digitõendite talletajatena sündmuskohal on politseiametnikud – menetlejad, uurijad. Talletamisel esinevate puuduste kohta selgus, et mingil määral esineb mõningaid puudusi. Seda kas siis sündmuskohal talletades või juba talletatud tõenditega. Muudatuste läbiviimise kohta selgus, et digitaalsete tõendite kohta on siiani suhteliselt vähe koolitusi läbi viidud ning neid ei ole ka palju tulemas. Lisaks tuleb antud töös välja ka see, et digitõendite olemus on keeruline, nad on haprad, hävinevad kergelt ning neid on suhteliselt raske tõendamiskõlbulikena talletada. Uurimuse tulemusest lähtuvalt tehti 3 ettepanekut, millised aitaksid digitaalseid tõendeid korrektsemalt talletada.
Võtmesõnad: tõend, digitaalne tõend, IT-kuritegevus, talletamine, säilitamine
Keywords: evidence, digital evidence, IT-crime, storing, preserving
Säilitamise koht: SKA PPK raamatukogu
Kaitsmisele lubatud: Kolledži direktor: Allkiri:
Vastab lõputöö nõuetele: Juhendaja: Janar Kummits Allkiri:

SISUKORD

SISSEJUHATUS

Erinevaid tõendite liike on palju ning neid võib liigitada mitmetesse erinevatesse kategooriatesse. Tõendi üheks liigituseks on isikuline ning esemeline liigitus. Sellise liigituse puhul on üheks esemelise tõendite liigiks sealhulgas ka digitaalsed tõendid. Autori arvates võiks digitaalset tõendit oma sisu poolest vaadelda kui eraldiseisvat tõendi liiki. Olenemata sellest, et andmekandja puhul on küll tegemist esemelise tõendiga, ei ole andmekandja iseenesest tõend vaid pigem tõendi allikas, kust on võimalik tõendusmaterjali otsida. Näiteks kõvaketta näol ei ole tegemist otseselt tõendiga, vaid tõendiks on sellelt kõvakettalt leitavad menetluse jaoks olulised dokumendid ja failid.

Digitaalsete tõendite kogumine ja talletamine on keeruline ja nimetatud protseduuride puhul suur oht eksida. Nimetatud tõendeid on vaja koguda ja talletada kindlaid protseduurilisi nõudeid järgides ning selle jaoks on vaja omada ka eriteadmisi.

Igapäevane elu on väga kiire ning pidevas arengus. Koos elu tavalise kulgemisega areneb ka tehnika ja suureneb tehniliste vahendite kasutamine ning inimeste teadlikkus erinevate digitaalsete infokandjate kasutusvõimalustest. Lisaks ulatuslikele interneti kasutamise võimalustele, sh ka mobiilsele kasutamisele, on iga päevaga suurenemas ka sellega seonduvate erinevate digitaalsete infokandjate kasutamine, mistõttu on antud teema kuritegude avastamise ja tõendite kogumise ning talletamise seisukohast aktuaalne.

Tõendid, mis enne digitaliseerumise pealekasvu olid käega katsutavad ja nähtavad, on nüüd kolinud pigem internetti, arvutitesse, erinevatele mälukaartidele jms. Selliseid tõendeid on iga päevaga järjest rohkem. Mõningad sellised tõendid on kergelt avastatavad ning talletatavad kuid mõningad jällegi vastupidi – selle tingib nii tehnika areng kui ka inimeste endi teadmised arenenud tehnika kasutamisest.

Antud lõputöös on uurimisprobleemina käsitletav asjaolu see, et üha suurema digitaliseerumise tõttu ei pruugi politseiamentikud omada piisavalt laialdasi eriteadmisi taoliste tõendite kogumise ja talletamise osas.

Digitaalseid tõendeid on varem Eestis lõputööde raames uuritud. Põhiliselt on neid uuritud selle eesmärgiga, et kuidas neid talletada kui nad on juba sündmuskohalt kaasa võetud. Seda

aga, kas digitaalsete tõendite andmekandjaid sündmuskohal talletavad politseiametnikud ka omavad selleks piisavalt eriteadmisi ja on selles pädevad, ei ole käesoleva lõputöö autori teada täpsemalt uuritud.

Lõputöö eesmärgiks on Põhja Prefektuuri politseiametnike sündmuskohal talletamisega seonduvate probleemide olemasolu ja nendega seonduvate asjaolude väljaselgitamine.

Sündmuskohal esmaseid toiminguid teostavad politseiametnikud on saanud erialase õppe raames digitõendite talletamise osas alusteadmised kuid on tõusetunud küsimus, kas neid teadmisi on ka vastavalt toimuvate tehniliste arengutega paralleelselt piisavalt täiendatud. Antud õpiprotsess on nö elukestev ning ei piirdu mitte ainult vanempolitseiametniku kvalifikatsiooni omandamisel saadud teadmistega, vaid need süvenevad nii töökogemuste, erialaste koolituste kui ka erialase kõrghariduse omandamise käigus.

Lõputöö koosneb kahest peatükist: teoreetilisest ja empiirilisest osast

Teoreetiline osa annab ülevaate sellest, mida täpsemalt mõistetakse erinevate tõendite all. Täpsemalt on antud peatükis kirjas digitaalsete tõendite kohta. Samuti ka kuidas talletada digitaalsete tõendite andmekandjaid nii, et nendest oleks uurimisel kasu. Antud peatükis on kajastatud ka see, kuidas digitaalsete tõendite säilimist tagada ning millised on üldised nõuded, mida peaks järgima selleks, et digitaalsed tõendid säiliksid ning täidaksid uurimisel alati oma eesmärki.

Lõputöö empiirilises osa kirjeldatakse uurimistöö eesmärki, püstitatud ülesandeid, uurimistöö valimit ja protseduuri ning antakse ülevaade saadud tulemustest.

Lõputöö eesmärgi saavutamiseks on püstitatud järgmised uurimisküsimused:

- Kes on sündmuskohal peamised digitaalsete tõendite talletajad?
- Kas sündmuskohal digitaalseid tõendeid talletavad ametnikud on piisavalt pädevad või mitte?
- Kas talletamise osas esineb puudusi/probleeme? Kui, siis milliseid?
- Milliseid muudatusi oleks vaja sisse viia, et digitaalseid tõendeid paremini talletada?

Uurimisküsimustest lähtuvalt püstitati alljärgnevad uurimisülesanded:

- Teada saada, kes peamiselt talletavad sündmuskohal digitaalseid tõendeid ja kas need ametnikud on piisavalt pädevad.
- Teada saada, millised on kõige õigemad viisid digitaalsete tõendite talletamiseks.

- Teada saada komplikatsioonidest, mis on tekkinud digitaalsete tõendite talletamisel ning kelle poolt need tekkinud on.
- Teada saada võimalikke lahendusi kui digitaalseid tõendeid ei osata korrektselt talletada ja mis selle põhjuseks on.

Lähtudes püstitatud uurimiseesmärgist ja sellele tuginevatest uurimisküsimustest, teostati käesoleva lõputöö puhul kvalitatiivse uurimismeetodina intervjuude läbiviimine. Kuna lõputöö eesmärgiks oli selgitada digitaalsete tõendite talletamisega seonduvaid probleeme Põhja prefektuuri politseiametnike näitel, siis moodustati intervjuude valim nende tööga kokku puutuvate ja ülevaadet omavate Põhja Prefektuuri kriminalistide (9 isikut) ja kriminaalasjade üle järelevalvet teostavate Põhja Ringkonnaprokuratuuri prokuröride ning prokuröri abide (10 isikut) ning Põhja Prefektuuri kriminaalbüroo igapäevaselt digitõenditega kokkupuutuvate uurijate (3 isikut) hulgast.

Uurimuse eesmärgiks oli teada saada, kas Põhja Prefektuuri politseiametnikud, kes puutuvad kokku digitaalsete tõendite talletamisega, on valimi moodustanud isikute seisukohalt piisavalt pädevad. Samuti ka see, et kas neid digitaalseid tõendeid talletavate politseiametnike teadmised ja arusaamad lähevad ajaga kaasa, sest tehnika on ju pidevas arengus. Lisaks veel nende tõendite talletamisel tekkinud komplikatsioonidest – kas on midagi valesti läinud või on kõik alati saadud tõendamiskõlbulikena talletada.

Lõputöö empiirilises osas antakse ülevaade uurimustöö tulemustest ja saadud vastuste põhjal tehakse olulisi järeldusi. Samuti tehakse mitmeid ettepanekuid digitaalsete tõendite talletamisega tõusetunud probleemide võimalikuks lahendamiseks.

1. ERINEVAD TÕENDID

Vastavalt Kriminaalmenetluse seadustiku § 63'le on tõend:

(1) Tõend on kahtlustatava, süüdistatava, kannatanu ja tunnistaja ütlus, eksperdiarvamus, eksperdi antud ütlus ekspertiisiakti selgitamisel, asitõend, uurimistoimingu, kohtuistungi ja jälitustoimingu protokoll või muu dokument ning foto või film või muu teabesalvestis.

(2) Kriminaalmenetluse asjaolude tõendamiseks võib kasutada ka käesoleva paragrahvi lõikes 1 loetlemata tõendeid. [1]

Tõendite hulka kuulub kõik sündmuskohal leitu olgu see siis kas kahtlustatava või hoopiski tunnistaja poolt jäetud. Kuna sündmuskohal kogutud tõendid pannakse kokku ning neid kirjeldatakse ka protokollides, siis lähevad tõendite alla ka ütlused, eksperdiarvamused ning muud dokumendid, mis on sündmuskohaga seotud ning vastavalt sündmuskohale koostatud.

Seega võib öelda, et tõendid on kõige vajalikumad tõendamaks kahtlustatava süüd ja osalust või siis mitteosalust antud kuriteos.

Lähtudes tõendi allikast võib tõendid liigitada:
Isikulised (ütlused) ja esemelised (asitõendid, dokumendid, protokollid, foto, film või muu teabesalvestus) tõendid.[2]

1.1. Tõend ja infotehnoloogiline tõend

Tänapäeva ühiskonnas kasutavad inimesed mitmes eluaspektis hüvedena erinevaid elektroonilisi seadmeid – sealhulgas meediaallikaid ja arvuteid. Kurjategijad aga peremehetsevad elektroonilises meedias ja arvutite kaasamises oma illegaalse tegevusega. Moodne ja praegune tehnoloogia laseb kahtlusalustel panna kuritegusid toime rahvusvaheliselt ja kaugelt, saades kätte intellekti ja nii läbi viia läbi intellekti võltsimisi

[1] Kriminaalmenetluse seadustik, Vastu võetud 12.02.2003, RT I 2003, 27, 166, jõustumine 01.07.2004, https://www.riigiteataja.ee/akt/123022011045 – välja otsitud 1. aprill 2011

[2] E. Kergandberg, T. Järvet, T. Ploom, O. Jaggo; *Kriminaalmenetlus, Teine, muudetud trükk;* Sisekaitseakadeemia, 2004, lk 22

ligikaudse anonüümsusega. Kohene kommunikatsioon ja elektrooniline mail võimaldab olla kohtumõistjaks kahtlusaluse ja ohvrite vahel.[3]

Kuna infotehnoloogial (edaspidi IT) on ühiskonnas üha suurenev roll, siis tuleb ka politseiametnikel üha rohkem nendega menetlusalaselt kokku puutuda. Erialakirjanduses on leitud, et termin ”infotehnoloogia” jääb antud kontekstis liiga kitsaks, kuna nt mobiiltelefonid kuuluvad rohkem kommunikatsioonitehnoloogia valdkonda. Sellest tulenevalt on kasutusele võetud termin “info(rmatsiooni)- ja kommunikatsioonitehnoloogia (või sidetehnoloogia)” (ingl.k. ”*Information and Communication Technology*”). Viimasel ajal on eriti anglo-ameerika maades üha rohkem kasutust leidnud termin ”kõrgtehnoloogia” (“*High Tech*”). Käesolevas väljaandes on siiski jäädud suupärasema termini ”infotehnoloogia” juurde ning selle all peetakse silmas ka kommunikatsioonitehnoloogia rakendusi.[4]

Tõendeid (nn digitaalsed tõendid) võib tänapäeval leida väga erinevatest seadmetest, mis kasutavad IT-d, näiteks majapidamisseadmed (tolmuimejad, pesumasinad, külmkapid, signalisatsiooni-, valgustus-, küttesüsteemid jne), uuemad sõidukid (sisseehitatud multimeediakeskused, navigatsioonisüsteemid), kontoritehnikast rääkimata. Tulevikus lisandub suure tõenäosusega IT rakendusvõimalusi veelgi. Võimalike juhtumite ring, kus politseiametnikul digitaalsete tõenditega kokku puutuda tuleb, on väga lai – tapmiskohalt või kahtlustatava juurest leitud pihuarvuti, mobiiltelefon või mälupulk, e-kirja teel toimepandud väljapressimine või pommiähvardus, pedofiilide tegevus suhtlus- ja tutvumisportaalis (nt www.rate.ee) või jututoas, lõpetades riigi infrastruktuuride (riigiasutused, pangad, energia- ja sideettevõtted jne) vastu suunatud keerukate rünnetega. On paratamatu, et infotehnoloogial on väga tähtis roll ühiskonnas, mida meil kaitsta tuleb.[4]

IT ning kuritegevus

IT sektori kiire areng ning järjest laialdasem IT vahendite kasutusele võtmine inimeste poolt on toonud kaasa olukorra, kus aina enam kuritegusid, sh mitte ainult klassikalised küberkuriteod, pannakse toime IT vahendite abil ning kus aina rohkemate kuritegude puhul on vajalik kuriteo tõendamiseks leida ja fikseerida tõendid arvuti kõvakettalt või mõnelt muult IT

[3] United States Secret Service, *Best practices for seizing electronic evidence v.3 A pocket guide for first responders*, lk 3

[4] Keskkriminaalpolitsei, *Infotehnoloogiakuritegude menetlemise käsiraamat*, 2011, Phare mestiprojekt EE 03 IB JH 04, uuendatud JLS/2009/ISEC/AG/077, lk 7

andmekandjalt, mis omakorda on toonud kaasa antud valdkonnas töötavate ametnike olulise koormuse kasvu.[5]

Kriminaalstatistika näitab selgelt nii arvutite abil kui arvutisüsteemide vastu toime pandud kuritegude arvu pidevat ja kiiret tõusu (KarS § 206,207,208,213,216-1,217; 2007 a. - 154 tk; 2008 a. - 401 tk; 2009 a. - 500 tk; 2010 a. - 426 tk; 2011 a. - 569 tk). Üksnes arvutikelmuste arv kasvas 2011 aastal võrreldes eelmise aastaga ca 26%.[5]

Tehniline ressurss on kõigis prefektuurides vananenud ja piiratud. Paljuski kasutatakse tehnikat, mis osteti 2005. aastal, kui loodi ja koolitati IT-grupid. Prefektuuride IT gruppidel on tõsiseid probleeme andmete säilitamise ruumiga, mida ei ole ühetaoliselt lahendatud, vaid iga üksus teeb seda oma parimal võimalikul moel. Alates 2005 aastast ei ole toimunud komplektset ja süstemaatilist IT gruppidele nende igapäevaseks tegevuseks vajaliku tark- ja riistvara uuendamist. Tööks vajalike vahendite kaasajastamine on toimunud kaootiliselt ja põhimõttel, et kui enam kuidagi tööd teha ei saa siis alles hangitakse uus töövahend.[5]

IT-ga seostatava kuritegevuse võib kategooriatesse jagada järgmiselt:

- **IT kui kuriteo objekt, sihtmärk.** Näiteks võib siin tuua arvutiviiruse levitamise, millega rünnatakse arvuti ning arvutiprogrammide funktsionaalsust, ning ründed teenuste vastu *(denial of service attacks)*, mille eesmärgiks on rünnatava arvuti või programmi kokku jooksmine/hangumine *(crash)* ja/või võrguühenduse häirimine või blokeerimine. KarS-i mõistes läheksid selle alla tüüpiliste arvutikuritegudena §§ 206-208, 213, 217.
- **IT kui kuriteo toimepanemise vahend.** Näiteks arvuti ja printeri kasutamine dokumentide võltsimiseks või väljapressimisnõuete saatmine e-posti teel, samuti lapsporno levitamine interneti teel. KarS-is IT kui kuriteo toimepanemise vahendi osas erisätteid ei ole, seega kuuluvad kvalifitseerimisele üldsätete järgi (nt § 214 „Väljapressimine" või § 178 „Lapsporno valmistamine või selle võimaldamine")
- **IT kui kurjategijate sidepidamis- ning suhtluskeskkond.** Näiteks MSN-i kasutamine teabevahetuseks kuritegelike ühenduste vahel või pedofiilide grupi liikmete omavaheline suhtlemine interneti jututoas. Üldjuhul ei ole KarS-i järgi eraldi karistatav tegevus (v.a. §189. Narkootilise ja psühhotroopse aine levitamise ettevalmistamine).

[5] IT-kuritegevus, http://ppa-siseveeb.polsise/kriminaalpolitsei/it-kuritegevus/index.dot – välja otsitud 26. Märts 2013

- **IT kui tõendi allikas.** Kõigi ülaltoodud tegevuste kohta võib kasutajaarvutitest ja võrguseadmetest leida informatsiooni, mis võib olla teadlikult talletatud või on salvestunud automaatselt, st tahtmatult. Näiteks:
    - ✓ kannatanu või kurjategija arvutis või meiliserveris salvestatud e-kiri;
    - ✓ ajutine dokument, mida selle koostaja ei salvestanud, kuid mis automaatselt talletati programmi poolt;
    - ✓ kolmandate isikute, nt internetiteenusepakkujate (Internet Service Provider – edaspidi ISP) valduses olevad salvestised (logid) kahtlustatava tegevuse kohta;
    - ✓ logikirjed kohtvõrgu kasutaja kontole sisse- ja väljalogimise kuupäevade ja kellaaegade kohta.[6]

IT kasutamine kurjategijate poolt ühest küljest hõlbustab kuritegude toimepanemist, teisalt aga jäävad enamasti maha jäljed. Politsei ülesanne on need jäljed üles leida ja neid kasutada kuritegude avastamisel ja tõendamisel.[6]

Infotehnoloogia kuriteod

Terminoloogia on antud valdkonnas põhjustanud kõige enam vaidlusi ja lahkarvamusi. Inglise keeles on enim kasutamist leidnud termin „Cybercrime", mõnevõrra vähem ehk „High-Tech Crime" ja „Information and Communication Technology Crime", mis kõik tähendavad sisuliselt üht ja sama asja. Käesoleva väljaande koostajad on otsustanud jääda termini „infotehnoloogiakuriteod" juurde, kuna termin on erialakeeles olnud pidevalt kasutusel ning kinnistunud. Samuti on „IT kuriteod" käibel ajakirjanduses ning see on teatud määral juurdunud ka kõnekeeles. Termini "infotehnoloogiakuriteod", lühendina „IT kuriteod", all võib mõista aga igasugust kuritegevust, mis on seotud arvutite ja arvutivõrkudega ning laiemalt igasuguste IT seadmete ja süsteemidega, mis kasutavad digitaalset arvutustehnoloogiat või digitaalsidet. IT kuriteod hõlmab nii ründed IT seadmete ja süsteemide vastu kui ka nende seadmete kasutamise kuriteo toimepanemise vahendina. [6]
Küberkuritegevuses peamise osa rünnetest nii infosüsteemide kui ka infosüsteemis paiknevate andmete vastu moodustavad varalise kasu saamise eesmärgil toime pandud kuriteod. Sellised kuriteod avalduvad tavaliselt teenuse pakkumise häirimises või teenuse töö katkestamises,

[6] Keskkriminaalpolitsei, *Infotehnoloogiakuritegude menetlemise käsiraamat*, 2011, Phare mestiprojekt EE 03 IB JH 04, uuendatud JLS/2009/ISEC/AG/077, lk 7-8

andmete konfidentsiaalsuse, terviklikkuse või käideldavuse rikkumises. Küberkuritegevus, sh arvutite- ja arvutisüsteemide vahendusel toime pandud kuriteod, on muutunud organiseerituks, rahvusvaheliseks ja suurt kriminaaltulu tootvateks. Arvutikuritegu on sageli eelkuriteoks ka rasketele majanduskuritegudele (nt rahapesu) või siis pannakse see toime arvutisüsteemide vahendusel.[7]

Eeltoodust tulenevalt on IT kuritegudeks:

- sissemurdmine (nn „häkkimist") võõrasse arvutisse, mis on KarS § 217 alusel kvalifitseeritav kui arvutisüsteemi ebaseaduslik kasutamine;
- e-posti vahendusel raha väljapressimine (KarS § 214) – see on tehniliselt väga lihtsasti teostatav nõudmata kurjategijalt erilist IT alast taipu, samas aga võib olla suhteliselt raskesti avastatav.[8]

IT kuritegude all mõistetakse järgmisi kuritegusid:

- arvuti või arvutisüsteemi ebaseaduslik kasutamine - isiku virtuaalkontot kasutatakse ilma tema nõusolekuta (näiteks on ilma isiku nõusolekuta kasutatud Rate/Orkut/Facebook vms kontot, e-posti kontole sisse logitud jne);
- arvuti kelmused
- arvutiviiruse sh spämmi teadlik levitamine;
- arvuti või arvutisüsteemi töö blokeerimine - erinevad ründed arvutile või arvutisüsteemile, mille tulemusel arvuti või arvutisüsteemi töö blokeeritakse nt ülekoormuse tõttu (nt DDos ründed), aga ka nt ründed kodulehtedele, foorumitele jne;
- identiteedi vargused - isiku identiteedi ebaseaduslik kasutamine ehk nn libakontode tegemine. Identiteedi vargusena on käsitletavad sellised tegevused nagu teise isiku nimel ilma isiku nõusolekuta (virtuaal)konto loomine, teise isiku nimel e-maili konto tegemine või sellelt kirjade väljastamine.[9]

IT kuritegevus ei ole täna enam eraldiseisev kuritegude rühm, mida on nn vertikaalselt defineeritud karistusseadustiku arvuteid ja arvutivõrke käsitlevates paragrahvides. Sarnaselt

[7] IT-kuritegevus, http://ppa-siseveeb.polsise/kriminaalpolitsei/it-kuritegevus/index.dot – välja otsitud 26. Märts 2013
[8] Keskkriminaalpolitsei, *Infotehnoloogiakuritegude menetlemise käsiraamat,* 2011, Phare mestiprojekt EE 03 IB JH 04, uuendatud JLS/2009/ISEC/AG/077, lk 8-9
[9] IT-kuriteod, https://www.politsei.ee/et/nouanded/it-kuriteod/ – välja otsitud 19. aprill 2013

„organiseeritud kuritegevusele", mida mõistetakse nn horisontaalselt, on ka infotehnoloogiakuritegude puhul tihti tegemist nn "traditsiooniliste" kuritegudega, mille toimepanemisel kasutatakse abivahendina IT seadmeid ja rakendusi („*new crime – new tools, old crime – new tools"* e tõlkes „uut tüüpi kuritegevus – uued vahendid, „traditsiooniline" kuritegevus – uued vahendid"). Antud lause on välja toodud Europoli 2002. a. trükises „Arvutitega seonduv kuritegevus EL-is" selgitamaks IT kuritegevuse „horisontaalset" olemust.[10]

1.2. Digitaalne tõend

Digitaalse tõendi või elektroonilise tõendi alla käib kõik tõendusjõudu omav informatsioon, mis on talletatud või edasi antud digitaalses vormis. Seda kasutatakse ka kohtus. Enne kui kohus aktsepteerib digitaalse tõendi, otsustatakse kas see digitaalne tõend on asjakohane, autentne või kuulujutt ning kas koopia on vastuvõetav või on vaja originaali.[11]

Sõna „digitaalne" võiks tähendada eesti keeles „numbriline" või „numbritest koosnev". „Digitaalne tõend" kujutab endast igasugust digitaalses ehk siis numbrilises vormis esinevat informatsiooni, mida on võimalik kasutada kohtus tõendamiseseme asjaolude selgitamisel. Kõige sagedamini kuriteopaigas leiduvad seadmed on lauaarvutid, sülearvutid, paljundusmasinad, digitaalfotoaparaadid ja muud tehnikavahendid, mida me kõik igapäevaselt kasutame.[12]

Digitaalsete tõendite abil saab vastata kuritegevuse peamistele küsimustele. Hõlmates endas seda, mis juhtus mis ajal (ajaline järjestus), kes mõjutas keda (seos), millegi asja päritolu (allika hinnang) ja et kes on selle eest vastutav (omistamine). Samas arvutisüsteemide keerukus vajab süvenemist sest üksikuid digitaalseid tõendeid võib ka mitmeti tõlgendada. Kinnitav informatsioon võib olla eluliselt vajalik õige järelduse tegemiseks. Selleks aga et digitaalseid tõendeid eesmärgipäraselt kasutada, tuleb kohtulikel praktiseerijatel aru saada ja regulaarselt kasutada teaduslikku meetodit. Teaduslik meetod koos kriminalistide meetodite ja

[10] Keskkriminaalpolitsei, *Infotehnoloogiakuritegude menetlemise käsiraamat,* 2011, Phare mestiprojekt EE 03 IB JH 04, uuendatud JLS/2009/ISEC/AG/077, lk 8-9
[11] Casey, E (2004*), Digital Evidence and Computer Crime, Second Edition*, lk 12
[12] Keskkriminaalpolitsei, *Infotehnoloogiakuritegude menetlemise käsiraamat*, 2011, Phare mestiprojekt EE 03 IB JH 04, uuendatud JLS/2009/ISEC/AG/077, lk 8

tehnoloogiaga võimaldabki meil kohaneda erinevate asjaolude ja nõuetega ning kindlustada selle, et saadud tulemused põhinevad faktidel.[13]

Arvutipõhised tõendid, ja digitaalsed tõendid üldse, on oma loomuse poolest väga haprad. Seda võib kahjustada, muuta või hävitada ebaõige käsitsemise või siis ebaõige vaatlusega. Selle tõttu tuleb sellist tüüpi tõendeid erilise ettevaatusega dokumenteerida, talletada, säilitada ja läbi vaadata. Midagi valesti tehes võib muuta selle kasutuskõlbmatuks või siis viia valede tulemusteni.[14]

Digitaalsete tõendite kasutamine on viimastel aastakümnetel tõusnud. Seda seetõttu, et kohtud on lubanud igasuguse digitaalse andmekandja (e-mailid, digifotod, digivideod, ja muud) kasutamist, et vajalikku informatsiooni kätte saada.[15]

Digitaalsete tõendite talletamine menetluses nõuab spetsiaalseid oskusi ja erialast ekspertiisi informatsiooni kogumisel ja talletamisel. Digitaalsete tõendite talletamine elektroonilistelt seadmetelt nõuab ametnikelt ka viimase tehnoloogia ja selle arenguga kursis olemist. Seetõttu peavad ametnikud saama koolitusi ja ise ka läbi tegema. Samas peab ka juhtkond olema toetav ning leidma aja ja raha oma töötajate koolitamiseks.[16]

Digitaalsetel tõenditel on järgmised olulised omadused:

- Enamasti on nad silmale nähtamatud, nagu ka sõrmejäljed ja DNA materjal. Digitõendite "nägemiseks" on vaja spetsiaalset tark- ja riistvara ning koolitatud spetsialisti.
- Nad võivad kergelt kahjustuda või isegi hävida. Seetõttu peavad kõik politseiametnikud, kel digitõenditega pistmist, teadma ja järgima käesolevas käsiraamatus toodud käitumisjuhiseid.
- Enamasti sõltuvad nad ajategurist. Näiteks paljud võrguseadmete logid kirjutatakse üle üsna lühikese aja jooksul. Samuti võivad internetikelmide materjalid kaduda internetist niipea, kui tajutakse politsei huvi.
- Tõendeid Eestis aset leidnud kuritegude kohta võib leida ka väljastpoolt riigipiire.

[13] Casey, E *Handbook of Digital Forensics and Investigation*, Academic Press, välja antud 2. september 2010, lk 21

[14] *ACPO Good Practice Guide for Computer-Based Evidence*, ACPO. välja antud 24 juuli 2010, lk 6

[15] Casey, E *Handbook of Digital Forensics and Investigation*, Academic Press, välja antud 2 September 2010, lk 567

[16] International Competition Network, *Anti-Cartel Enforcement Manual*, välja antud märts 2010, Chapter 3 lk 8

- Tõendiks võib olla nii kasutaja enda poolt arvutisse teadlikult sisestatud kui ka arvuti töö käigus automaatselt tekkinud informatsioon.[17]

Digitaalseid tõendid võib menetluse seisukohalt jagada kaheks:

- **Tõendid andmekandjatel** – näidetena võib siin tuua arvuti kõvaketta, flopi (FDD), digikaameras kasutatava mälukaardi või mobiiltelefoni SIM-kaardi. Valdkond, mis tegeleb andmekandjatel oleva tõendusmaterjali tuvastamise ning fikseerimisega, kannab inglise keeles nimetust „computer forensics“ (eestikeelne vaste arvutikriminalistika, arvutiekspertiis). Andmekandjal oleva informatsiooni tuvastamiseks ja tõendina sobilikult kujul fikseerimiseks on põhimõtteliselt kaks võimalust:
  - ✓ Politseiasutuse vastavas spetsialiseeritud üksuses teostatakse arvuti ja/või andmekandja uuring, mille tingimused, käik ja tulemused talletatakse vaatlusprotokollis ning vajadusel sellele lisatud andmekandjal (failid CD-plaadil, flopil jne);
  - ✓ Arvuti ja/või andmekandja saadetakse menetleja ekspertiisimääruse alusel EKEI infotehnoloogiaekspertiisi. Ekspertiisi käik ja tulemused talletatakse ekspertiisiaktis eksperdiarvamusena.
- **Tõendid arvutivõrkudes**, eriti Internetis toimuva tegevuse kohta – võrguseadmetes salvestatud logide abil on võimalik näiteks tuvastada isikute tegevust arvutivõrkudes, mille lõpptulemusena on võimalik jõuda juba kahtlustatava arvutini, mis seejärel saadetakse ekspertiisi või teostatakse arvuti tehniline uuring politseiasutuse vastavas spetsialiseeritud üksuses.[17]

Digitaalsete tõendite klassifitseerimine

Digitaalseid tõendeid võib klassifitseerida, individualiseerida (objekti kirjeldavate eritunnuste põhjal) ja võrrelda mitmel erineval viisil.

Üks klassifitseerimise viise on näiteks:

Sisuline – uurijad kasutavad e-maili sisu et liigitada ja kindlaks teha, millisest arvutist see pärit on. Lisaks ka vahetatud failid sisaldavad erinevaid kilde digitaalsetest andmetest, mida

[17] Keskkriminaalpolitsei, *Infotehnoloogiakuritegude menetlemise käsiraamat*, 2011, Phare mestiprojekt EE 03 IB JH 04, uuendatud JLS/2009/ISEC/AG/077, lk 8

saab päris tihti ka individualiseerida ja klassifitseerida.

Otstarbeline – selleks, et seda klassifitseerida ja individualiseerida, kontrollivad uurijad, kuidas programmid funktsioneerivad. Nt programm, mis tundub, et teeb midagi kasulikku või siis toimib meelelahutusena, on tavaliselt klassifitseeritud Trooja hobuse programmina.

Iseloomu põhjal – faili nimed, sõnumid ja kuupäevatemplid on abiks antud digitaalsete tõendite grupi klassifitseerimisel ja individualiseerimisel.[18]

Viis omadust, mis digitaalsetel tõenditel peab olema selleks, et nad oleksid kasulikud:

- Lubatav – tõendit peab saama kasutada kohtus. Selle reegliga mittenõustumine on sama hea kui seda tõendit polekski sündmuskohalt kaasa võetud. Kuid sellisel juhul on selle kahju palju suurem.
- Autentne – tõend peab olema seotud juhtumiga selleks, et midagi tõestada. Tõend peab olema seotud sündmuskohaga asjasse puutuvana.
- Täielik – ei ole piisav koguda tõendeid, mis näitavad ainult ühte sündmuse vaatenurka. Koguma ei peaks mitte ainult tõendeid, mis tõestavad ründaja tegusid vaid ka tõendeid, mis tõestavad nende süütust. Näiteks kui saad tõestada et kurjategija oli sisse logitud, pead teadma ka seda, kas keegi teine oli sisse logitud ning kes. Samas pead ka mõtlema, miks just nemad seda ei teinud. Seda nimetatakse süüd välistavaks asjaoluks ja on uurimise üks oluline osa.
- Usaldusväärne – tõendid ja analüüsid ei tohi panna kahtlema tõendite autentsuses ja tõele vastavuses.
- Usutav – tõend, mida esitad, peab olema üheselt arusaadav ja olema usutav ka kohtule. Ei ole ju mõtet esitada kahemõistelisi tõendeid, kuna sellest ei saada aru.[19]

Digitaalne tõend versus tavaline tõend

Digitaalne tõend on esemelise tõendi üks liik. Kuigi digitaalne tõend on vähem kombatav kui teised esemelise tõendi liigid (nt sõrmejäljed, DNA, relvad, arvuti komponendid), on see ikkagi esemeline tõend. Digitaalne tõend luuakse magnetväljade ja elektriimpulsside abil,

[18] Digital Evidence, Harley Kozushko, 2003, lk 3, http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf - välja otsitud 20. Märts 2012

[19] Digital Evidence slideshow 2003, Harley Kozushko, lk 3-4, http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Presentations/DigitalEvidence.pdf?bcsi_scan_123264D0DBEECA8E=0&bcsi_scan_filename=DigitalEvidence.pdf – välja otsitud 12. Aprill 2011

mida kogutakse ja analüüsitakse spetsiaalsete tööriistade ja tehnika abil. Kohtud on otsustanud, et sellist mittemateriaalset omadust võib käsitleda tõendina.[20]

Digitaalsel tõendil on mitmeid eeliseid võrreldes teiste esemeliste tõenditega:

- Sellest saab teha identse koopia ning seda saab uurida kui originaali. See on tavaline digitaalse tõendi uurimisviis selleks, et originaali mitte kahjustada.
- Õigete vahenditega on väga lihtne kindlaks teha, kas digitaalset tõendit on muudetud või rikutud, originaaliga võrreldes.
- On suhteliselt raskesti hävitatav. Isegi siis kui on ära kustutatud, võib digitaalseid tõendeid arvuti kettalt kätte saada.
- Kui kurjategijad üritavad digitaalseid tõendeid hävitada, võivad jääda koopiad sellest kohtadesse, millest kurjategijad ei tea.[20]

1.3. Digitaalsete tõendite leidmine, säilitamine ja talletamine

Politseiametnike tööaeg on sageli kiire ja sündmusterohke. Iga politseiametniku töökohustuste hulka kuulub muuhulgas kodanike abistamine probleemsetes olukordades, asjakohane reageerimine seaduserikkumistele, sageli ka esimese politseiametnikuna mõne raskema kuriteo sündmuskohale jõudmine.[21]

Esimesena sündmuskohale saabunud politseiametnik peab kõigepealt tegelema sealse olukorraga – hoolitsema kannatanu eest, kutsuma välja kiirabi, turvama sündmuskoha, vaatama sündmuskoha üle potentsiaalsete tõendite leidmiseks jne.[21]

Esmane kontakt kuriteosündmusega võib toimuda ka muud moodi, nt laekub jälitusteave uimastivahendaja tegevuse kohta või saabub kannatanu avaldus kelmuse kohta.[21]

Digitaalsete tõendite säilimisel on politseiametnikul eriti oluline roll. Nimelt on politseiametniku ülesanne tagada digitaalsete tõendite olukorra säilimine enne fikseerimist. Samuti peab politseiametnik fikseerima tõendi just sellises olukorras nagu ta antud hetkel on. Kui tõend on fikseeritud, tuleb säilitada see samas olukorras selleks, et andmeid ei läheks kaotsi. Seda just sellepärast, et digitaalsete tõendite info ei ole tavaliselt silmaga nähtav ning

[20] Casey, E, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 2000, lk 4-5
[21] Keskkriminaalpolitsei, Tallinn 2005, *Infotehnoloogiakuritegude menetlemise käsiraamat versioon 1.0*, Phare mestiprojekt EE 03 IB JH 04, lk 12-14

üks vale liigutus võib kõik leiduvad tõendid hävitada. [22]

Kõigi nende juhtumite puhul peab esmane menetleja:

- ära tundma potentsiaalse tõendi (tõendiallika) – näiteks tunnistajad, sõrmejäljed ja DNA;
- turvama tõendi – võttes selle kontrolli alla ja tagades selle puutumatuse;
- tagama tõendi säilimise – tõendusmaterjaliga ümberkäimisel (kogumisel, pakendamisel, transportimisel) võtma tarvitusele abinõud, et tõend ei läheks kaduma ja et tõendi terviklikkus säiliks, st et see ei muutuks ega saaks kahjustada (nt sõrmejälgede ja DNA-ga seotud tõendusmaterjali säilimise kindlustamine).[22]

Sama kehtib ka digitaalsete tõendite kohta. Esmane menetleja peab ära tundma, kus digitaalseid tõendeid võib leida, tagama nende puutumatuse ja säilimise.[22]

Võimalike digitaalsete tõendite äratundmine

Viimaseid aastaid on iseloomustanud üha laienev IT kasutamine ja IT seadmete mitmekesistumine. Tavaliselt on neid seadmeid kerge tuvastada, kuna nad on tavakasutuses ja kõigil on nendega kogemusi. Näiteks võib siin tuua mobiiltelefonid, pihuarvutid ja digitaalkaamerad. Kuid on ka teistsuguseid näiteid – sõidukite elektroonikasüsteemides võib olla andmeid diagnostika eesmärkidel. Kui selline sõiduk on seotud kuriteo toimepanemisega, võivad need andmed olulised olla. Paljude seadmete puhul võib leida andmeid asukoha kohta nende GPS-terminalidest. Samuti võib tähtsat infot sisaldada kontoritehnika, nagu näiteks faksimasin (viimati valitud numbrid jpm).[22]

Võimalike tõendite äratundmise puhul on oluline hinnata nende asjakohasust. Kuriteopaigas tuleb politseiametnikul otsustada, mis tüüpi digitaalsed tõendid antud olukorras tähtsust omavad ning sellele vastavalt ka seadmed turvata.[22]
Allikad, kus võib digitaalseid tõendeid olla:

- Seade ja selle komponendid
- Funktsioonid, millega seade töötab ja mis hõlbustavad töötamist
- Tarkvara, dokumendid, fotod, pildifailid, e-mailid ja lisad, andmebaasid, interneti kasutamise ajalugu, vestluslogid, sõprade/tuttavate loendid ja sündmuste logid

[22] Keskkriminaalpolitsei, Tallinn 2005, *Infotehnoloogiakuritegude menetlemise käsiraamat versioon 1.0*, Phare mestiprojekt EE 03 IB JH 04, lk 12-14

- Seadmel olev informatsioon mis puudutab selle seadme kasutamist, näiteks: sisse tulnud ja väljuvad kõned ja faksi numbrid
- Identifitseerimis informatsioon, mis on seotud arvutisüsteemiga, näiteks: IP-aadress [23]

Neid allikaid võib olla igasuguseid erinevaid: näiteks faksi-masinad, scannerid, printerid, veebikaamerad, mp3-ed, telefonid, arvutid, mälukaardid ja palju-palju muud.

Tõendite säilimise tagamine

Tõendi säilimine on tagatud, kui see on politsei kontrolli all ja seda ei saa kõrvaldada, muuta ega kahjustada. Paljudel juhtudel algab tõendi turvamine inimeste eemalhoidmisega seadmest. See põhimõte kehtib kõigi (asi)tõendite puhul.[24]

Kõige esimene digitaalsete tõenditega seotud nõue on tagada, et mitte keegi – eriti käib see kahtlustatavate kohta – ei puudutaks võimalikke tõendeid sisaldavat seadet ega selliste seadmete ühendusi (toide!).[24]

Osa digitaalsetest tõenditest võib leiduda kahtlustataval taskus, nagu näiteks mobiiltelefon ja pihuarvuti. Need tuleks kohe sisenemisel ära võtta. Politseinikud peaksid eriti ettevaatlikud olema pihuarvutitega, kuna nendes sisalduvat teavet saab aku eemaldamisega hetkega hävitada. Kindlasti teavad seda ka paljud kurjategijad.[24]

Võib juhtuda, et koostöövalmiduse sildi all pakuvad kahtlustatavad oma abi. Seda ei tohi vastu võtta, ükskõik kui siiras see ka ei tunduks.[24]

Paljudes IT seadmetes sisalduvad andmed on kergesti muudetavad või kustutatavad. Isegi tähtsusetuna tunduv tegevus võib ohustada tõendi kohtukõlbulikkust.[24]

Oluline on teada, et IT seadmete kasutamisel jäävad tegevusest enamasti maha jäljed, mis võivad tagantjärele tuvastada, millal seade viimati töötas ning mida sellega tehti. Kui selgub, et seade on töötanud pärast seda, kui politsei oli seadme ära võtnud, annab see kaitsjale võimaluse väita, et politsei on süüstavad tõendid ise tekitanud. Vähemalt saab kaitsja öelda, et politsei ei tegutsenud vastavalt oma parimatele tavadele. Käitumisjuhiseid IT seadmetega ümberkäimisel peab teadma iga politseiametnik, kes sündmuskohal/läbiotsimiskohal puutub kokku võimalike tõenditega.[24]

---

[23] U.S. Department of Justice, *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders*, välja antud november 2009, lk 5, 37-38

[24] Keskkriminaalpolitsei, Tallinn 2005, *Infotehnoloogiakuritegude menetlemise käsiraamat versioon 1.0*, Phare mestiprojekt EE 03 IB JH 04, lk 15

Tõendite talletamine

Kui ei ole õpitud kuidas digitaalsete tõenditega ümber käia:

- Ei tohi püüda uurida või leida arvuti või muu elektroonilise seadme sisu
- Ei tohi muuta arvuti või muu elektroonilise seadme seisundit
- Ei tohi vajutada nuppe ega hiirt
- Kui arvuti või muu seade on välja lülitatud, tuleb see nii jätta
- Ei tohi liigutada arvutit või muud elektroonilist seadet, mis on sisse lülitatud
- Ei tohi aktsepteerida abi pakkumisi või muud tehnilist abi tundmatutelt isikutelt
- Tuleb digitaalsete tõendite kohta abi küsida väljaõppe saanud ning vajaliku tehnikaga varustatud personali käest [25]

Kuigi andmekandjatelt tõendite otsimisega tegelevad otseselt vaid üksikud politseiametnikud, on kõigil siiski hea teada, kuidas see toimub.[26]

Peale seadme või andmekandja äravõtmist antakse andmekandja üle vaatluseks IT kuritegude spetsialistidele prefektuuris, Keskkriminaalpolitseis või saadetakse Eesti Kohtuekspertiisi Instituudi IT-osakonna ekspertiisi.[26]

Prefektuuride ja KKP spetsialistide ning EKEI ekspertide tegevus vaatluse/ekspertiisi läbiviimisel on paljuski sarnane.[26]

Esmalt tehakse andmekandjast korrektne üks-ühene koopia (tõmmis). Seejärel uuritakse seda koopiat, kasutades uuringuarvutis töötavat spetsiaalset tarkvara, mis võimaldab suure hulga andmete seast välja sõeluda need tõendid, mis omavad kriminaalasjas tõenduslikku tähtsust. Seejuures on abiks kriminaalasja menetleva ametniku poolt esitatud otsingumärksõnad – näiteks uimastite tootmise puhul lähteainena kasutatavate kemikaalide nimetused vms. Arvutikriminalistika tarkvara võimaldab tuvastada ka tavatarkvaraga kättesaamatud andmed, näiteks kasutaja poolt kustutatud failid.[26]

Uuringu tulemused edastatakse menetlejale vaatlusprotokolli (prefektuurid ja KKP) või ekspertiisiaktina (EKEI), mis lisatakse toimiku materjalide juurde.[26]

Andmekandjate hulka kuuluvad nii mobiiltelefonide SIM-kaardid või digikaamerate mälukaardid kui ka suure andmemahuga kõvakettad. Ainus praktiline viis kõvaketastelt

[25] U.S. Department of Justice, *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders*, välja antud november 2009, lk 11-12

[26] Keskkriminaalpolitsei, Tallinn 2005, *Infotehnoloogiakuritegude menetlemise käsiraamat versioon 1.0*, Phare mestiprojekt EE 03 IB JH 04, lk 15

tõendeid otsida on arvutivõimsuse ja spetsiaalse tarkvara abil. Tuleb teostada süstemaatiline uuring, mis põhineb juhtumi kohta olemasoleval informatsioonil ning menetleja poolt etteantud otsingukriteeriumitel. Uurija ning spetsialist peavad seejuures tegema tihedat koostööd.[27]

Uurija:

- keerukamate juhtumite puhul konsulteerib IT kuritegude spetsialistiga juba enne läbiotsima asumist;
- tegutseb IT seadmete äravõtmisel juhindudes seadusest ja käesolevas käsiraamatus toodud käitumisjuhistest;
- annab äravõetud materjali viivitamata üle, täites selleks vastava vormi;
- abistab arvutiuuringut teostavat spetsialisti juhtumi kohta käiva lisainformatsiooni ja täiendavate otsingukriteeriumite esitamisega.[27]

IT kuritegude spetsialist:

- läheb läbiotsijatega kaasa, kui asjaolud seda nõuavad, ja abistab neid läbiotsimisel;
- teeb andmekandjatest uuringukoopiad (üksühesed tõmmised);
- teostab koopia alusel uuringu (vaatlus);
- talletab uuringu tingimused, käigu ja tulemused (koostab vaatlusprotokolli);
- vajadusel annab kohtule selgitusi uurimistoimingu kohta.[27]

1.4. Üldised nõuded digitaalsete tõendite säilimiseks

Kui on tegemist kuriteoga, mis on toime pandud või seotud arvutiga, siis tuleb koheselt tegutseda, et kõik võimalikud tõendid jääksid alles.[28]

Vaata, millises seisus seade on – näiteks kui arvuti on välja lülitatud, siis tuleb see jätta välja lülitatuks. Kui arvuti on aga sisse lülitatud, siis tuleb jätta nii ning ise mitte proovida arvutist midagi otsida.[28]

Kui seade on sisse lülitatud, ei tohi seda mingil juhul välja lülitada sest väljalülitamine võib aktiveerida lukumehhanismi.[28]

- Tuleb pildistada ekraani kui võimalik ja lindistada või filmida nähtav informatsioon

[27] Keskkriminaalpolitsei, *Infotehnoloogiakuritegude menetlemise käsiraamat*, 2011, Phare mestiprojekt EE 03 IB JH 04, uuendatud JLS/2009/ISEC/AG/077, lk 17-18

[28] United States Secret Service, *Best practices for seizing electronic evidence v.3 A pocket guide for first responders*, lk 3

- Tuleb eemaldada kõik voolukaablid (tavaliselt on parem kui eemaldada need allikalt mitte seinast)
- Ei tohi proovida vaadata andmeid või üldse mingisuguseid salvestatud meediat[29]

Kui seade on välja lülitatud, ei tohi seadet sisse lülitada sest see võib muuta või hävitada tõendid arvuti süsteemis.[29]

Kui tekib kahtlus, et arvuti püüab kuidagimoodi selles leiduvaid tõendeid hävitada, tuleb arvuti koheselt välja lülitada – eemaldades peavoolujuhe.[29]

Tuleb lahti ühendada kõik telefoniliinid, tehes seda pigem seinast kui seadmest. Seejärel tuleb dokumenteerida ja sildistada.[30]

Koguda ja lindistada oluline informatsioon:

- Tuleb korjata kokku käsiraamatud ja teised juhised, mis on saadaval
- Lindistada oluline informatsioon [30]

Üheks heaks võimaluseks talletada seadme lahti ühendamisel kõik nii nagu algselt on, on sildistamine. Sildistamise abil saab hiljem tuvastada, milline juhe kus kohas oli. Eriti hea on sellest ka pilti teha, et oleks ka teistele arusaadavam. Kindlasti tuleb kõik ka protokolli kirja panna. Kõik tehtud tegevus tuleb dokumenteerida.[30]

Tuleb kinni pidada üldisest pakkimise, transportimise ja ladustamise juhistest:

- Kuna patareidel ja akudel on limiteeritud eluiga, võivad andmed kaduda kui patareid saavad tühjaks.
- Seega, tuleb võtta ühendust spetsialistiga ning teavitada et antud telefon, mis on aku või patareidega varustatud, on vaja kiirest ekspertiisi saata.[30]

NB! Arvuti ja teiste elektroonikaseadmetega tuleb kindlasti arvestada staatilise elektri ohuga. Arvuti juhtmete lahti ühendamiseks peab seade olema vooluvõrgust eemaldatud. Äärmiselt soovitatav on enda maandamine kaablite lahtiühendamisel – tuleb võtta palja käega kinni arvutikorpuse metallosast. Staatilist elektrit ei maksa alahinnata.[31]

[29] United States Secret Service, *Best practices for seizing electronic evidence v.3 A pocket guide for first responders*, lk 3
[30] Seizure of e-evidence, 2003
[31] Infotehnoloogia ekspertiiside määramise juhend EKEI, Pavel Laptev, uuendatud 11.08.2009

2. PÕHJA PREFEKTUURI POLITSEIAMETNIKE PÄDEVUS DIGITAALSETE TÕENDITE TALLETAMISEL

Antud lõputöös on uurimisprobleemina käsitletav asjaolu see, et üha suurema digitaliseerumise tõttu ei pruugi politseiamentikud omada piisavalt laialdasi eriteadmisi taoliste tõendite kogumise ja talletamise osas.

Lõputöö eesmärgiks on Põhja Prefektuuri politseiametnike sündmuskohal talletamisega seonduvate probleemide olemasolu ja nendega seonduvate asjaolude väljaselgitamine.

Uurimuse põhjal otsitakse informatsiooni tõendite talletamisel tekkinud komplikatsioonidest – kas on midagi valesti läinud või on kõik alati saadud tõendamiskõlbulikena talletada.

Uurimuse raames on pädevust määratletud kui igakülgset ja arengutega kaasaskäivat teadmist digitõendite talletamisel.

Lähtudes püstitatud uurimiseesmärgist ja sellele tuginevatest uurimisküsimustest, teostati käesoleva lõputöö puhul kvalitatiivse uurimismeetodina intervjuude läbiviimine. Kuna lõputöö eesmärgiks oli selgitada digitaalsete tõendite talletamisega seonduvaid probleeme Põhja prefektuuri politseiametnike näitel, siis moodustati intervjuude valim nende tööga kokku puutuvate ja ülevaadet omavate Põhja Prefektuuri kriminalistide (9 isikut) ja kriminaalasjade üle järelevalvet teostavate Põhja Ringkonnaprokuratuuri prokuröride ning prokuröri abide hulgast (10 isikut). Samuti ka Põhja Prefektuuri uurijate hulgas, kes puutuvad digitaalsete tõenditega oma töös kokku igapäevaselt. Kahjuks moodustas valimi vaid 3 isikut neljast osakonnast, kuna rohkem vastajaid lihtsalt ei olnud.
Andmete kogumine toimus 2012 aasta märts-aprill ning 2013 aasta märts-mai.
Selle aja jooksul viidi läbi intervjuu Põhja Prefektuuri kriminalistide ning selle talituse juhi hulgas. Saamaks teada, kuidas nemad digitaalsete tõenditega kokku puutuvad. Samuti ka kriminalistide teadmised antud valdkonnas – kas nad oskavad digitaalseid tõendeid õigesti talletada. Antud intervjuud toimusid 2012 aasta märtsis-aprillis ning 2013 aasta märtsis-aprillis. Intervjuu viidi läbi nii telefoni teel kui ka kohapeal, küsimustiku abil (vt LISA 1), mis koostati lähtudes uurimisküsimustest. Intervjuudele antud vastused fikseeriti sõltuvalt vastajast kas paberkujul või elektroonselt. Kokku töötab antud teenistuses 16 kriminalisti ning

lisaks ka nende juht. Intervjuule vastas 50% antud teenistuse kriminalistidest, lisaks talituse juht.

Teisena viis töö autor läbi intervjuu Põhja Ringkonna prokuröride ning abiprokuröride hulgas. Saamaks teada, millised on digitaalsete tõendite talletamisel kitsaskohad ning probleemid, kes neid nn "vigu" peamiselt teevad ning mis see põhjus nende arvates on. Antud intervjuu toimus 2013 aasta märtsis-aprillis. Intervjuu viidi läbi küsimustiku abil (vt LISA 2), mis koostati lähtudes uurimisküsimustest. Intervjuule vastas 10 prokuröri ja abiprokuröri kolmest erinevast osakonnast. Kõik intervjuule antud vastused on elektroonsed.

Kolmandana viis töö autor läbi intervjuu Põhja Prefektuuri uurijate hulgas, kes puutuvad oma igapäevatöös kokku digitaalsete tõenditega. Antud intervjuu toimus 2013 aasta aprillis-mais. Intervjuu viidi läbi küsimustiku abil (vt LISA 3), mis koostati lähtudes uurimuse teoreetilisest ülesehitusest. Küsimustik saadeti kokku neljale kriminaalbüroo osakonnale kuid vastas 2 Põhja Prefektuuri kriminaalbüroo majanduskuritegude osakonna uurijat ning 1 narkokuritegude osakonna uurija. Kõik antud vastused on kirjas elektroonselt.

Intervjueeritavatele selgitati enne vastamist, mida käesoleva lõputöö autor digitaalsete tõendite ja nende talletamise all silmas on pidanud. Seda selleks, et intervjueeritavad saaksid aru, mille kohta küsimustik täpsemalt käib.

2.1. Uurimustöö tulemused ja analüüs

Järgnevalt on välja toodud kolme erineva intervjueeritud grupi vastuste põhjal tehtud tulemused ja analüüs.

Kriminalistide hulgas tehtud intervjuude analüüs ja tulemused

Kokku intervjueeriti 8 kriminalisti lisaks talituse juhile, kes töötavad Põhja Prefektuuri kriminalistikatalituses – see on 50% antud talituses töötavatest kriminalistidest.

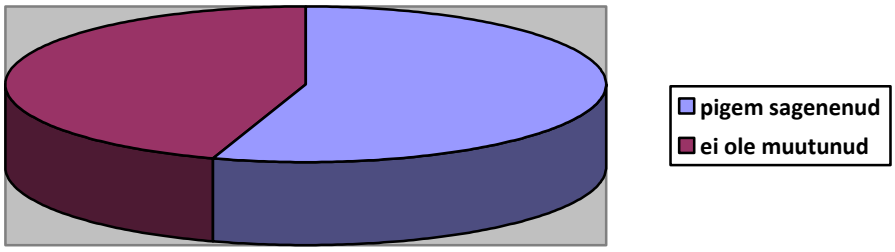
Tööstaažid varieeruvad alates 5-st kuni 23-ni. Kriminalistina töötamise aeg varieerub samuti väga vähesest kuni paljuni ehk siis – pooleteisest aastast kuni 19-ni. Üldiselt on intervjueeritud kriminalistid muul politseiametniku ametikohal tööl olnud vähemalt 2 aastat – enne kriminalistina tööle asumist. See aga näitab seda, et kriminalistide töö on üliolu line ning kohe peale politseikooli lõppu sinna nii lihtsalt tööle ei saa.

Küsimusele, kes peamiselt talletavad sündmuskohal digitaalseid tõendeid – kas Teie, kui kriminalistid, või muudel ametikohtadel töötavad politseiametnikud, vastas 78% (7 isikut) vastanud kriminalistidest, et peamiselt talletavad sündmuskohal digitaalseid tõendeid nemad – kriminalistid. Täpsustava lausena on üks intervjueeritav lisanud ka seda, et sündmuskohal töötavate kriminalistide puudumisel teevad seda ka teised politseiametnikud muidugi juhul kui osatakse ise teha. Lisaks sellele veel vajavad selliseid tõendeid sellised politseiametnikud, kes ei kaasa väga kriminaliste vaid oskavadki ise seda kõike teha. Ühe vastanu arvates tekib aga vajadus kohe kui sündmuskohal või selle vahetus läheduses on valvekaamera. Kui pole teada kurjategija sündmuskohalt lahkumise viis/suund või on see just teada ning on võimalik saada täiendavat informatsiooni kurjategija(-te) kohta.

Intervjuu tulemusena saadi teada, et erinevatel sündmuskohtadel on kriminalistidel vaja digitaalseid tõendeid ja/või nende andmekandjaid talletada üldiselt väga harva – ligikaudu 5% juhtudest. Intervjueeritavad vastasid täpsustava lausena, et kõikidest neil olevatest sündmustest on ligikaudu 6 juhtumit aastas, mille puhul on vaja digitaalseid tõendeid talletada. Taoliste juhtumite puhul on valdavalt tegemist raskete isikuvastaste kuritegudega – ehk siis surmaga (enesetapud, tapmised). Samuti lisas intervjueeritav, et enesetappude puhul näiteks kui kuskil ei ole hüvastijätu kirja jäetud ja kui sündmuskohal on arvuti, pakendatakse arvuti normidele vastavalt ning saadetakse eksperdile uurimiseks. Seda selleks, et ehk leidub seal digitaalse tõendina mingisugunegi enesetapukiri – mis annab infot toimunud sündmuse kohta. Samuti leidub aeg-ajalt selliseid sündmuskohti, kus on vaja talletada digitaalseid tõendeid ja/või nende andmekandjaid, ka röövimiste ja varguste puhul. Seal siis täpsemalt näiteks kas telefonide näol või erinevate andmekandjate (mälupulgad, jm) näol. Erinevatel andmekandjatel võib leiduda informatsiooni kurjategijate või teo toimepanemise kohta. Muidugi võib ka lisada need sündmused, kus on olemas valvekaamerad, mis on sündmuse hetkel töötanud - taskuvargused, tänavaröövid, peksmised, avalikud/salajased vargused asutustest. Kõik eelpool mainitu, näitab seda, et peamiselt ei ole selliseid sündmuskohti nende igapäevatöös. Ning mõningatel juhtudel käivad ka teised politseiametnikud sündmuskohal erinevaid digitaalseid tõendeid ja/või andmekandjaid talletamas. Samuti selgus intervjuu tulemusena ka see, et selliste juhtumite alla, kus kriminalistidek on vaja digitõendeid talletada, kuuluvad ka seksuaalkuriteod ning ka majanduskuriteod.

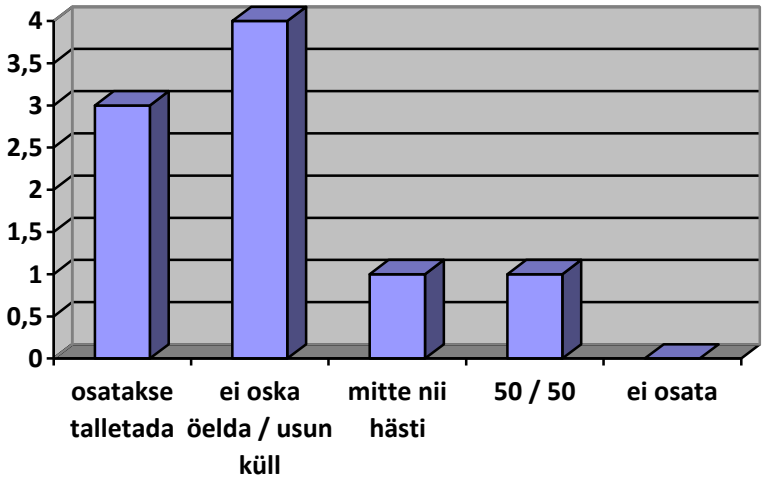
Küsimusele, kas viimasel ajal on sagenenud digitaalsete tõendite talletamine sündmuskohal või on see pigem vähenenud, vastas (vt joonis 1) ligikaudu 55% vastajatest (5 isikut), et see on pigem sagenenud kui vähenenud. Peamiselt on sagenemise põhjusena intervjueeritud

kriminalistid välja toonud selle, et elu areneb pidevalt edasi. Samuti ka seetõttu, et pidevalt võetakse aina uusi ja uusi digiseadmeid kasutusele. Arvatakse ka et digitaalsete tõendite talletamine on ka selle tõttu sagenenud, et inimesed jätavad oma jälgi igale poole – arvutitesse, internetti ning on ka suurenenud videovalve osakaal. Üldiselt võib öelda, et elu on muutunud interaktiivsemaks ning digiseadmeid kasutatakse rohkem kui enne. 45% vastanud kriminalistidest (4 isikut) ütles, et sagedus ei ole nende arvates muutunud – või vähemalt nendel endil ei ole olnud rohkem selliseid sündmuskohti kui enne.



Joonis 1. Digitõendite osakaal viimastel aastatel

Küsimusele: Kas teistel ametikohtadel töötavad politseiametnikud oskavad Teie arvates korrektselt talletada digitaalseid tõendeid, vastasid intervjueeritud kriminalistid väga erinevalt (vt joonis 2). Nimelt 33% vastanud kriminalistidest (3 isikut) vastas, et teistel ametikohtadel töötavad politseiametnikud oskavad korrektselt talletada digitaalseid tõendeid. 44% vastanud kriminalistidest (4 isikut) kirjutas vastusena „ei oska öelda“ või “usun küll”. 11% (1 isik) jällegi, et „mitte nii hästi“. Üks vastanutest kirjutas vastuseks „50/50“. Täpsemalt tähendab see vastanu arvates seda, et mõningad politseiametnikud, kes töötavad teistel ametikohtadel ning käivad sündmuskohtadel digitaalseid tõendeid ja/või nende andmekandjaid talletamas, oskavad neid talletada. Mõned üksikud aga ei oska. Vastustest võis välja lugeda, et üldiselt ei soovitud kolleege halvustada ja nende puudustele avalikult osutada. Me kõik võime ju osata ühte asja väga perfektselt kuid teist mitte nii hästi.

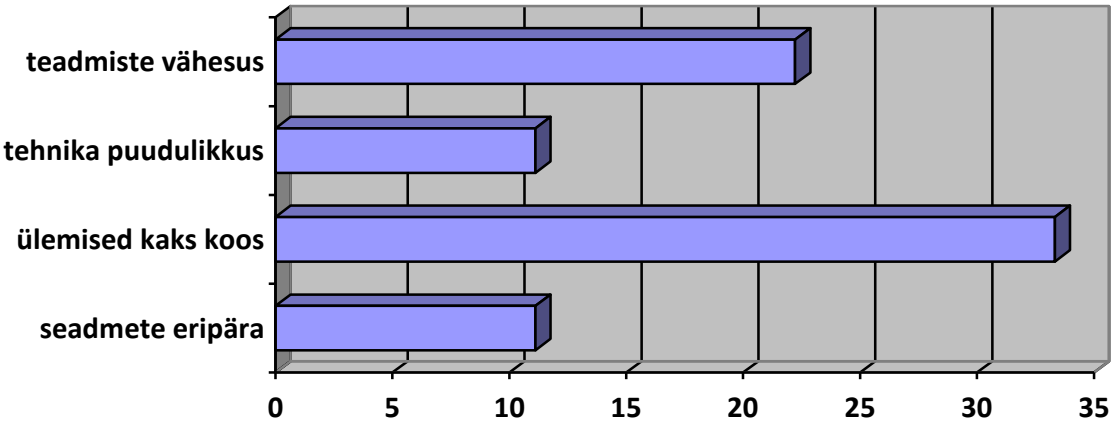


Joonis 2. Politseiametnike oskus talletada digitaalseid tõendeid

Ka küsimusele: Kas on esinenud juhtumeid, kus mingisuguste eripärade tõttu on tõendite talletamisel esinenud probleeme, vastasid intervjueeritud kriminalistid erinevalt. Nimelt 78% (7 isikut) intervjueeritud kriminalistidest vastas ei ning 22% (2 isikut) vastas antud küsimusele jaatavalt. Peamiselt on ebaõnnestumise põhjuseks see, et sündmuskohal puudub vajalik tehnika ning tänu sellele on ebaõnnestunud ka talletamine.

Sündmuskohal digitaalsete tõendite ja/või andmekandjate talletamisel ebaõnnestunumise kohta vastas 78% (7 isikut) intervjueeritud kriminalistidest, et ei ole enda teada ebaõnnestunud. Kaks vastanut aga ei osanud öelda sest pole negatiivset tagasisidet olnud. Selle kohta, kas intervjueeritud kriminalistid teavad juhtumeid, kus teised politseiametnikud on sündmuskohal talletanud digitaalseid tõendeid ning hiljem tuleb välja, et need ei ole tõendamiskõlbulikud, ei tea osatud kommenteerida kuna puudus vastavasisuline tagasiside.

Selle põhjuseks, miks mõningaid digitaalseid tõendeid ja/või nende andmekandjaid ei suudeta tõendamiskõlbulikena talletada, vastasid kriminalistid erinevalt (vt joonis 3). 22% (2 isikut) intervjueeritutest on antud põhjusena välja toonud teadmiste vähesuse. Üks vastanu tõi aga välja tehnika puudulikkuse – ei ole piisavalt ajakohast tehnikat, et talletada korralikult. Samas tõi teine intervjueeritav antud vastusena välja seadmete eripära, st et mõningate seadmete puhul ei olegi võimalik kõiki tõendeid tõendamiskõlbulikena talletada. Sel juhul peab arvestama ka seadme omaniku poolt seatud seadistustega, mis vale käitlemisega võivad hävineda. Kolm vastanut kümnest (33%) tõid vastusena välja mõlemad variandid – nii tehnika puudulikkuse kui ka teadmiste vähesuse. 22% (2 isikut) vastanud kriminalistidest aga ei osanud selle kohta midagi öelda.



Joonis 3. Digitõendite vale talletamise põhjused

Tehtud täienduskoolituste küsimusele vastasid suurem osa intervjueeritud kriminalistidest (55% - 5 isikut), et neid on vähe ja võiks olla rohkem. Üks vastanu kirjutas vastusena et tema arvates on neid piisavalt ning üks vastanu, et oleks vaja tehnikat. Öeldi ka veel, et kui oleks selle alane koolitus, siis miks ka mitte. Antud küsimuse kohta saadud vastused näitavad seda, et meie pidevalt arenevas ühiskonnas on veelgi enam vaja täiendada oma teadmisi ja tehnikat selles valdkonnas, mis on seotud ühiskonna kiire arenguga. Samuti näitab see seda, et hetkel tööl olevad kriminalistid soovivad ennast pidevalt arendada ning tahavad olla igas valdkonnas paremad ning omada rohkem teadmisi. Muidugi tõi üks vastaja välja ka oma arvamuse, et see teema ei ole kriminalistide seisukohalt primaarne – kokkupuuteid on vähe, probleeme pole tekkinud, seega ei pea täiendkoolitusi esmatähtsaks. Tavaliselt aitab üldine tehniline taiplikkus või kõne teadjamale kolleegile. Mis on ka tegelikult väga õige tähelepanek, sest kriminalistide töös on muid primaarseid teemasid, mille alaseid täienduskoolitusi oleks vaja rohkem kui ainult digitaalsete tõendite kohta.

Kokkuvõtvalt võib öelda, et kriminalistid ei puutu sündmuskohtadel eriti digitaalsete tõenditega (arvutid, telefonid, jm) kokku. Pigem tegelevad sellega muud politseiametnikud, kes sündmuskohale lähevad. Intervjuu tulemusena selgus, et kui siiski on kriminalistidel kokkupuuteid digitaalsete tõenditega (aastas ligikaudu 5%), siis on need olnud alati positiivsed. Talletamisel ei ole midagi valesti läinud ega ka muid suuri puudusi ette tulnud. Kõik on saadud alati tõendamiskõlbulikena talletada. Kui aga on olnud mingisugust nõu või teadmisi juurde vaja, osatakse alati kellegi poole pöörduda – olgu selleks siis kaaskolleeg, kes teab rohkem või siis ekspert.

Koolituste küsimuse kohta sooviksid nad kõik neid juurde. Mõningal napib teadmisi ning sooviks neid omada. Mõni jällegi soovib lihtsalt oma teadmisi täiendada ning pidevalt kursis olla kõigega, mis mingilgi määral seotud nende tööga. Mõni aga soovib lihtsalt saada juurde teadmisi selle kohta, mis lihtsalt ühel hetkel võib töös kasutusele tulla kuid ei pruugi.

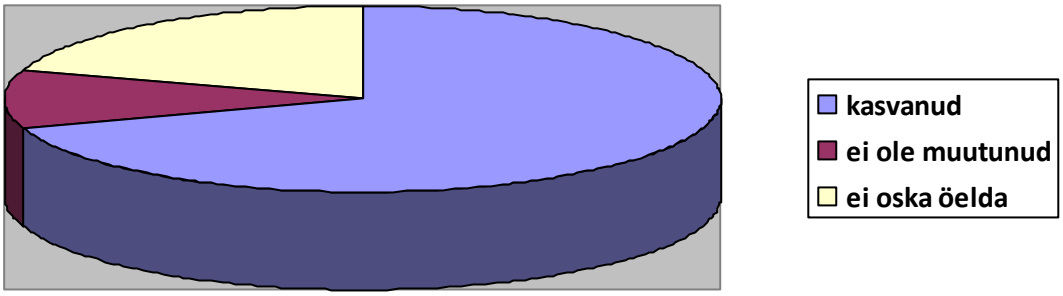
Prokuröride hulgas tehtud intervjuu analüüs ja tulemused

Intervjuule vastas kokku 10 prokuröri ja abiprokuröri kolmest erinevast Põhja Ringkonna prokuratuuri osakonnast.

Põhja Prefektuuride menetluses olevate kriminaalasjadega on vastanud tegelenud ja neid juhtinud enamuses juba vähemalt 3 aastat. Kaks vastajat on ka vastavalt 13 ja 15 aastat. Keskmiseks töötatud aastateks tuleb vastanute põhjal ligikaudu 8 aastat.

Põhja Prefektuuri juhtumitega, millistes on tõendeid saadud digitaalsetest allikatest, puutuvad 70% vastanutest (7 isikut) kokku mõned korrad aastas. Ning 30% (3 isikut) vastanutest ütles, et tihti. Võiks lausa öelda, et iga kolmas kriminaalasi on kas otseselt või kaudselt seotud digitaalsete tõenditega. Peamiselt on sellisteks juhtumiteks arvutikelmused, omastamised, maksukuriteod (majandustegevused). Muidugi on ka muid juhtumeid, kuid need on vastanud välja toonud ning nendes puututakse digitaalsete tõenditega kõige rohkem kokku. Üks vastaja tõi välja ka selle, et viimase statistika kohaselt on kelmuste arv aastaga kasvanud ligi 30%.

Küsimusele, kas digitaalsete tõendite osakaal viimase kolme aasta jooksul on kasvanud või mitte (vt joonis 4), vastas 70% intervjueeritavatest (7 isikut), et nende arvates on kasvanud. Vastusena ei oska öelda, vastas 20% (2 isikut) vastanutest ning 10% (1 isik), et tema arvates ei ole muutunud. Seda et kahanenud on, ei vastanud keegi. Kasvu põhjuseks on intervjueeritavad toonud välja erinevaid aspekte. Ühed kirjutasid põhjuseks, et kurjategijad on nooremad ja targemad ning tehnika ja programmidega hästi varustatud. Üks tõi põhjusena välja ka selle, et tavaliste tõendite osakaal langeb ja kaitsjate oskus neid tõendeid nn „nullida“, kasvab pidevalt. Seetõttu on vaja ka otsida uusi lahendeid teatud kriminaalasjades. Seepärast on ka kasvanud jälitustõendite ja digitaalsete tõendite hankimine.

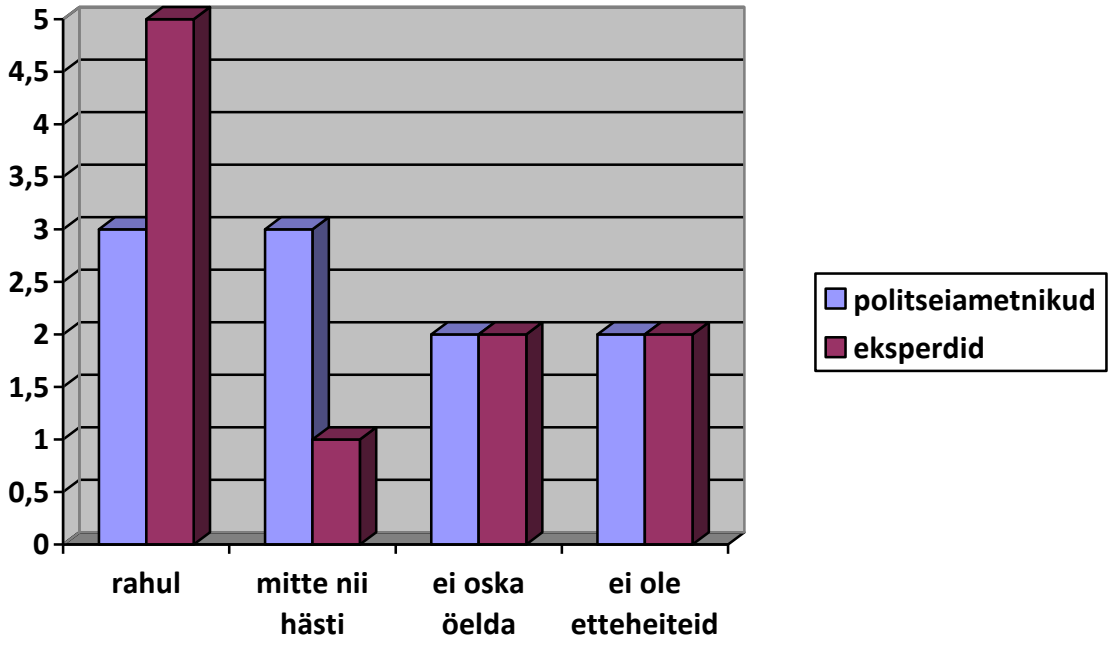


Joonis 4. Digitõendite osakaal viimaste aastate jooksul

Selle kohta aga, et kes on peamiselt nende menetluses olevate kriminaalasjade digitaalsete tõendite talletajateks, saadi väga erinevaid vastuseid. 3 vastanut kirjutas vastuseks et põhiliselt (90%) on digitaalsete tõendite talletajateks politseiametnikud, menetlejad ning ülejäänud (10%) ulatuses eksperdid. Teise vastusena saadi, et politseiametnikud talletavad lihtsamaid digitaalseid tõendeid ning eksperdid siis raskemaid. Ühe vastusena oli välja toodud ka see, et on esinenud selline juhtum, kus uurija oleks pidanud ise digitaalset tõendit uurima, kuid saatis hoopis eksperdile. Nimelt oli antud asjas vaja teha mailbox'i vaatlust. Vastanu arvates peaksid oskama seda mistahes kaasaegsed uurijad. Ühe probleemina, miks digitaalseid tõendeid ei taheta nii väga kasutada ning sageli jäetakse menetluses välja, tõid vastajad välja selle, et meie EKEI IT-ekspertiisis on tohutud järjekorrad – isikkoosseis väike. Milleks siis raisata IT-ekspertide niigi väärtuslikku aega ja tööressurssi sellise kergema asja peale mida saab ka ise teha. Samas on mõningad vastajad välja toonud ka koostöö – selle all siis mõeldud koostööd nii ekspertide kui ka politseiametnike vahel. Kui midagi jääb arusaamatuks siis osatakse alati kellegi poole pöörduda – olgu selleks siis ekspert või mõni muu, kes oskab rohkem informatsiooni pöördutava asja kohta anda.

Küsimusele, kus paluti hinnata enda kogemustele toetudes digitaalsete tõendite talletamise pädevust nii politseiametnike kui ka ekspertide poolt, vastati väga erinevalt (vt joonis 5). Nimelt ütles 50% vastanutest (5 isikut), et ekspertide tööga ollakse rahul. Samas kui politseiametnike tööga ollakse rahul vaid 30% vastanutest (3 isikut). Ehk kaks vastanut nende viie hulgast kirjutasid, et eksperdid on pädevad, kuid politseiametnikud mitte. Samuti arvas 20% vastanutest (2 isikut), et politseametnikud ei oska nii väga hästi digitaalseid tõendeid talletada. Kuid siiski kirjutati ka samade vastajate poolt vastuseks, et oleks vaja teadmisi tõsta,

kas siis koolitustega või kuidagi muudmoodi. Üks kirjutas ka vastuseks, et ollakse pädevad siis kui on täpne juhis kätte antud. Siiski talletatakse ka asju, mida vaja ei ole. Politseiametniku ebapädevuse põhjusena tõi üks vastaja välja mitte oskamatuse, vaid motivatsiooni puuduse, sest tegelikult puutub iga politseiametnik oma igapäevaelus kokku erinevate andmekandjatega – arvutite, mobiiltelefonide ja muu sellisega. Sama vastanu arvates on paljudelt andmekandjatelt andmeid lihtne kätte saada, kuid mõned lihtsalt ei soovi seda teha. Siiski leidub ka selliseid politseiametnikke, kel puuduvad isegi elementaarsed arvutikasutamise oskused (nt oskus leida faili, näidata mõne faili asukohta, teha väljatrükke, vms). Koolis on seda õpetatud, kuid siis ei ole piisavalt teadmiste omandamisele tähelepanu pööratud või on lihtsalt unustatud. Intervjueeritavate hinnangutest nähtub, et ekspertide oskused on tasemel. Joonist vaadates saab aru, et tegelikult ei olda politseiametnike tööga rahul, kuivõrd vaid kahel vastajal kümnest ei ole etteheiteid. Siiski on positiivne see, et ekspertide tööga ollakse rohkem rahul kui politseiametnike.



Joonis 5. Politseiametnike ja ekspertide oskus talletada digitaalseid tõendeid

Küsimusele kas on täheldatud digitaalsete tõendite talletamisel mingisuguseid puudusi, vastasid peaaegu kõik jaatavalt. Peamiselt on puudustena välja toodud tehnika, selle puudumine; teadmiste puudulikkus, see, et ei osta talletada või ei osata tehnikat käsitleda. Jällegi on välja toodud EKEI võimekus – piiratud on ekspertiiside või uuringute läbiviimine. Samuti on välja toodud ka kogemuste puudumine. Üldjoontes ollakse rahul kuid tõdetakse, et

alati saab paremini. Seda, kelle poolt olid puudustega tõendid talletatud ning millist kaalu need menetluses omasid, ei osanud keegi täpsemalt öelda.

90% vastajatest (9 isikut) on seisukohal, et tegelikkuses on digitaalsete tõendite talletamine problemaatiline. Üldiselt on küll menetlejate või uurijate poolt vajalikud toimingud ära tehtud, kuid siiski on vastanud seisukohal, et nii politseiametnikele kui ka prokuröridele oleks vaja veelgi rohkem koolitusi antud teema valdkonnas. Elu on pidevas arengus ja iga päevaga tekib aina uusi digitaalseid tõendeid ning kohti kus need paiknevad, juurde. Selle tõttu on vaja viia läbi koolitusi, sest pidevalt avastatakse midagi uut. Samas vajaks ka mõni harva esinev talletamisega seonduv asjaolu koolitusel kinnistamist. Kindlasti oleks hea saada ka praktilisi kogemusi lisaks koolitustele. Sealhulgas rohkem praktilist koostööd teiste riikide kolleegidega. Üks vastaja tõi välja ka selle, et tema arvates oleks kõige olulisem õpetada digitaalsete tõendite fikseerimist menetlusse ehk kuidas selliseid tõendeid korrektselt vormistada. Teine vastaja tõi välja selle, et uurijad ei oska talletada digitõendeid eeskätt selles mõttes, et nad ei tea kust neid otsida ning nad ei soovi ka eriti ennast selles valdkonnas täiendada. Selle vastaja arvates valitseb arusaam, et arvutist informatsiooni saamine on liiga spetsiifiline tegevus ja sellega peavad tegelema ainult vastava ala spetsialistid.

Muutuste kohta vastas samuti pea 90% (9 isikut), et oleks vaja juurde koolitusi. Üks vastaja tõi lausa välja, mida oleks tema arvates vaja muuta: oluline on koolitus IT-valdkonnas, mida otsida sündmuskohal ja mida-kuidas ära võtta, talletada. Kuidas leida tõendit, kellelt abi saaks küsida, kas seda tõendit üldse on mõtet otsida? Millised sammud teha, et tõendit, mida me veel leidnud ei ole, ei hävitataks menetluse jooksul. Vastaja sõnul on olnud kohtunikega vaidlus, et kas internetis tagant järgi kirjavahetuse lugemine peab ikka kohtu loal olema või mitte. Milline võimekus on politseil, kui puuduvad kirjavahetuse lugemiseks paroolid? Teine vastaja kirjutas, et probleeme on tekkinud selliste tõenditega, mille puhul algselt ei ole teada selle olulisus, kuid millelt hiljem tuleb välja oluline tõend. Läbiotsimise käigus ei ole aga antud tõend korralikult pakendatud või pitseeritud ning hiljem ongi kohtus selle tõendi usaldusväärsuse tõendamisega probleeme.

Probleeme on palju, kuid siiski on läbivaks vastuseks, prokuröride arvates, asjade paremaks muutmisel koolitus. Ühe võimalusena tõi üks intervjueeritav välja ka soovituse: kuna menetlusseadustik võimaldab, tuleks rohkem kaasata spetsialiste, see tähendab isikuid, kellel on eriteadmisi; kes koos uurijatega osaleb aktiivselt vastavate tõendite otsimises ja talletamises, kes hiljem võib vajaduse korral kohtus spetsialistina esineda ja nö kaitsta tõendeid kohtu ees.

Prokuröride hulgas tehtud intervjuu tulemusena võib öelda, et üldiselt ollakse rahul selle tööga, mida tehakse digitaalsete tõendite talletamisel. Seda siis kas sündmuskohal või ka hiljem kui selgub, et mõni digitaalne tõend on menetluse seisukohast oluline, kuid varem kahe silma vahele jäänud. Siiski võiks alati paremini olla ning politseiametnikel vastavaid teadmisi samuti rohkem olla.

Negatiivse asjaoluna võib välja lugeda aga selle, et ekspertidele digitaalsete tõendite leidmiseks või talletamiseks vajalikud tõendid jäetakse pigem ekspertidele saatmata või proovitakse kuidagi teist teed pidi tulemus kätte saada. Seda siis kas muude tõenditega või siis muu spetsialisti poole pöördudes. Nimelt on EKEI-s nii pikad järjekorrad ja antud osakonnas väike isikukoosseis, mistõttu ei jõuta asjadega kiiresti tegeleda. Lihtsam on ju pöörduda inimese poole, kes samuti oskab sama asja, kuid teeb selle poole kiiremini. Menetluse seisukohalt on see ka parem, sest siis jõuab menetlus kiiremini oma lõpuni.

Uurijate hulgas tehtud intervjuu analüüs ja tulemused

Kokku vastas 3 Põhja Prefektuuri uurijat. 2 neist olid Põhja Prefektuuri Kriminaalbüroo majanduskuritegude talitusest ning 1 vastanu oli Põhja Prefektuuri Kriminaalbüroo narkokuritegude talitusest. Kuna vastajaid oli kokku 3 siis saadud tulemusi ei saa üldistada, kuid neid kasutatakse lõputöös nende kolme isiku seisukoha kirjeldamiseks.

Vastanud on Põhja Prefektuuris uurijana töötanud juba vähemalt seitse aastat. Põhja Prefektuuris üldse, kuid teisel ametikohal on vastanud töötanud alates 11 aastast kuni 18,5 aastani. Põhja Prefektuuri juhtumitega, millistes on tõendeid saadud digitaalsetest allikatest, puutuvad kõik kolm vastanut kokku igapäevaselt – nende hulgas ka erinevate andmekandjate vaatlustega.

Kuna igapäevatöös puututakse kokku digitaalsete tõenditega, siis küsimusele, kust oma teadmised digitõendite kohta olete saanud, tõi üks vastanu välja, et on need saanud nii koolitustelt, spetsialistidega vesteldes kui ka ise internetist otsides. Teine vastanu koolitusi saanud ei ole ning teadmised tulevad töö käigus, elust enesest. Kolmas vastanu ei ole Eestis koolitustel käinud, küll aga välismaistel. Kolmas vastanu lisas veel seda, et 2006/2007 aastal on nende grupiga läbi viidud koolitus kogu Põhja Prefektuuri kriminaalbüroole, mis käsitles digitaalseid tõendeid, nende kogumist jne. Juhtumeid, milles tuleb ette digitaalseid tõendeid, on palju erinevaid. Üldiselt on nendeks kuriteod, mille eeluurimiseks on alustatud kriminaalmenetlus.

Digitaalsete tõendite osakaal viimase kolme aasta jooksul on kahe vastanu arvates kasvanud. Selle põhjuseks on nad välja toonud erinevaid aspekte. Ühe vastanu arvates on põhjuseks kindlasti interneti kasutajate arvu suurenemine mitte ainult Eesti vabariigis, vaid terves maailmas. Teine vastanu tõi põhjuseks selle, et tegusid toime panevate isikute teadlikkus politseitööst ning seadusesilma hammaste vahele jäämise vältimiseks on tõusnud. On juhtumeid, kus ainus viis isikut konkreetse kuriteoga seostada on analüüsida ja vaadelda temalt menetlustoimingutega kätte saadud tehnikavahendeid. Ka politsei teadlikkus ning võimalused tänapäevastest vahenditest tõendite leidmiseks on tõusnud. Samas kolmanda vastanu arvates on seda väga raske hinnata sest menetluslikult on digitaalsed tõendid lihtsalt üks tõendi liik. Pigem peaks vastanu arvates siinkohal küsima, kas selliseid tõendeid kasutatakse kohtus tõendina rohkem või mitte. Selle kohta aga prokuratuuri tagasiside puudub.

Küsimusele, kes on Teie arvates peamiselt digitaalsete tõendite talletajateks, kas teie kui uurijad või muud ametnikud (politseiametnikud, eksperdid), tuli väga erinevaid vastuseid. Nimelt ühe vastanu arvates talletavad menetlejad ja uurijad digitaalseid tõendeid kindlasti rohkem kui tavalised politseiametnikud (nagu näiteks patrullpolitseinikud, liikluspolitseinikud jne). Ekspertide töö osas ei osatud kommentaari anda. Teise vastanu arvates on peamisteks talletajateks politseiametnikud. Eksperdid ainult juhul kui on kaasatud uurimistoimingusse või on saadetud asitõendid ekspertiisi. Kolmas vastas, et tema arvates on see seotud konkreetse kuriteoliigi menetlemisega. Nt majandusalaste kuritegude, korruptsioonijuhtumite puhul, kus on mahukad materjalid ning suurem osa menetlustoimingute käigus ära võetud tõenditest asuvad andmekandjatel, on peamiseks talletajaks ilmselgelt ekspertiisiasutus, kes teostab antud esemetele ekspertiisi või siis vaatlust. Narkokuritegude puhul teeb selle töö suuresti ära menetleja/uurija, kes talletab ning säilitab muutmata kujul antud informatsiooni.

Küsimusele, kus paluti hinnata enda kogemustele toetudes digitaalsete tõendite talletamise pädevust nii politseiametnike kui ka ekspertide poolt, saadi erinevaid vastuseid. Ühe vastaja poolt toodi välja, et digitaalsete tõendite talletamisega pidevalt kokkupuutuvad politseiametnikud omavad rohkem kogemusi ja teadmisi. Ekspertide töö kohta ei osatud kommentaari anda. Teise vastanu arvates võiks tavapolitseinike tase võimalike digitõendite ümberkäimisel olla parem. Samuti peaks vastanu arvates panustama rohkem spetsialistidesse, kelle ülesandeks on erinevate andmekandjate vaatlus ning analüüs. Kolmanda vastanu arvates jätab menetlejate poolelt digitõendite talletamine soovida ning ekspertide osas ei oska kommenteerida. Vastanu arvates puuduvad politseil veel paljud vahendid, milliste kasutamine

on digitaalsete tõendite talletamisel ning fikseerimisel vajalikud. Samuti peaks iga menetleja saama ka vastava elementaarse esmase koolituse.

Küsimusele, kas digitaalsete tõendite talletamisel on täheldatud mingisuguseid puudusi, vastasid kõik jaatavalt. Puudustena on üks vastaja välja toonud tehnilise võimekuse – nt mobiiltelefonide vaatlusel peaks olema iga vaatlust teostava üksuse kasutuses vastav tarkvara, mis ei lubaks vaatluse käigus teha vaadeldavas objektis muudatusi. Vormistamine on iga üksuse puhul kohandatud vastava prokuröri soovidele ning vajadustele. Teise vastanu arvates on puudustena vormistamine, tehniline võimekus ja teadmiste puudulikkus ning lisaks ka liigne enesekindlus. Kolmanda vastanu arvates tuleks pöörduda abipalvega kolleegide poole kui endal jääb teadmistest puudu. Kolleegid selgitavad ja annavad nõu ning kui ise ei oska aidata, öeldakse, kelle poole võiks pöörduda.

Küsimusele, kui olete tuvastanud mingisuguseid puudusi digitaalsete tõendite talletamisel, siis kelle poolt olid antud tõendid talletatud (mitte nimeliselt) ja millist kaalu need kriminaalmenetluses omasid, vastas üks, et sellist juhust ei ole esinenud. Teine aga, et kuna enamus kokkuvõttega prokuratuuri saadetud menetlused lähevad kokkuleppemenetlusse, siis on üleüldse väga raske hinnata digitaalsete tõendite kaalu. Vigu tehakse nii esmasel kokkupuutel kui ka edasises käitlemises. Kolmas soovis öelda vaid, et digitaalsete tõendite vaatluseid tegevad ametnikud peavad olema oma töös tunduvalt korrektsemad, teadlikumad menetlusest, oma töö tähtsusest ning tõendi talletamise kvaliteedi olulisusest.

Vastavalt eelmisele küsimusele, arvatakse et digitaalsete tõendite talletamine Põhja Prefektuuris on problemaatiline. Muudatuste ja parandustena on vastanud välja toonud nii valdkonnapõhised koolitused kui ka konkurentsivõimelise palga, ehk vastanute arvates peaks palka tõstma selleks, et tõuseks ka motivatsioon tõendeid tõendamiskõlbulikena talletada. Ühe vastanu arvates aitaks muutusena teadmisi omavate isikute või spetsialistide kontaktide edastamine, kelle poole võiks vajadusel pöörduda. Ühe vastusena on välja toodud ka see, et oleks vaja rohkem riist- ja tarkvaralisi vahendeid. Samuti ka rohkem inimesi, kes digitõendite talletamisega tegeleksid. Üldiselt arvatakse, et inimesed küll õpivad töö käigus, kuid siiski oleks vaja ka rohkem selle teemalisi koolitusi.

2.2. Uurimustöö järeldused

Vastavalt tehtud intervjuu tulemusena võib öelda, et vastanute arvates on digitaalsete tõendite osakaal viimaste aastate jooksul kasvanud. Nimelt üle poole kolme grupi intervjueeritavatest tõdesid, et see on tõusnud. Samas oli ka neid, kes arvasid vastupidist.

Lõputöö eesmärgi saavutamiseks on püstitatud järgmised uurimisküsimused:

- Kes on sündmuskohal peamised digitaalsete tõendite talletajad?
- Kas sündmuskohal digitaalseid tõendeid talletavad ametnikud on piisavalt pädevad või mitte?
- Kas talletamise osas esineb puudusi/probleeme? Kui, siis milliseid?
- Milliseid muudatusi oleks vaja sisse viia, et digitaalseid tõendeid paremini talletada?

Järgnevalt on analüüsitud intervjuudest selgunud aspekte ning nende põhjal tehtud järeldused.

Esimene küsimus – kes peamiselt talletavad sündmuskohal digitaalseid tõendeid ja kas need ametnikud on piisavalt pädevad, leidis antud uurimustöös vastuse. Nimelt puutuvad prokurörid digitaalsete tõenditega kokku alles siis kui on juba kõik tõendid talletatud ning ka vaatlused tehtud, st prokurörid näevad kogu pilti tehtud tööde tulemuslikkusest. Uurija näeb seda kõike enne kui asi jõuab prokurörideni ning puutub selle kõigega ise suhteliselt palju kokku. Ekspert või kriminalist näeb aga selles osas suhteliselt vähe – ainult siis kui teda kaasatakse ning ta saab mingisugustki tagasisidet. Ei ole sätestatud, millise protseduuri puhul eksperte kaasatakse**,** kuid on välja kujunenud nende kaasamine eelkõige raskemate tõendite puhul. Mõnikord kasutatakse ka osakonnas leiduvate spetsialistide või IT-ametnike abi, et tõendeid talletada või uurida. Seda aga sellepärast, et ekspertidele tõendeid saates on vastuste saamine küllaltki pikaajaline protsess. Mõnikord on järjekorrad lausa 6 kuud, et suhteliselt kerge uuring teatud tõendi osas läbi viia. Vastustest selgus, et politseiametnikud seevastu puutuvad sündmuskohal tõenditega kõige tihedamini kokku.

Teine küsimus, kas sündmuskohal digitaalseid tõendeid talletavad ametnikud on pädevad või ei, leidis samuti oma vastuse. Vastavalt prokuröride, uurijate ja abiprokuröride hulgas läbi viidud intervjuu tulemusena võib öelda, et digitaalsete tõenditega tegelevad politseiametnikud

ei ole eriti pädevad. Nimelt ei ole politseiametnikud alati piisavalt hästi kursis, kuidas või mida täpselt talletada vaja on. Mõnikord võetakse liiga palju nn. tõendeid sündmuskohalt kaasa või siis teinekord jällegi vastupidi. Samas kriminalistide hulgas läbi viidud intervjuu tulemusena selgus, et nende arvates oskavad politseiametnikud piisavalt hästi digitõendeid talletada. Prokuröride ja abiprokuröride hulgas läbi viidud intervjuu tulemusena selgus veel ka, et eksperdid on väga pädevad, kuid ekspertiisi vastuse saamisega läheb kauem aega kui tavaliste spetsialistide käest vastuse saamisega.

Kolmas küsimus – kas talletamise osas esineb puudusi, mis on tekkinud digitaalsete tõendite talletamisel ning kelle poolt need tekkinud on, tuli ka antud uurimistöös välja. Nimelt antud intervjuu tulemusena selgus, et kuna peamiselt tegelevad sündmuskohal digitaalsete tõenditega politseiametnikud – uurijad, menetlejad, siis nende poolt tuleb ka kõige rohkem vigu. See on aga iseenesest loogiline, sest ei saa ju midagi valesti teha kui antud asjaga ei tegele. Samas on mõningad komplikatsioonid tekkinud ka tehniliste viperuste tõttu. Üldiselt ollakse aga digitaalsete tõendite talletamisega rahul – olgu see siis tehtud menetleja, uurija või eksperdi poolt. Muidugi alati saab kõike paremini.

Neljas küsimus – milliseid muudatusi oleks vaja sisse viia, et digitaalseid tõendeid paremini talletada, leidis ka intervjuudes vastuse. Suures osas kattub nii kriminalistide, uurijate kui ka prokuröride ja abiprokuröride arvamus. Nimelt selgus, et selle alaseid koolitusi on siiani suhteliselt vähe läbi viidud ning tuntakse et antud teemalisi koolitusi oleks rohkem juurde vaja. Samuti pole neid koolitusi ka väga palju tulemas. Kui mõni selle teemaline koolitus on tulemas, siis saab koolituse kohtade arv suhteliselt kiiresti täis. Käesoleva töö autori hinnangul sooviksid nii politseiametnikud, uurijad kui ka prokurörid osaleda koolitustel, mis hõlmab endas digitaalsete tõendite teemat: kuidas neid talletada, mismoodi neid säilitada ja palju muud. Seda eriti sellepärast, et elu areneb iga päevaga ning leitakse järjest uusi digitaalseid tõendeid või siis võimalusi mingisuguse tõendi talletamiseks. Me kõik soovime kursis olla kõige värskemate ja aktuaalsemate teadmistega.

KOKKUVÕTE

Lõputöö eesmärgiks on Põhja Prefektuuri politseiametnike sündmuskohal talletamisega seonduvate probleemide olemasolu ja nendega seonduvate asjaolude väljaselgitamine.

Lõputöö eesmärgi saavutamiseks on püstitatud järgmised uurimisküsimused:

- Kes on sündmuskohal peamised digitaalsete tõendite talletajad?
- Kas sündmuskohal digitaalseid tõendeid talletavad ametnikud on piisavalt pädevad või mitte?
- Kas talletamise osas esineb puudusi/probleeme? Kui, siis milliseid?
- Milliseid muudatusi oleks vaja sisse viia, et digitaalseid tõendeid paremini talletada?

Lähtudes püstitatud uurimiseesmärgist ja sellele tuginevatest uurimisküsimustest, teostati käesoleva lõputöö puhul kvalitatiivse uurimismeetodina intervjuude läbiviimine. Kuna lõputöö eesmärgiks oli selgitada digitaalsete tõendite talletamisega seonduvaid probleeme Põhja prefektuuri politseiametnike näitel, siis moodustati intervjuude valim nende tööga kokku puutuvate ja ülevaadet omavate prefektuuri kriminalistide (9 isikut) ja kriminaalasjade üle järelevalvet teostavate Põhja Ringkonnaprokuratuuri prokuröride ning prokuröri abide (10 isikut) ning Põhja Prefektuuri kriminaalbüroo igapäevaselt digitõenditega kokkupuutuvate uurijate (3 isikut) hulgast.
Peamiste digitõendite talletajatena sündmuskohal on politseiametnikud – menetlejad, uurijad – või siis eksperdid, kriminalistid kui neid kaasatakse (eriti oluliste sündmuste puhul). Vastavalt uurimustööle selgus, et eksperte kaasatakse menetlustesse suhteliselt vähe. Kindlalt paigas ei ole, millise protseduuri puhul kaasatakse eksperte, kuid siiski raskemate tõendite puhul seda tehakse.

Sündmuskohal digitaalseid tõendeid talletavad politseiametnikud ei ole prokuröride arvates, kes üldiselt talletamisega kokku ei puutu ning näevad peamiselt tulemusi, kuigi pädevad. Siiski arvavad nad, et pädevuse poolest on eksperdid väga pädevad. Miinusena tõid nad välja selle, et vastuse saamisega neilt läheb kauem aega kui tavaliste spetsialistide käest vastuse saamisega. Kriminalistide hinnangul on aga politseiametnikud pädevad, kuid kuna nende

hinnang võib olla mõjutatud piiratud omavahelisest koostööst (ainult 6 juhtumit aastas), siis puudub nende hinnangu andmiseks piisav tagasiside.

Digitõendite talletamise puuduste kohta selgus uurimustöös läbi viidud vastuseid analüüsides, et aeg-ajalt ikka esineb mingil määral puudusi – seda kas sündmuskohal talletades või siis juba talletatud tõenditega. Kuna peamiselt tegelevad sündmuskohal digitaalsete tõenditega politseiametnikud – uurijad, menetlejad, siis nende poolt tuleb ka kõige rohkem vigu. See on aga iseenesest loogiline – ei saa ju midagi valesti teha kui antud asjaga ei tegele. Samas tuli uurimustöö tulemusena välja ka see, et mõningad komplikatsioonid on tekkinud ka tehniliste viperuste tõttu. Kas siis näiteks ei ole mingit kuupäeva näha (msni vestlus) või ei saa antud asja üldse nii kasutadagi nagu tegelikult peaks saama.

Muudatuste läbiviimiste kohta selgus, et selle alaseid koolitusi on siiani suhteliselt vähe läbi viidud ning tuntakse et oleks rohkem antud teemalisi koolitusi juurde vaja. Samuti pole neid koolitusi ka väga palju tulemas. Kui mõni selleteemaline koolitus on tulemas, siis saab koolituse kohtade arv suhteliselt kiiresti täis. Käesoleva töö autori hinnangul sooviksid nii politseiametnikud, prokurörid kui ka uurijad osaleda koolitustel, mis hõlmab endas digitaalsete tõendite teemat – kuidas neid talletada, mismoodi neid säilitada ja palju muud. Seda eriti selle pärast, et elu areneb iga päevaga ning leitakse järjest uusi digitaalseid tõendeid või siis võimalusi mingisuguse tõendi talletamiseks. Me kõik soovime kursis olla kõige värskemate ja aktuaalsete teadmistega.

Kuna kriminaalstatistika alusel oli kirjas, et IT-kuritegude arv on tõusnud viimastel aastatel ligi 30%, siis leidis see fakt ka uurimustööd läbi viies kinnitust ning on kirjas teoreetilises osas.

Toetudes teoreetilisele osale, tuleb välja ka see, et digitaalsete tõendite olemus on suhteliselt keeruline. Nad on haprad, hävinevad kergelt ning neid on suhteliselt raske tõendamiskõlbulikena talletada kui ei ole eelnevaid teadmisi või kokkupuudet. See leidis ka uurimustööd tehes kinnitust. Raske on tõendeid õigesti talletada ka sellepärast, et neid viise, kuidas õigesti talletada on päris palju. Siiski on olemas mõned elementaarsed asjad, mida saab kasutada pea kõikide digitaalsete tõendite talletamisel ja käsitsemisel.

Toetudes uurimistulemuste analüüsile ja lõputöös käsitlevatele teooriatele, teeb autor järgmised ettepanekud:

- Viia läbi rohkem koolitusi antud valdkonnas kõikidele politseiametnikele, kes vähegi puutuvad oma igapäeva töös kokku digitaalsete tõenditega. Selle tulemusena oleks tõendite talletamine kiirem ja korralikum ning ei esineks puudusi. Muidugi võiks seda teha ka prokuröride hulgas – sest nemad teostavad ju menetluses järelevalvet.

- Digitõendite avastamine, talletamine ja uurimine peaks muutuma igapäevasemaks. Intervjuude tulemusena selgus, et päris paljudel kordadel jäetakse digitaalsed tõendid eksperdile saatmata pikkade järjekordade tõttu. Sellest tulenevalt võiks viia sisse järgmise punkti.
- Luua ja kaasata sündmuskohtadele antud teema spetsialiste – see muudaks menetluse tulemuste saamise kiiremaks. Näiteks kui oleks olemas spetsialistid antud valdkonnas ja nad sündmuskohaga kaasata, saaks digitõendite vastused poole kiiremini. Muidugi raskemate digitaalsete tõendite leidmise puhul oleks hea kaasata ekspert. See, et spetsialist teeks kergema töö ära, muudaks ekspertide töö ka palju lihtsamaks. Selle tõttu lüheneksid ka EKEI-s tõendite uurimiseks olevad järjekorrad.

SUMMARY

This present thesis contains 42 pages and 3 appendixes (6 pages). List of references consists of 17 items, of which 10 are in English and 7 in Estonian. The thesis is written in Estonian and summary is in English.

The goal of this work, above all, is to find out problems in collecting and storing digital evidences on scene by Northern Prefecture police officers.

To achieve the purpose of this work, following research questions were put up: 1) who are main digital evidence storers on the scene? 2) if the clerks, who collect digital evidences on the scene, are competent enough or not? 3) if any drawbacks/problems occur in storing digital evidences? If so, then which? 4) what kind of changes is needed to introduce, to make digital evidence storing better?

Based on the research questions, the study was conducted using interviews as a qualitative method. Interviews were carried out amongst 9 Northern Prefecture criminalists, 10 Northern district attorney generals and assistant attorney generals and 3 Northern Prefecture investigators.

Results of the study showed that the main digital evidence storers on the scene are police officers – investigators, or experts, criminalists when they are involved. As a result of the study it was found that there are some kind of drawbacks which are in storing digital evidences. These drawbacks are either collecting on the scene or with stored evidences. For the changes, that need to be done, it was found out that there haven't been hardly any schooling in the theme of digital evidence and also there aren't many to come too. In addition doing this research, it was found that digital evidence is complicated, they are fragile, easily destructible and they are quite hard to store right.

Based on the results of the study, three proposals were made that would help store digital evidence more correctly and efficiently.

VIIDATUD ALLIKATE LOETELU:

Kriminaalmenetluse seadustik, Vastu võetud 12.02.2003, RT I 2003, 27, 166, jõustumine 01.07.2004, https://www.riigiteataja.ee/akt/123022011045 – välja otsitud 1. aprill 2011

E. Kergandberg, T. Järvet, T. Ploom, O. Jaggo; *Kriminaalmenetlus, Teine, muudetud trükk;* Sisekaitseakadeemia, 2004, lk 22

United States Secret Service, *Best practices for seizing electronic evidence v.3 A pocket guide for first responders*, lk 3, 6, http://www.forwardedge2.com/pdf/bestpractices.pdf – välja otsitud 20. märts 2012

Keskkriminaalpolitsei, *Infotehnoloogiakuritegude menetlemise käsiraamat*, 2011, Phare mestiprojekt EE 03 IB JH 04, uuendatud JLS/2009/ISEC/AG/077, lk 7-9; 17-18; 42-45

IT-kuritegevus, http://ppa-siseveeb.polsise/kriminaalpolitsei/it-kuritegevus/index.dot – välja otsitud 26. Märts 2013

IT-kuriteod, https://www.politsei.ee/et/nouanded/it-kuriteod/ – välja otsitud 19. aprill 2013

Casey, E (2004*), Digital Evidence and Computer Crime, Second Edition*, lk 12

Casey, E *Handbook of Digital Forensics and Investigation*, Academic Press, välja antud 2 September 2010, lk 21, 567

ACPO Good Practice Guide for Computer-Based Evidence, ACPO. Välja antud 24 juuli 2010, lk 6

International Competition Network, *Anti-Cartel Enforcement Manual*, välja antud märts 2010, Chapter 3 lk 8

Digital Evidence, Harley Kozushko, 2003, lk 3, http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/DigitalEvidencePaper.pdf – välja otsitud 20. Märts 2012

Digital Evidence slideshow 2003, Harley Kozushko, lk 3-4, 19-28, http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Presentations/DigitalEvidence.pdf?bcsi_scan_123264D0DBEECA8E=0&bcsi_scan_filename=DigitalEvidence.pdf – välja otsitud 12. Aprill 2011

Casey, E, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 2000, lk 4-5

Keskkriminaalpolitsei, Tallinn 2005, *Infotehnoloogiakuritegude menetlemise käsiraamat versioon 1.0*, Phare mestiprojekt EE 03 IB JH 04, lk 12-15, 40, 45

U.S. Department of Justice, *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders*, välja antud november 2009, lk 5, 11-12, 37-38

Seizure of e-evidence, 2003

Infotehnoloogia ekspertiiside määramise juhend, EKEI, Pavel Laptev, uuendatud 11.08.2009

LISA 1. INTERVJUU KÜSIMUSED – KRIMINALISTID

Kui pikk on Teie tööstaaž?:

……...…

Kui kaua olete töötanud kriminalistina?:

.....

Kui tihti on erinevatel sündmuskohtadel kriminalistidel vaja digitaalseid tõendeid ja/või nende andmekandjaid talletada (võrreldes tavaliste tõenditega)?:

……...

Millega põhiliselt need sündmuskohad seotud on – mis juhtumid peamiselt?:

.....

Kas viimasel ajal on sagenenud digitaalsete tõendite talletamine sündmuskohal või on see pigem vähenenud? Mis põhjusel?:

……..

Kes peamiselt talletavad sündmuskohal digitaalseid tõendeid? Kas Teie, kui kriminalistid, või muudel ametikohtadel töötavad politseiametnikud?:

……...…

Kas teistel ametikohtadel töötavad politseiametnikud oskavad Teie arvates korrektselt talletada digitaalseid tõendeid?:

……..…

Kas on esinenud juhtumeid, kus mingisuguste eripärade tõttu on tõendite talletamisel esinenud probleeme?:

……...…

Kui mitu korda olete ebaõnnestunud digitaalsete tõendite ja/või andmekandjate talletamisel sündmuskohal? Kui olete, siis mis on põhjuseks olnud?:

.....

Kas Teie teada on olnud juhtumeid, kus teised politseiametnikud talletavad sündmuskohal digitaalsed tõendid ning hiljem siis tuleb välja, et need ei ole tõendamiskõlbulikud?:

.....

Mis on Teie arvates see peamine põhjus, miks mõningaid digitaalseid tõendeid ja/või nende andmekandjaid ei suudeta tõestamiskõlbulikena talletada? – näiteks kas teadmiste vähesus või tehnika puudulikkus?:

.....

Kas Teie hinnangul on piisavalt võimaldatud antud teema puhul Teile täienduskoolitusi või soovite neid veelgi?:

……...

LISA 2. INTERVJUU KÜSIMUSED – PROKURÖRID JA ABIPROKURÖRID

Millises osakonnas töötate?:

Kui kaua olete töötanud prokurörina ja millistes valdkondades? Kui kaua sellest olete juhtinud Põhja prefektuuri poolt menetletavaid kriminaalasju?:

Kui tihti puutute kokku juhtumitega (Põhja Prefektuuri), millistes on tõendeid saadud digitaalsetest allikatest (arvuti, kõvaketaste, mälukaartidega, jne)?:

Millist tüüpi juhtumid need peamiselt on?:

Kas digitaalsed tõendid on muutunud menetluses olulisemaks ja nende kogumine viimase 3-e aasta jooksul sagedasemaks või on need vähenenud? Mida arvate selle põhjuseks olevat?:

Kes on peamiselt Teie menetluses olnud/olevates kriminaalasjades digitaalsete tõendite talletajateks? Palun määrake nende osaluse ligikaudne protsentuaalne suurus (näiteks politseiametnikud 60% ja eksperdid 40%).

Palun hinnake enda kogemustele toetudes digitaalsete tõendite talletamise pädevust nii politseiametnike kui ka ekspertide poolt.:

Kas olete täheldanud digitaalsete tõendite talletamisel mingisuguseid puudusi?: Kui jah, siis milliseid puudusi olete digitaalsete tõendite talletamisel täheldanud (vormistamine, tehnilise võimekuse, teadmiste puudumine jne)?:

Kui olete täheldanud digitaalsete tõendite talletamisel puudusi, siis milliseid? Kelle poolt olid antud tõendid talletatud (mitte nimeliselt) ja millist kaalu need kriminaalmenetluses omasid?:

Kui olete seisukohal, et digitaalsete tõendite talletamine on problemaatiline, siis millised oleksid Teie seisukohalt selle parandamiseks vajalikud sammud?:

Kas Põhja Prefektuuri menetlejate tegevus digitaalsete tõendite talletamisel vastab Teie ootustele või oleks selles osas vajalik viia sisse mingisuguseid muudatusi (näiteks koolitused, rohkem suunata ekspertidele, vm)?:

LISA 3. INTERVJUU KÜSIMUSED – UURIJAD

Kui kaua olete töötanud uurijana? Kui kaua sellest ajast olete töötanud Põhja Prefektuuris?

Kui palju teate digitaalsete tõendite kohta ning kust olete oma teadmised saanud (koolitused, või muu)?:

Kui tihti puutute kokku juhtumitega (Põhja Prefektuuri), millistes on tõendeid saadud digitaalsetest allikatest (arvuti, kõvaketaste, mälukaartidega, jne)?:

Millist tüüpi juhtumid need peamiselt on?:

Kas digitaalsed tõendid on muutunud menetluses olulisemaks ja nende kogumine viimase 3-e aasta jooksul sagedasemaks või on need vähenenud? Mida arvate selle põhjuseks olevat?:

Kes on Teie arvates peamiselt digitaalsete tõendite talletajateks? Kas teie kui menetlejad või muud ametnikud (politseiametnikud, eksperdid)?:

Palun hinnake enda kogemustele toetudes digitaalsete tõendite talletamise pädevust nii politseiametnike kui ka ekspertide poolt.:

Kas olete täheldanud digitaalsete tõendite talletamisel mingisuguseid puudusi?: Kui jah, siis milliseid puudusi olete digitaalsete tõendite talletamisel täheldanud (vormistamine, tehnilise võimekuse, teadmiste puudumine jne)?:

Kui olete talletanud mingisuguseid puudusi digitaalsete tõendite talletamisel, siis kelle poolt olid antud tõendid talletatud (mitte nimeliselt) ja millist kaalu need kriminaalmenetluses omasid?:

Kas digitaalsete tõendite talletamine Põhja Prefektuuris on Teie arvates problemaatiline? Kui jah, siis millised oleksid Teie seisukohalt selle parandamiseks vajalikud sammud/muudatused?: