TARTU ÜLIKOOL

SOTSIAALTEADUSTE VALDKOND

ÕIGUSTEADUSKOND

Avaliku õiguse osakond

Gerd Raudsepp

DIGITAALSETE TÕENDITE KOGUMISE JA KASUTAMISE PERSPEKTIIVIKUS KRIMINAALMENETLUSES

Magistritöö

Juhendaja: *dr. iur.* Mario Rosentau

Tartu

2018

Sisukord

SISSEJUHATUS

Kaasaegne ühiskond sõltub üha enam erinevatest kommunikatsioonivõrgustikest, mobiilsetest seadmetest, asjade internetist ehk nutistust[1], küberfüüsikaliste süsteemide[2] tehnoloogiatest, pilvepõhistest süsteemidest ja paljust muust taolisest. Kasutades ära kõrgetasemelisi informatsiooni- ning tehnoloogiasaavutusi, on kommertsasutuste, ettevõtete vahelised tehingud ja valitsuste pakutavad teenused kasvanud sellisel määral, et muutnud on iga indiviidi elustiili ning -kvaliteet. Eeltoodud revolutsioonide ühendamine reaalse eluga toob kaasa hulganisti kasutegureid ja uusi võimalusi. Samal ajal tekitab infotehnoloogia areng üha uusi materiaal- ja menetlusõiguslikke ohte ning küberturvalisuse probleeme, nagu näiteks identiteedivargus, küberkiusamine, lekitatud andmete ärakasutamine või informatsiooni varjamine.[3]

Tuginedes infotehnoloogia kiirele arengule ning uute tehniliste võtete väljakujunemisele on äärmiselt oluline, et ka õiguslikud probleemid saaksid sellega seoses lahenduse. Kahtlemata tekib erinevate innovaatiliste lahenduste kujunemisel õiguslünki ning takistusi, mis on vaja ületada. Üheks eeltooduks on kindlasti digitaalse maailma arenemise korral digitaalsete jälgede ning tõendite väljakujunemine.

Tõendid, mis saadakse arvutitest, on kohtuvaidlustes olnud kasutusel sama kaua, kui inimesed on kasutanud arvutisüsteeme. Peamiselt on digitõendite kasutamine kohtumenetluses edukas, kus paljud kuriteod, sh mitte vaid küberkuriteod, on saanud lahenduse just tuginedes tõenditele, mis on talletatud digitaalselt või fikseeritud digitaalsest andmekandjast. Arvutitehnikud ja juristid on välja töötanud erinevaid tehnilisi võtteid, protokolle digitaalsete tõendite säilitamiseks, analüüsimiseks ning kasutamiseks kohtumenetluses.[4]

Digitaalkriminalistika käsitab digitaalsete tõendite kogumist ja analüüsimist eesmärgiga kasutada neid tõenditena nii tsiviil-, haldus- kui ka kriminaalasjades.[5] Digitaalkriminalistika

[1] Lühidalt öeldes on asjade internet omavahel ühendatud internetiühendusega seadmete võrk, milles olevad seadmed jagavad ja vahetavad informatsiooni kasutajale, üksteisele ning täidavad koos teatud ülesandeid. Allikas: https://www.am.ee/node/5287

[2] Küberfüüsikalised süstesteemid on süsteemid, mis seovad läbi infotöötluse füüsilist maailma virtuaalse maailmaga. Allikas: http://kfst.ee/korduma-kippuvad-kusimused/

[3] L. Caviglione, S. Wendzel, W. Mazurzcyk. The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security & Privacy (V: 15, Issue: 6), November/December 2017. IEE, 2017, lk 12.

[4] P. Sommer. Emerging Problems in Digital Evidence. Presentation to Criminal Bar Association, 2007. Ettekande lühikokkuvõte.

[5] B. Nelson, A. Phillips, C. Steuart. Guide to Computer Forensics and Investigations. Third edition. Cengage Learning, 2014, lk 2

mängib üha enam rolli ka tsiviilkohtumenetluse puhul, intellektuaalomandi vaidlustes, töövaidlustes ning infotehnoloogia turvalisuse intsidentide puhul.[6]

K. Palm on enda 2013. a. uurimistöös „Digitaalsed tõendid ja nende talletamine Põhja Prefektuuri näitel" analüüsinud digitaalsete tõendite osakaalu tõusu viimastel aastatel. Võttes aluseks informatsiooni inimestelt, kes digitõenditega igapäevases töös kokku puutuvad. Uurimisvalimisse kuulusid kriminalistid, kellest 55% hinnangul on digitaalsete tõendite osakaal kriminaalmenetluses kasvanud,[7] ning prokurörid, kellest 70% leidsid, et digitõendeid on varasemaga võrreldes kriminaalmenetluses kasutusel rohkem.[8] Olgugi, et uurimistöös oli valim üsnagi väike ning hõlmas vaid väikest osa Eesti uurijatest ning prokuröridest, näitab uurimistöö tulemus, et digitaalsete tõendite kasutus kasvab iga aastaga.

Tuginedes eeltoodule, on oluline sätestada või kohandada seadusandlus vastamaks infotehnoloogia valdkonnas toimuvatele muudatustele. Digitaalsed tõendid on oma olemuselt ning omadustelt füüsilistest tõenditest erinevad. Seetõttu on küsitav, kas digitõendite kogumisele, säilitamisele ning analüüsimisele on võimalik rakendada kõik kriminaalmenetluse seadustiku sätteid, tõlgendusi ning põhimõtteid. Teisalt kerkib probleem, kas digitõendite kogumine, analüüsimine, säilitamine ja kohtumenetluses kasutamine on kehtiva seadustiku raames üleüldse võimalik.

Nagu varem mainitud, leidub digitaalseid tõendeid kõikjal meie ümber. Põhimõtteliselt iga indiviid omab mingit tehnikaseadet, mis on võimalik talletama, edastama või vastu võtma informatsiooni, mis võib uurimises omandada digitaalse tõendi väärtuse. Eeltoodud protsess toimub pahatihti inimese enda teadmata. Tähtis on välja tuua, et igasugune teave või informatsioon iseenesest ei ole digitõend. Tõendi väärtuse omandab informatsioon juhul, kui see on kogutud vastavalt seaduses sätestatud menetlusreeglitele ning informatsioon omab kriminaalmenetluses tõendavat väärtust, lükkab ümber või kinnitab kuriteo kriitilist elementi. Lisaks võib digitõendid sisaldada teavet kuriteo tehiolude kohta, tuvastamaks kurjategija motiivi, kuriteo toimepanemise kohta või muid olulisi asjaolusid.

Digitaalsed tõendid võivad väljenduda erinevates vormides ning tuleneda erinevatest allikatest. Tõendiks võib olla nii digitaalne pilt, e-kiri kui ka arvutisüsteemist tuletatav

[6] R. McKemmish. When is Digital Evidence Forensically Sound?. In: Ray I., Shenoi S. (eds) Advances in Digital Forensics IV. DigitalForensics 2008. IFIP — The International Federation for Information Processing, vol 285. Springer, Boston, MA, 2008, lk 3-4.
[7] K. Palm. Digitaalsed tõendid ja nende talletamine Põhja Prefektuuri näitel. Lõputöö, Sisekaitseakadeemia, Politsei- ja Piirivalvekolledž. 2013, Lk 24-25.
[8] Samas, lk 28-29.

logifail. Sõltuvalt tõendi liigist võib olla erinev nii tõendi omandamise viis kui ka selle analüüsimise protsess.

Käesolevas magistritöös analüüsin digitaalsete tõendite kogumist ning kasutamist kriminaalmenetluse raames, kuivõrd kriminaalmenetlus on isikute põhiõiguste riive suhtes kõige intensiivsem ning tulenevalt süütuse presumptsioonist ei ole keegi kohustatud tõendama enda süütust. Isikut süüdistavate tõendite kogumise kohustus lasub Eesti Vabariigil ning kedagi ei käsitata kuriteos süüdi olevana enne, kui tema kohta on jõustunud süüdimõistev kohtuotsus. Tuginedes sellele on uurijatel ning prokuröridel kohustus viia kriminaalmenetluses kohtueelne uurimine läbi äärmiselt põhjalikult, kaalutledes iga tõendi põhjapidavust, usaldusväärsust ning kooskõla menetlusnormidega.

Kahtlemata omab digitaalsete tõendite regulatsioon suurt tähendust ka muude kohtumenetluse liikide puhul, ent autori hinnangul on digitaalsete tõendite kasutamise problemaatika praktikas enimlevinum eelkõige kriminaalmenetluse puhul. Viimane baseerub kohtumenetluse liikidest tulenevatel eripäradel, kriminaalmenetluse eesmärgiks on koguda tõendeid eesmärgiga mõista isik süüdi. See paneb raskuspunkti uurimisasutustele ning prokuratuurile. Tsiviilkohtumenetluses lasub reeglina tõendite esitamise kohustus osapooltel endil, mis tähendab, et kohtuasjas vajalikku ning relevantset informatsiooni on kohustatud koguma kohtuvaidluse osapooled ja tõendi lubatavause regulatsioon erinev oluliselt kriminaalmenetluse sätetest.

Digitaalsete tõendite kogumise, analüüsimise ja kasutamise protsessi saab tinglikult jagada kaheks. Esmalt, uurijad, kes tegelevad kuriteo menetlemisega, peavad välja selgitama, millised tõendid on kuriteo aspektist tähtsad ning vajalikult. Teiseks, kohtuekspertiis või uurimisasutus peab läbi viima reeglitekohased analüüsid, mille tulemusena omandaks leitud informatsioon ning analüüsi tulemus tõendusväärse perspektiivi ehk tõend fikseeritakse. Digitõendi fikseerimiseks on tarvis järgida seaduses sätestatud menetlusreegleid.

Digitaalse uurimist läbiviiv uurija mängib uurimisprotsessis fundamentaalset osa, juhtides selleks süüdistatava või kahtlusaluse personaalarvuti, mobiiltelefoni või tahvelarvuti digitaalkriminalistikalist analüüsi või internetiliikluse tuvastamist ja analüüsimist küberkaitse vastaste juhtumite korral.[9]

[9] R. McKemmish. When is Digital Evidence Forensically Sound?. In: Ray I., Shenoi S. (eds) Advances in Digital Forensics IV. DigitalForensics 2008. IFIP — The International Federation for Information Processing, vol 285. Springer, Boston, MA, 2008, lk 3-4.

Digitaalsete tõendite korral on võimalik tuua välja kaks peamist probleemset valdkonda, esiteks, uurimisasutuste tehnilised kitsendused ning takistused, ja teisalt digitaalsete tõendite lubatavuse ja kogumise problemaatika tuginedes kriminaalmenetluse seadustikule. Käesolev magistritöö ei käsitle kõiki, vaid olulisemaid digitõendite tehnilisi probleeme.

Kriminaalmenetluses võib digitaalsete tõendite kogumine olla äärmiselt kompleksne ning keeruline, tuginedes peamiselt tõendite immateriaalsetele ning kergesti muudetavale olemusele, eriti metaandmetest tulenevatest tõendite analüüsimise korral. Tehnoloogia muudab uurimisprotsessi ning tõendite salvestamise äärmiselt kaitsetuks eksimuste, tehniliste talitlushäirete ning tõendite fabrikatsiooni ees.[10] Eeltoodud aspektid võivad hõlpsasti põhjustada tõendite mittelubatavuse kohtus, mistõttu on digitõendite kogumise ning analüüsimise käigus oluline teadvustada ning ületada tehnilisi komistuskivisid.

Uurimisprotsessi läbiviimisele ning tõendite kogumisele järgneb kriminaalmenetlus kohtus, mis mh sisaldab kogutud ja analüüsitud tõendite esitamist ning kohtu veenmist tõendite usaldusväärsuses. Prokuratuur esitab tõendid eesmärgiga täita tõendamise kvalitatiivne norm ehk veenda kohut mingi asjaolu ilmnemisest väljaspool mõistlikku kahtlust.[11] Juhul, kui digitaalsete tõendite esitamisel kohtus pole järgitud seadusest tulenevaid menetlussätteid, võib tõend olla kohtumenetluses lubamatu.

Käesoleva töö eesmärgiks on analüüsida, kas digitaalsete tõendite kasutamine kohtumenetluses on perspektiivikas ning kas kehtiv digitaalsete tõendite kogumise, analüüsimise ning kasutamise reeglistik arvestab digitõendite unikaalseteid omadusi. Eeltoodu sisustamiseks on muuhulgas vajalik välja tuua digitõendite mõiste nii kodumaises kui ka välismaises õiguskirjanduses. Oluline on sätestada erinevate digitaalsete tõendite liikide omapärad, erisused ja kogumise meetodid tuginedes kriminaalmenetluse seadustikule.

Töö hüpoteesiks on, et kriminaalmenetluses on digitaalsete tõendite kasutamine kehtiva seadusandluse kohaselt perspektiivikas, st kehtiva seadusandluse kohaselt on digitõendite kasutamine lubatud ning nende kogumine kriminaalmenetluse seadustiku kohaselt reguleeritud.

Magistritöö kirjutamisel olen kasutanud võrdlevat ja analüütilist uurimismeetodit. Töös võrdleb autor kehtivat seadusandlust sellega, mida näevad ette rahvusvahelised ning Eestile siduvad välislepingud ja kas Eesti siseriiklik seadusandlus on kooskõlas välislepingus sätestatuga. Töö peamine eesmärk on analüüsida, kas kehtiv seadusandlus võimaldab

[10] C. Reed. Computer Law, Seventh Edition. Oxford University Press. 2008, lk 715.
[11] Samas, lk 717.

digitaalseid tõendeid kriminaalmenetluses kasutada ja kas kriminaalmenetluse seadustikus esineb digitõendite kasutamise suhtes olulisi lünki või puudusi. Täiendavalt, esitab autor enda poolsed võimalused täiendamaks kriminaalmenetluse seadustiku digitõendite regulatsiooni.

Töö on strukturaalselt jaotatud neljaks peatükiks. Esimeses peatükis toon välja digitaalsete tõendite mõiste ning omadused tuginedes välismaistele ning kodumaistele kirjandusallikatele. Täiendavalt, nagu eelnevalt mainitud, esineb mitmeid allikaid, millest on võimalik digitaalseid tõendeid koguda. Peatükis on samuti välja toodud kategooriatena seadmete liigid, millest on võimalik digitaalseid tõendeid koguda.

Teine peatükk keskendub digitaalkriminalistikale kui teadusharule, mis tegeleb digitaalsete tõendite kogumise, säilitamise ja analüüsimisega. Igal teadusharul on sätestatud põhiprintsiibid, millest tuleb uurimise läbiviimise kestel juhinduda. Autor toob välja digitaalkriminalistika peamised printsiibid, millest digitaalkriminalistid igapäevases töös johinduvad ning mis on leidnud rahvusvahelist tunnustust. Saamaks paremat arusaama digitaalkriminalistika töö olemusest, uurib autor teadusharu mudelit ehk tööplaani ning vahendeid, mille abil on võimalik tõendite analüüsimist läbi viia. Täiendavalt toob autor välja digitaalkriminalistika arengu ning rolli Eestis tuginedes seadusandlusele ning kirjandusele. Peatüki viimane osa käsitleb digitaalkriminalistika tehnilisi probleeme, mh fabritseeritud tõendite mõistet, nende loomise viise ning võltstõendite tuvastamise metoodikat.

Kolmandas peatükis toob autor individuaalselt välja kõige levinumad digitaalsete tõendite liigid ning millised on leiduvatest tõenditest tuletatavad tõenduslikku väärtust omavad osad. Kuivõrd digitaalseid tõendeid on võimalik omandada igast digitaalse meedia hoiustamist, edastamist või vastuvõtmist võimaldavast seadmest, on peatükk jaotatud erinevateks alapeatükkideks. Liigituse aluseks on digitõendite olemus, mille alusel on võimalik eristada digitaalsetelt andmekandjatelt tuletatavaid andmeid ning metaandmeid, mida on võimalik omandada arvutisüsteemidest ning internetist.

Neljas peatükk keskendub digitaalsete tõendite kasutamisele kohtumenetluses ehk magistritöö hüpoteesi analüüsimisele. Eelkõige tuleb kõne alla digitaalsete tõendite klassifitseerimine Eesti seadusandluse raames kriminaalmenetluse seadustikus sätestatud tõendi definitsiooni raames. Viimane tähendab sisuliselt tõendi lubatavust kriminaalmenetluses. Täiendavalt, tulenevalt digitaalsete tõendite omaduste eripärast, on vajalik analüüsida, kas tõendite kogumisele on kriminaalmenetluse seadustikus sätestatud regulatsioon, mis üleüldse sätestab meetodid digitõendite kogumiseks. Teisalt tuleks tulevikus sätestada, kas kehtiv regulatsioon arvestab digitõendite unikaalsest iseloomust tulenevaid eripärasid.

Magistritööd kõige enam iseloomustavad märksõnad on: digitaalsed tõendid, digitaalkriminalistika, kriminaalmenetlus, infotehnoloogia ja tõendamine.

1. DIGITAALSED TÕENDID

1.1. DIGITAALSE TÕENDI OLEMUS

Digitaalne tõend on defineeritud kui igasugune informatsioon, mis on talletatud või edastatud arvuti abil, mille eesmärk on tõendada või ümber lükata teooria sellest, kuidas kuritegu toimus. Digitõendid võivad sisaldada informatsiooni kuriteo kriitiliste koosseisuliste asjaolude ja tehiolude, näiteks motiivi või alibi kohta.[12] Eeltoodud definitsiooni all võivad kõne alla tulla nii dokumentaalsed tõendid, video-, audio- või fototõendid kui ka digitaalsetest andmekandjatest leiduvad metaandmed.

Alternatiivse lähenemise kohaselt on võimalik digitaalset tõendid defineerida kui igasugust tõendamisväärtust omavat informatsiooni, mis on talletatud või edastatud digitaalselt ning kohtuvaidluse osapoolel või kohtul on õigus eeltoodud tõendit kasutada kohtumenetluse käigus. E-mailid, digitaalsed fotod, elektroonilised dokumendid, vestluste ajalood, internetilehitsejate ajalood, andmebaasides leiduv informatsioon, ajutistest failidest ja varukoopiatest tulenev teave, võivad osutuda kohtumenetluse käigus määrava tähtsusega tõenditeks. Eeltoodud jäljed ning digitõendid on kõikjal meie ümber, immateriaalsed ja implitsiitsed, paljudel juhtudel isik, kes jälje lõi, ei ole teadlik selle jälje loomisest.[13]

Autori hinnangul omab viimasena käsitletud digitaalse tõendi definitsioon paremat vastet praktilistele vajadustele. Kuivõrd ühiskond ja tehnoloogia areneb ning muutub ajas kiire tempoga, tuleb digitaalsed tõendid defineerida võimalikult kitsalt, ent samas piisavalt laiahaardeliselt, et hõlmata kõikvõimalikud tulevikus tekkivad tõendite liigid. Samal ajal on oluline, et definitsioon ei oleks niivõrd laiahaardeline, et see kaotaks oma sisu. Eeltoodu all pean silmas seda, et kasutades sõnastust „igasugune tõendamisväärtust omav informatsioon mis on talletatud või edastatud digitaalselt“, hõlmab sisuliselt ka tulevikus tekkida võivaid digitaalsete tõendite liike. Näiteks, kui tulevikus tekib mingi uus digitaalse meediaseadme liik, hõlmab eeltoodud mõiste iseenesest ka seda. Sellegipoolest ei ole digitõendi definitsioon niivõrd laialivalguv, et see kaotaks enda mõtte.

Eeltoodud digitaalse tõendi mõiste on vaid abistav, mitte siduv. Tuginedes asjaolule, et kriminaalmenetluse seadustik ei defineeri digitaalse tõendi mõistet, ei ole seadusandja poolt

[12] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 7

[13] A. Castiglione, G. Cattaneo, G. De Maio, A. De Santis, G. Costabile and M. Epifani. The Forensic Analysis of a False Digital Alibi. 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Palermo, 2012, lk 114

loodud siduvat mõistet digitaalsete tõendite kvalifitseerimiseks. Kriminaalmenetluses sätestatud tõendi mõiste ei erista füüsilist ega digitõendit, mistõttu saab peatükis käsitletud digitaalse tõendi mõistet kasutada vaid informatiivselt, saamaks paremat arusaama digitõendite olemusest ning omadustest.

Üldiselt seostatakse digitaalseid tõendeid eelkõige kriminaalmenetlusega, peamiselt küberkuritegudega nagu näiteks krediitkaardipettus, digitaalne lapspornograafia levitamine ja loomine. Digitaalseid tõendeid on võimalik kasutada ka muude karistusseadustiku eriosas sätestatud koosseisude või tehiolude tõendamiseks ning tsiviil- või halduskohtumenetluses tähtsust omavate asjaolude, nõuete või vastuväidete tõendamiseks. Näiteks kurjategija e-postkast või mobiiltelefon võib sisaldada informatsiooni selle kohta, milline oli tema motiiv tapmise puhul või edastada uurijale informatsiooni kuriteo kriitiliste asjaolude kohta, nagu näiteks kuriteo kellaaeg, kuriteo toimepanemise koht jne. Teisalt võib arvelduskonto väljavõte tõendada, et kostja on tegelikult enda kohustuse hageja ees täitnud ning hageja hagil tsiviilkohtumenetluses puudub alus.

Kriminaalmenetluse seadustiku [14] (edaspidi KrMS) § 63 lõike 1 kohaselt on tõend kahtlustatava, kannatanu, tunnistaja või asjatundja ütlus, ekspertiisiakt, eksperdi antud ütlus, ekspertiisiakti selgitamisel, asitõend, uurimistoimingu, kohtuistungi ja jälitustoimingu protokoll või videosalvestis, samuti muu dokument ning foto või film või muu teabetalletus.

Digitaalsete tõendite kvalifitseerimine KrMS § 63 lg 1 alusel tekitab praktikas tihtipeale segadust, eelkõige aspektist, kas digitaalne tõend on asitõend, muu dokument või muu teabetalletus. Lisaks sellele võib olla problemaatiline teatud spetsiifiliste ja praktikas harva vahetult kasutatavate tõendi vormide lugemine tõendiks KrMS § 63 lg 1 järgi - nimelt näivad antud normis loetletud relevantsed tõendi liigid ehk asitõend, muu dokument ja muu teabetalletus osutavat eelkõige mingisugusele andmekandjale salvestatud (ingl. k. *stored*) teabele, samal ajal kui tõendusteavet võib omada ka erinevate seadmete vahel liikuv (ingl. k. *transmitted*) digitaalne teave, mida kogutakse reaalajas.[15] Digitõenditena tulevad kõne alla eelkõige isiku meediaseadmetest või internetist tuletatav metateave.

Kontseptsuaalselt on digitaalsed tõendid sarnased teiste füüsiliste tõenditega – tegemist on informatsiooniga võimaldamaks uurijatel siduda omavahel kuriteo tehiolusid ehk inimesi ja sündmusi aja ning kohaga, loomaks kuritegudele kausaalse olemuse. Sellest olenemata, on

[14] Kriminaalmenetluse seadustik – RT I, 05.12.2017, 8
[15] J. Tehver. Digitaalsete tõendite kasutamise võimaldamine. 2016, lk 2. Arvutivõrgus kättesaadav: https://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf

digitaalsed tõendid laiahaardelisemad, sisaldades personaalsemaid isikuandmeid ning vajades spetsiaalset väljaõpet ning töövahendeid.[16] Sisuliselt omavad digitaalsed tõendid võrreldes füüsiliste tõenditega rohkem tõenduslikku väärtust, võttes arvesse lisaks andmetele leitavad metaandmed.[17]

Omadustelt on digitaalsed tõendid peidetud, latentsed (sarnaselt DNA-le või sõrmejälgedele), lihtsasti muudetavad, manipuleeritavad ning hävitatavad ja ülitundlikud ajalistele faktoritele.[18]

Tehnoloogia kiire areng, meediakandjatel hoiustatavate digitaalsete andmete haavatavus ning immateriaalne iseloom muudavad digitaalsed tõendid äärmiselt kaitsetuks tehnilistele eksimustele, juhuslikule muutmisele, kahjulikele sekkumistele ning fabrikatsioonile. Tehnilised takistused kombineeritud õiguslike probleemidega võivad lõppastmes põhjustada digitaalse tõendi mittelubatavuse. Isegi juhul, kui digitaalne tõend on kohtumenetluses lubatud, võib tehniliste eksimuste esinemine mõjutada selle mõjukust.[19]

Digitaalsete tõendite loojat on enamasti väga raske identifitseerida. Täpsemalt öeldes, on võimalik jälgida, kes on loodud tõendi allika omanik, ent digitaalne tõend iseenesest ei sisalda informatsiooni selle kohta, kes või mis on selle loonud.[20] Juhul, kui digitaalsed andmed esinevad vormis, mis sisaldavad individuaalseid tunnuseid, nt e-kirja saatja või vastuvõtja nimi, kõnesalvestis, digiallkiri tekstifailil jne, on võimalik digitaalne tõend siduda konkreetse isikuga.[21]

1.2. DIGITAALSETE TÕENDITE ALLIKAD

Arvutid ja muud tehnikavahendid on tänapäeva ühiskonnas üldlevinud ning kõigile kättesaadavad. Digitaalseid andmeid luuakse, levitatakse, töödeldakse ja kustutatakse igapäevaselt, tihtipeale inimese enda teadmata.

[16] S. E. Goodison, R. C. Davis, B. A. Jackson. Digital Evidence and the U.S. Criminal Justice System. Identifying Technology and other Needs to more efficiently acquire and utilize Digital Evidence. National Institute of Justice. 2015, lk 3
[17] S. Saleem. Protecting the Integrity of Digital Evidence and Basic Human Rights during the Process of Digital Forensics. Stockholm University. 2015, lk 22.
[18] M. B. Mukasey, J. L. Sedwick, D. W. Hagy. Eletctronic Crime Scene investigation: A Guide for first responders, Second edition. U.S. Department of Justice Office of Justice Programs. 2008, lk IX.
[19] G. Peterson, S. Shenoi. Advances in Digital Forensics XIII. Springer. Orlando, FL, USA. 2017, lk 25.
[20] A. De Santis, A. Castiglione, G. Cattaneo, G. De Maio, M. Ianulardo. Automated Construction of a False Digital Alibi. Springer, Berlin, Heidelberg. 2011, lk 2.
[21] P. Gladyshev,. Formalising Event Reconstruction in Digital Investigations. Doktoritöö, Department of Computer Science, University College Dublin. 2004, lk 16.

Digitaalseid tõendeid võib leida igal pool ja ajahetkel, näiteks inimese personaalne meiliboks salvestab iga külastuse, saadetud või vastuvõetud e-kirja, saatmata e-kirja projekti ja mõningatel juhtudel kustutatud e-kirju. Digitaalseid tõendeid leidub ka erinevates igapäevaelus kasutatavates seadmetes, näiteks mobiiltelefonides, sülearvutites, digitaalkaamera mälukaartides jne.

Alljärgnevad digitaalsete allikate liigid hõlmavad peamisi digitaalsete tõendite allikad. Tulenevalt digitaalsete tõendite allikate üldomadustest on võimalik välja tuua kolm peamist digitaalsete tõendite allikat – avatud arvutisüsteemid, kommunikatsioonisüsteemid ja sisseehitatud arvutisüsteemidega seadmed.

1.2.1. Avatud arvutisüsteemid

Üldsusele on avatud arvutisüsteem (ingl. k *open computer systems)* tuntud kui arvuti ehk süsteemikogum, mis koosneb kõvakettast, klaviatuurist, monitorist ja võrguühendusest. P on sellisteks võrku ühendatud sülearvutid, lauaarvutid ja serverisüsteemid. Eeltoodud süsteemid oma talletamisvõimega võivad olla rohkete digitaaltõendite allikaks. Harilik arvutifail võib sisaldada süüstavat informatsiooni või omada siduvat teavet, mis võib kuriteo uurimisel kriitilise tähtsusega olla. Informatsioon selle kohta, kuna fail loodi, kes on tõenäoliselt loodud faili autor või kas fail on loodud mõne teise arvutisüsteemi kaudu, on digitaalkriminalistika aspektist ning kuriteo uurimisel tähtis teave.[22]

Uppsala Ülikooli õigusteadlased leiavad, et arvutite rolli kuritegude toimepanemisel on võimalik liigitada järgnevatel alustel[23]:

- Arvuti kui kuritegeliku käitumise vili. Paljud inimesed omandavad ja kasutavad tarkvara ilma tarkvaratootjate loata. Sellisel juhul on arvuti ise, täpsemalt öeldes, konkreetne programm, mida illegaalselt andmekandjal hoiustatakse või arvutisse installeeritakse, õigusrikkumise tulemus;
- Kuriteo toimepanemise vahend. Näiteks võib kurjategija kasutada arvutit selleks, et viia läbi küberrünnak teise arvuti või internetis leiduva veebilehe vastu. Lisaks eeltoodule on arvuti kuriteo toimepanemise vahendiks ka juhul, kui kurjategija kasutab arvuti printerit inimröövi lunarahakirjade või valeraha printimiseks;

[22] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 7.
[23] L.Qian, F. Höglin, P. A. Diaz. Computer Forensics. Uppsala University, 2007, lk 3.

- Vahend, mida kasutatakse kuriteo toimepanemisel juhuslikult. Kuivõrd arvutit ning muid digitaalse meedia seadmeid kasutavad igapäevaselt peaaegu kõik inimesed, võib esineda olukord, kus kurjategijad kasutavad arvutit kuriteo toimepanemisel iseenesele teadmata või kogemata, nt salvestades kogu kirjavahetuse kaastoimepanijatega;
- Vahendina kuriteo toimepanemiseks kui andmekandjana ladustamaks digitaalseid andmeid. Kõne alla tuleb näiteks olukord, mil küberkurjategija kasutab arvutit mingi küberründe läbiviimiseks ning hoiustab omandatud informatsiooni enda kõvakettale, mida ta hiljem kaastoimepanijatega jagab.

Tuginedes eeltoodule võivad arvutisüsteemid olla nii kuriteo toimepanemise otsesed vahendid kui ka sisaldada tõendeid kuriteo asjaolude, sh koosseisu ning tehiolude kohta.

1.2.2. Kommunikatsioonisüsteemid

Eelkõige peetakse kommunikatsioonisüsteemide (ingl. k *communication system)* all silmas traditsioonilisi telefonisüsteeme, juhtmevabu telekommunikatsioonisüsteeme ja internetti tervikuna. Näiteks võib telekommunikatsioonisüsteemide abil edastada SMS/MMS sõnumeid, interneti vahendusel e-kirju jne.[24]

Digitaaltõendeid võib leida näiteks teabes selle kohta, millal sõnum saadeti, kes selle saatis või milline informatsioon seisnes saadetud sõnumis, sh manuste olemasolu ja nende sisu. Selleks, et saada informatsiooni selle kohta, millal on sõnum saadetud, tuleb analüüsida vahendusserveritest ja ruuteritest, omandatud logifaile. Mõningad arenenumad kommunikatsioonisüsteemid on võimelised salvestama kogu sõnumi sisu, sh sõnumi teksti ning lisad, telefonivestlused jne.[25]

1.2.3. Sisseehitatud arvutisüsteemidega seadmed

Seadmed, millesse on sisseehitatud arvutisüsteemid (ingl. k *embedded computer systems*), hõlmavad endas mobiiliseadmeid, kiibikaarte ja teisi süsteeme, mis võivad digitaalseid

[24] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 8.
[25] Samas, lk 8.

tõendeid sisaldada. Mobiiliseadmetes võib leida digitaalseid fotosid, videosid, vestlusi, mis on saadetud sõnumitena või sotsiaalvõrgustike vahendusel, kui ka muud personaalset teavet, näiteks informatsiooni, mida hoiustavad mobiilirakendused, nt isiku kalender. Navigatsioonisüsteemide abil on võimalik määrata kindlaks sõiduki trajektoor või asukoht. Autodesse sisseehitatud tajumis- ning diagnostikamoodulid võivad säilitada informatsiooni selle kohta, milline võis mingil ajahetkel olla sõiduki kiirus või pidurite seisukord. Ka paljudel tänapäevastel kodutehnikavahenditel, näiteks mikrolaineahjudel, on sisseehitatud arvutisüsteemid, mis laevad internetist informatsiooni ning talletavad seda. Näiteks on teada juhtum, mil süütamise kaasuse uurimisel selgus, et põlengu põhjustas mikrolaineahi, mis oli programmeeritud kindlaks määratud ajal vallandama tulekahju.[26]

Seega võib tänapäevases infoühiskonnas digitaalseid tõendeid leida igal kõikjal, kus liigub digiandmeid. Isegi igapäevases kasutuses olevad seadeldised nagu näiteks mikrolaineahi või mobiiltelefon, võivad sisaldada digitaalseid tõendeid. [27]

[26] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 8.
[27] Samas, lk 8.

2. DIGITAALKRIMINALISTIKA

Digitaalkriminalistika on teaduslikult tuletatud ning tõestatud meetodite kasutamine digitaalsete tõendite allikast omandatud tõendite säilitamiseks, kogumiseks, valideerimiseks, tuvastamiseks, analüüsimiseks, tõlgendamiseks, dokumenteerimiseks ja esitamiseks eesmärgiga aidata kaasa või toetada kuritegelike sündmuste asjaolude rekonstrueerimist või aidata ennetada kuritegude toimepanemist.[28]

Digitaalkriminalistika kui eriala ning teadusliku distsipliini juured ulatuvad 1980-ndatesse, mil õiguskaitseasutused pidid kiiresti reageerima arvutialaste kuritegevuste kiirele tõusule.[29] Teadusharu eesmärk ei ole mitte tõendada isiku süüd või süütust, vaid esitada usaldusväärset tõendusmaterjali täielike ning osaliste tõendusmaterjalide tõlgendamise kohta.[30]

Vastuoluks leitakse, et üks esimesi digitaalkriminalistika juhtumeid leidis aset 1970ndatel. Juhtum kujutas endast olukorda, mil kaks kohalikku andmete taastamise eksperti töötasid üle 70 tunni selleks, et taastada ainsat koopiat andmesüsteemist, mille hooletu uurija kogemata kustutas.[31]

Digitaalkriminalistika algusaegadel oli teadusharu peamisteks tunnusteks riistvara, tarkvara ja rakenduste primitiivsus, andmefailide kustutamise tõkestamine ning ametlike menetlusreeglite, töövahendite ning erialase väljaõppe puudumine.[32]

Õiguskaitse seisukohast argumenteeritakse, et digitaalkriminalistika kui teadusdistsipliini tekkepõhjuseks oli vajadus luua tehniline lahendus õiguslikule probleemile.[33] Tehniline lahendus hõlmab elektrooniliste andmete ekstraheerimist algallikatest järgides menetlusreegleid, veendumaks, et fikseeritud informatsioon on kohtumenetluses tõendina aktsepteeritav.[34]

[28] Collective work of all DFRWS attendees. A Road Map for Digital Forensic Research. DFRWS. Utica, New York, USA, 2001, lk 16.
[29] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 10.
[30] A. Varol, Y. Ü. Sönmez. Review of Evidence Analysis and Reporting Phases in Digital Forenscics Process. IEEE, Türgi, 2017, lk 923.
[31] S. Garfinkel. Digital Forensics Research: The Next 10 Years. DFRWS 2010 USA, Portland, lk 65.
[32] Samas, lk 65-66.
[33] P. Craiger, M. Pollitt, J. Swauger. Law enforcement and digital evidence. Handbook of Information Security, Volume 2, H. Bidgoli (Ed.), John Wiley, New York, pp. 739–777, 2006, lk 743.
[34] D. Ryan, G. Shpantzer. Legal aspects of Digital Forensics. The George Washington University. Washington, D.C., USA. 2002, lk 2.

Tänapäeval on võimalik digitaalkriminalistika abil uurida erinevaid juhtumeid, alustades andmete taastamisest kuni küberrünnakute rekonstrueerimiseni.[35]

Digitaalkriminalistika on puhul on võimalik välja tuua peamised tegevusvaldkonnad, milleks on andmete taastamine, andmete hävitamise tuvastamine, krüpteerimine, dekrüpteerimine, peidetud andmete leidmine, IP-aadresside abil kurjategijate tuvastamine jne.[36]

Teadusharu peamiseks ülesandeks on fikseerida digitaalseid tõendeid, mis on nii otseselt kui kaudselt omandatud digitaalsest meediast. Selleks, et mõista digitaalkriminalistika eesmärki, on esmalt vajalik teadvustada arvutite ning muude meediavahendite roll kuritegude toimepanemisel.[37] Digitaalsete tõendite otsene kogumine seisneb eelkõige mingil andmeid säilitaval seadmel leiduva materjali fikseerimises ja kasutamises kohtumenetluses tõendina. Kaudne andmete omandamine kujutab endas erinevate metaandmete, süsteemi- või logifailide, analüüsimise käigus fikseeritud informatsiooni kasutamist kuriteo tehiolude tõendamiseks dokumenteeritud vormis.

Tuginedes eeltoodule on digitaalkriminalistika peamisteks ülesanneteks hankida nii otsest kui kaudset tõendusmaterjali, mida on võimalik leida arvutitest või muudest digitaalsetest allikatest. Tegemist on sisuliselt sarnase protsessiga füüsiliste tõendite omandamisele, mil uurijad koguvad materiaalseid tõendeid toimepandud kuritegude koosseisu ning tehiolude kohta. Teisest aspektist on digitaalkriminalistika eesmärk koguda tõendeid, mis ei ole sarnased füüsilistele tõenditele. Esmalt tulevad kõne alla tõendid, mida on võimalik omandada teatud digitaalse meedia vahendusel erinevate analüüside ning uuringute teostamise teel. Teisalt tõendid, mis on uurimise hetkeks kustutatud, ent mida on võimalik taastada.[38]

Eelnevalt tõdesime, et digitaalkriminalistika eesmärgiks on ka andmete taastamine. Küll aga ei ole tegemist andmete taastamisega infotehnoloogia terminoloogia mõistes. Viimase eesmärgiks on taastada informatsiooni arvutist, millest on andmed kogemata kustutatud, kaotatud elektrikatkestuse või serveri ühenduse katkemise tõttu. Teine oluline aspekt, mis eristab andmete taastamist digitaalkriminalistikas on teadmine sellest, mida otsitakse. Digitaalkriminalistika eesmärgiks on otsida või taastada andmeid, mille kasutajad on peitnud või kustutanud, eesmärgiga kindlustada kogutud ja analüüsitud tõendite valiidsus ja lubatavus kohtumenetluses. Paljudel juhtudel uurivad digitaalrkiminalistid arvutit teadmatuses, kas see

[35] L. Caviglione, S. Wendzel, W. Mazurcyk. The future of Digital Forensics: Challenges and The Road Ahead. *IEEE Security & Privacy*, vol. 15, no. 6, pp. 12-17. November/December 2017, lk S65.
[36] Samas lk S65.
[37] L.Qian, F. Höglin, P. A. Diaz. Computer Forensics. Uppsala University. 2007, lk 3.
[38] Samas, lk 3.

mingeid tõendeid sisaldab. Juhul, kui tuvastatakse digitaalseid andmeid, ei pruugi need olla täielikud ja tõendi loomiseks tuleb leitud informatsiooni osadest tervik moodustada.[39]

2.1. DIGITAALKRIMINALISTIKA PRINTSIIBID

Digitaalkriminalistika näeb digitõendite analüüsimiseks ette suure hulga tunnustust leidnud uurimistehnikaid ja -meetodeid. Tulenevalt digitaalkriminalistika eripärast ei kasuta teadusharu mõistet "väljaspool mõistlikku kahtlust" ilma piisava aluseta. Me ei saa olla kindlad selles, mis kuriteopaigal toimus, omades väga limiteeritud informatsiooni toimunud sündmuste kohta, veelgi enam, seda digitaalsel kujul. Seega saab distsipliin välja tuua vaid järeldustele rajatud teooriad, mis tuginevad limiteeritud informatsioonile kuriteo asjaolude kohta.[40]

Digitaalkriminalistika printsiipide puhul on sisuliselt tegemist nii seaduses sätestatud protseduurireeglite kui ka teadusharupõhiste reeglite järgimisega, tagamaks tõendi kogumise, uurimise ja analüüsimise efektiivsuse ning lubatavuse kohtumenetluses. Tuginedes eeltoodule lähtuvad digitaalkriminalistid digitaalsete tõendite kogumisel alltoodud printsiipidest.

2.1.1. Tõendite vahetumine

Peamine eesmärk igasuguses uurimises on kurjategija jälgede uurimine ning nendevaheliste seoste loomine. Vahetu informatsiooni omamine digitaalsete tõendite olemasolu kohta ei oma iseenesest tõenduslikku väärtust. Omandatud teave tuleb menetlussätete kohaselt fikseerida ning seostada kuriteo tehioludega.[41]

Tuginedes Locardi printsiibile loob kontakt kahe asja vahel alati mingi jälje. See printsiip kehtib igasuguse kokkupuute puhul, sh võivad jäljed olla nii digitaalsed kui füüsilised. Lühidalt öeldes, jääb kahe objekti kokkupuutest alati maha jälg, mida mõningatel juhtudel ei ole niivõrd lihtne avastada. Jälg, mis tekib, võib väljenduda nii füüsilises kui ka digitaalses maailmas. Digitaalsed tõendid võivad paljastada kahtlusalus(t)e ja kannatanu(te) vahelise

[39] B. Nelson, A. Phillips, C. Steuart. Guide to Computer Forensics and Investigations. Third edition. Course Technology, Cengage Learning, 2010, lk 4.
[40] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 14-15.
[41] Samas, lk 16.

suhtluse või kokkupuute, tegevuse internetis või muud informatsiooni, mis loob uurimisele digitaalse dimensiooni.[42]

Arvutisse sissetungimise korral jätab ründaja alati maha mitmed jälgi enda kohalolekust, sh sissekanded failisüsteemidesse, registritesse, süsteemilogidesse ja võrgutasandil olevatesse logidesse. Lisaks digitaalsetele jälgedele võib kurjategija jätta ka füüsilisi jälgi, näiteks arvutiklahvile vajutades sõrmejälg või DNA.[43]

See tähendab, et digitaalse uurimise puhul on pahatihti füüsilised ning digitaalsed tõendid omavahel läbi põimunud. Lisaks digitaalsele dimensioonile võib uurimine hõlmata ka füüsilisi tõendeid, millele tuleb tähelepanu pöörata ning tuvastada. Füüsilised tõendid aitavad uurijatel mõista kuriteo tehiolusid, sh aidates kaasa digitaalsete tõendite kogumisele või analüüsimisele.

2.1.2. Tõendite omadused

Isiku ning kuriteopaiga vaheline kontakt loob jälje, mis kuulub reeglina ühte kahest kategooriast: a) selliste omadustega tõendid, mida on võimalik liigitada üldiste tunnuste abil ning; b) selliste omadustega tõendid, mida on võimalik liigitada individuaalsete tunnuste abil.[44] Digitaalkriminalistid peavad tõendite analüüsimisel arvesse võtma iga nii tõendi individuaalseid kui üldisi tunnuseid.

Üldised tunnused on asjade üldlevinud omadused, nt saapa jälg, ent individuaalsed omadused on unikaalsemad ning neid on suurema tõenäosusega võimalik siduda konkreetse inimese, tegevuse või tehioludega.[45]

Näiteks, Microsoft Word tarkvara puhul võib dokumenti analüüsides leida, et dokument on võltsing, kuivõrd analüüsi käigus leiab tuvastust fakt, et fail on loodud kasutades sellist tarkvara versiooni, mis on avaldatud mitmeid aastaid enne analüüsitava dokumendi loomise kuupäeva. Kui on oht, et digitaalsed tõendeid on varjatud või hävitatud, võivad üldised

[42] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 16.
[43] Samas, lk 16-17.
[44] Samas, lk 17.
[45] Samas, lk 18.

tunnused paljastada, et mingis konkreetses arvutis on kasutatud spetsiifilist krüpteerimismehhanismi või andmete hävitamise vahendit.[46]

Konkreetsemad individuaalseid omadusi on palju raskem, ent mitte võimatu, identifitseerida kasutades digitaalkriminalistika töömeetodeid. Nt spetsiifilised printerimudelid märgivad iga prinditud lehe spetsiaalse vesimärgiga, mida on võimalik siduda konkreetse printeri mudeliga. Unikaalsed tunnused digitaliseeritud fotodel võimaldavad tuvastada, et kahtlusaluse skänner või digikaamera oli mingi konkreetse kuriteoga seotud. [47]

Seega tuleb digitaalset uurimist läbi viies pöörata erilist tähelepanu digitõendite iseloomulikele joontele - esmalt need tuvastada ning piiritleda ja teisalt võtta uurimisprotsessi kestel arvesse nende iseärasusi.

2.1.3. Digitõendite kriminalistikaline usaldusväärsus

Kriminalistikaline usaldusväärsus tähendab selliste digitaalsete tõendite loomist, millele on võimalik kohtumenetluse kestel tugineda. Mõningad autorid on eeltoodud mõistepaari defineerinud kui läbipaistva digitaalkriminalistika protessi rakendamist tagamaks analüüsitavate andmete originaaltähenduse ning lubatavuse kohtumenetluses.[48]

Traditsioonilinse kriminalistika puhul leitakse, et tugeva tõendiga on tegemist juhul, kui fikseeritud teave ei muuda algset tõendi allikat. Digitaalkriminalistika puhul ei saa eeltoodud väitega nõustuda, sest enamikel juhtudel omandatakse informatsioon arvuti kõvakettalt või muult digitaalselt andmekandjalt. Isegi, kui andmete ekstraheerimiseks kasutatakse *write-blocker* [49] seadme kasutamisel muutub kõvaketta esialgne seisukord. Muudatused võimaldavad uurijatele juurdepääsu kõvaketta salajastele osadele, samal ajal töödeldakse originaaltõendit. Seega ei saa väita, et digitaalkriminalistika puhul oleks tegemist tugevate tõenditega vaid juhul, kui tõendi esialgset allikat ei muudeta. Digitaalsed andmed, mis fikseeritakse tõendina, omandatakse algandmete muutmise protsessi tulemusena.[50]

[46] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 18.
[47] Samas, lk 18.
[48] R. McKemmish. When is Digital Evidence Forensically Sound?. Ray I., Shenoi S. (eds) Advances in Digital Forensics IV. DigitalForensics 2008. IFIP — The International Federation for Information Processing, vol 285. Springer, Boston, MA, 2008, lk 10.
[49] Seade, mis võimaldab omandada kettalt informatsiooni ilma ohuta ketta muud sisu kahjustada.
[50] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 19.

Digitaalkriminalistika puhul on tugevate tõendite eelduseks tõendi loomise ja kogumise protseduuri dokumenteerimine. Tõend on usaldusväärne ja läbipaistev juhul, kui on teada, millisest allikast tõend pärineb ning kuidas seda töödeldi. Kriminalistika vaatepunktist on tähtis, et tõendite kogumise protsess muudaks algset tõendi allikat võimalikult vähe ja igasugused muudatused oleksid dokumenteeritud ning määratletud. Digitaalkriminalistika puhul võib tõendi kohta väita, et tegemist on tugeva tõendiga juhul, kui tõendi kogumise protsess säilitab täieliku ja täpse representatsiooni originaalandmetest, selle autentsuse ja terviklikkuse.[51]

Terminit kriminalistikaline usaldusväärsus on võimalik kirjeldada läbi nelja kriteeriumi. Esmalt, kogutud digitaalne tõend peab omama digitaalses uurimises mingit tähendust ehk olema vajalik kuriteo koosseisu või tehiolude tõendamiseks. Teiseks tuleb tõendi fikseerimisel üles märkida kõikvõimalikud tarkvara- ning riistvara lahenduste kasutamisest tulenevad eksimused ning tehnilised probleemid. Kolmandaks peab digitaalse analüüsimise protsess olema läbipaistev, st kõik tõendi fikseerimiseks võetud sammud tuleb dokumenteerida. Viimaseks aitab digitaalse tõendi usaldusväärsust saavutada uurija töökogemusele tuginemine.[52]

2.1.4. Digitõendite autentsus

Autentimine seisneb kohtu veenmises selles, et esitatud protokolli, tõendi või andmete sisu on muutmata kujul, informatsioon pärineb väidetavast allikast ja kõrvaline informatsioon, näiteks tõendi kuupäev, on täpne.[53]

Autentimine on kaheosaline protess, milles tuleb esmalt üle vaadata tõend tervikuna veendumaks, et andmed kinnitavad või lükkavad ümber neid asjaolusid, mida esitaja väidab. Edasise analüüsi käigus tuleb kindlaks määrata esitatud informatsiooni tõendamisväärtus.[54]

Tõendi autentsus tähendab seda, et esitatud tõend on see, mida uurija või prokurör väidab. Tõendi autentsuse printsiip on lähedalt seotud tõendi asjakohasusega. Digitaalne tõend peab

[51] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 19.
[52] R. McKemmish. When is Digital Evidence Forensically Sound?. Ray I., Shenoi S. (eds) Advances in Digital Forensics IV. DigitalForensics 2008. IFIP — The International Federation for Information Processing, vol 285. Springer, Boston, MA, 2008, lk 10-13.
[53] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 21.
[54] Samas, lk 21.

tõendama neid kuriteo asjaolusid, mis on esitaja eesmärgiks, vastasel juhul pole tegemist asjakohase tõendusmaterjaliga.[55]

2.1.5. Tõendite valdajate ahel

Tõendi autentsuse aspektist on äärmiselt tähtis, et tõendi fikseerimise protseduur säilitatakse ja dokumenteeritakse. Iga inimene, kes digitaalse uurimise kestel informatsiooni töötles, võib olla kohustatud andma tunnistusi selle kohta, et tõend, mida kohtus esitatakse, on identne sellega, milline see oli uurimise kestel. Võimaldamaks digitaalsete tõendite autentsust, tuleb dokumenteerida tõendi fikseerimise protseduur toimingute, tõendit töödelnud isiku nimede, kuupäeva ja muude oluliste tunnuste järgi.[56]

Tõendi valdajate ahelat võib defineerida kui teekaarti näitamaks teabe kogumise, analüüsimise ning säilitamise protsessi, omandamaks digitaalse tõendi väärtuse ning olemaks kohtus lubatud.[57]

Esitades kohtumenetluses digitaalse tõendi ning teades, kuidas seda töödeldi ja analüüsiti, ei ole piisav. Uurija peab dokumenteerima täpse loetelu tõendi fikseerimise protsessist, sh selle, kes seda töötlesid ning millistel ajahetkedel. Uurija peab olema võimeline kogu digitaalse uurimise protsessi kestel vastama järgnevatele küsimustele - mis digitaalse tõendiga on tegemist, millisest allikast kõnealune tõend koguti, kes selle leidis, ja käitles, kuna see leiti, tõendile esmakordselt juurde pääseti, uuriti või edastati ja milline on konkreetse digitaalset tõendit eesmärk tõendamisel.[58]

Ilma eeltoodud ahela loomise ning dokumenteerimiseta on võimalik argumenteerida, et tõendit on töödeldud ebaõigesti ning seda võidakse olla muudetud, asendatud süüstava sisuga tõendiga või rikutud muul viisil.[59] Tõendi käitlemise ahela säilitamine ning esitamine on

[55] S. Van Deusen Phillips. Legal Considerations for Electronic Evidence, Part 2: Relevance and authenticty. Word Press, 2010. Arvutivõrgus kättesaadav: https://crlgrn.wordpress.com/2010/04/26/legal-considerations-for-electronic-documentation-part-2-relevance-and-authenticity/ (viimati külastatud 23.04.2018)
[56] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 21.
[57] M.G.Nagaraya. Investigators chain of custody in digital evidence recovery. Bureau of Police Research and Development, Indian Police Journal, 2006, lk 154.
[58] J. Cosic, M. Baca. (Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. The 33rd International Convention MIPRO. Opatija, Croatia, 2010, lk 1.
[59] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 22.

oluline, sest nagu eelpool mainitud, on digitaalsed andmed hõlbsalt muudetavad, kompromiseeritavad juhul, kui korrektseid ettevaatusabinõusid ei rakendada.[60]

Tõendi käitlemise ahela korrektne rakendamine aitab uurijal tõendada, et süüstavat tõendit ei ole muudetud ning uurijad ei ole tõendeid tehislikult fabritseerinud mõistmaks inimest aluseta süüdi.[61]

2.1.6. Digitõendite terviklikkus

Digitaalkriminalistika puhul on oluliseks elemendiks garanteerida digitaalse tõendi muutmatus ajast, mil see koguti kuni digitõendi fikseerimiseni ja kasutamiseni kohtumenetluses. Eeltoodu kohustab uurijat tagama digitaalse tõendi terviklikkuse.[62]

Digitaalkriminalistika puhul kujutab tõendi terviklikkuse hindamise protsess esialgse digitaalse "sõrmejälje" ning fikseeritud tõendi vahetut võrdlemist.[63]

Lähtuvalt eeltoodud printsiibist tuleb originaaltõendist luua digitaalne koopia. Protseduuri eesmärk on luua originaalfaili peegelpilt, mida on võimalik analüüsida ilma ohuta muuta või hävitada potentsiaalset tõendusmaterjali sisaldavat originaaldokumenti või –faili.[64] Digitaalse koopia loomine võimaldab uurijatel algfailis leiduvat teavet analüüsida ohuta, et originaalfail häviks ning edasine analüüs poleks võimalik.

Tõendi terviklikkuse kontrollimiseks kasutatakse räsifunktsioone. Peamised räsifunktsioonid, mida digitaalkriminalistika kasutab, on SHA-1 (ingl. k. *Secure Hash Algoritm 1*) ning MD5 (ingl. k. *Message Digest 5)*. Räsifunktsioone abil genereeritakse originaaltõendile ning tõendi kriminalistilisele koopiale kontroll- ehk *hash* väärtus. [65] Tuginedes asjaolule, et originaaltõendi ning digitaalse koopia puhul on tegemist sisuliselt identsete failidega, peavad räsifunktsioonide abil genereeritud kontrollväärtused olema võrdsed.

---

[60] J. Cosic, M. Baca. (Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. The 33rd International Convention MIPRO. Opatija, Croatia. 2010, lk 1.
[61] Samas, lk 2.
[62] V. Schmitt, J. Jordaan. Establishing the Validity of MD5 and SHA-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in these Algorithms. International Journal of Computer Applications (0975 – 8887) Volume 68– No.23, April 2013. Lk 40.
[63] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011. Lk 22-23.
[64] S. von Solms, C. Louwrens, C. Reekie and T. Grobler. A Control Framework for Digital Forensics. Olivier M.S., Shenoi S. (eds) Advances in Digital Forensics II. IFIP Advances in Information and Communication, vol 222. Springer, Boston, MA. 2006, lk 4.
[65] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011. Lk 22-23.

Kontrollväärtus (ingl. k *hash value)* on matemaatiliste kalkulatsioonide tulemusena fikseeritud kontrollväärtus. Kontrollväärtuse omistamiseks sisestatakse faili andmed programmi, millest koostatakse matemaatiliste protsesside tulemusena fikseeritud kontrollväärtus.[66]

Kontrollväärtused on hindamatu väärtusega osa digitaalkriminalistikast, digitaalsete tõendite loomiseks, identifitseerimiseks ja klassifitseerimiseks. Uurijate peamine eesmärk räsifunktsioonide kasutamisel on säilitada digitaalse informatsiooni tõenduslik terviklikkus.[67]

2.1.7. Digitõendite objektiivsus

Igasuguse kriminalistilise analüüsi nurgakiviks on objektiivsus ehk erapooletus. Tõendi esitamine ning tõlgendamine peab olema eelarvamustevaba, tagamaks kohtunikele selgeima võimaliku vaate kuriteo tehioludest. [68]

Objektiivsuse saavutamiseks on efektiivseim meetod kasutada tõendit viisil, mil iga järeldus esitatakse koos seda toetava tõendusmaterjaliga. Teiseks objektiivsuse tagamise meetodiks on tõendi igakülgne ja korduv uurimine. Tõendi teistkordsel analüüsimisel võidakse leida, et tõendi hindamine pole läbi viidud objektiivselt või tuvastada muid nõrkusi, mis võivad hiljem tõendi fikseerimisel abiks olulised olla.[69]

2.1.8. Digitaalsete andmete analüüsimise korratavus

Iga teadusliku meetodi puhul on oluline eksperimendi või vaatluse korratavus. Eriti kaalukaks saab see juhul, mil sellest oleneb inimese vabadus või elatusvahendid. Seega võib osutuda vajalikuks, et uurija peab olema võimeline kordama juba läbi viidud tõendi analüüsimise protsessi. Selleks, et taoline verifitiseerimine oleks võimalik, on oluline detailselt dokumenteerida digitaalse tõendi kogumise ning analüüsimise sammud. See võimaldab vajaduse korral kolmandal isikul iseseisvalt korduvanalüüsi läbi viia. Dokumenteerida tuleb

[66] Establishing the Validity of Md5 and Sha-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in these Algorithms. International Journal of Computer Applications (0975 – 8887) Volume 68– No.23, April 2013. Lk 40.
[67] Samas, lk 40.
[68] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011. Lk 24.
[69] Samas, lk 24.

näiteks digitaalse tõendi asukoht ja muud iseloomulikud tunnused, kui ka töövahendid, millega andmeid töödeldi.[70]

2.2. DIGITAALKRIMINALISTIKA MENETLUSMUDEL

Digitaalsete tõendite kriminalistikalise analüüsi eripärasused tulenevad konkreetsest kaasuse asjaoludest ning reeglina baseeruvad teadmistele, kogemustele, ekspertiisile, põhjalikkusele ning mõningatel juhtudel uurija uudishimule uurimisprotsessi läbi viies.[71]

Protseduure, mis fikseerivad elektroonilisest dokumendist või teabest lubatud elektroonilise tõendi, nimetatakse digitaalkriminalistika etappideks. Digitaalkriminalistikalisele analüüsile saab viidata kui uurijale teadaolevatest andmetest tõendusmaterjali tuvastamisele. Eeltoodud protsessis on võimalik identifitseerida neli võtmetegevust – ülevaade võimalikest tõenditest, hüpoteesi seadmine, andmete otsimine hüpoteesi kinnitamiseks või ümber lükkamiseks ning analüüsitulemuste dokumenteerimine.[72]

Konkreetset kaasust ette valmistades on mõistlik sätestada ning täita järgmised uurimise etapid[73]:

- Luua esialgne hinnang lähtuvalt eesseisva kaasuse liigist. Määramaks kindlaks kaasuse liiki ning iseärasusi, on soovitatav intervjueerida inimesi, kes on sellega seotud ning esitada küsimusi intsidendi kohta. Eeltoodud võimaluse puudumisel tähelepanelikult tutvuda kuriteopaika või muude kuriteo tehiolusid kirjeldavate asjaoludega.
- Määrata kindlaks esialgne lähenemisviis kaasusele. Välja mõelda ning üles märkida sammud, mida on tõendite leidmiseks vajalik järgida ning uurida. Juhul, kui ilmneb, et oluline on personaalarvuti või muu digitaalse seadme arestimine, määrata kindlaks selle võimalikkus ning muud menetlusõiguslikud sammud. Täiendavalt on oluline kindlaks määrata millised tõendid või teave on juba kogutud või uurijatele teada.

[70] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 25.
[71] E. Casey. Handbook of Digital Forensics and Investigation. Academic Press. 2009, lk 24.
[72] S. von Solms, C. Louwrens, C. Reekie and T. Grobler. A Control Framework for Digital Forensics. Olivier M.S., Shenoi S. (eds) Advances in Digital Forensics II. IFIP Advances in Information and Communication, vol 222. Springer, Boston, MA. 2006, lk 345.
[73] B. Nelson, A. Phillips, C. Steuart. Guide to Computer Forensics and Investigations. Third edition. Cengage Learning. 2014, lk 30-31.

- Luua detailne kontrollnimekiri. Kontrollnimekiri aitab määratleda uurimises vajalikud sammud ning oletatava aja nende sooritamiseks. Samm on tõhus järgimaks uurimise eesmärke ning mitte kõrvale kalduma uurimises kriitilist tähtust omavatest elementidest.
- Määratleda, milliseid ressursse on uurimises vaja kasutada. Näiteks, tuginedes sellele, milline on analüüsitaval arvutil kasutatav operatsioonisüsteem, on võimalik välja tuua võimalikud tarkvararakendused või muud meetodid, mida digitaalsete tõendite kogumiseks või analüüsimiseks on vaja kasutada.
- Digitaalse tõendi originaalallikast koopia loomine.[74]
- Riskide identifitseerimine. Üksikasjalikult välja tuua potentsiaalsed ohud, mis on konkreetsest seadmest tõendite tuletamisel aktuaalsed. Näiteks, kui kahtlusalune omab arvutialaseid eriteadmisi, tuleb kaaluda võimalust, et digitaalseid tõendeid ei ole võimalik niivõrd lihtsalt leida, kuivõrd andmed võivad olla krüpteeritud või salasõnaga kaitstud.
- Eemaldada või minimaliseerida tuvastatud riskid. Identifitseerida riskide maandamise võimalus. Näiteks, kui eelnevalt on tuvastatud, et kõvaketas on salasõnaga kaitstud, on mõistlik luua mitu erinevat digitaalset koopiat, juhuks, kui üks koopiatest hävineb.
- Koostatud plaani üle kontrollimine. Üle vaadata eelnevalt loodud detailne plaan ning sammud, mis on juba täidetud. Üks etapi osa on kontrollväärtuste verifitseerimine veendumaks, et digitaalsed koopiad on loodud õigesti ning tehnilisi probleeme ei esine.
- Digitaalsete tõendite analüüsimine ning vajadusel andmete taastamine. Kasutades asjakohaseid tarkvararakendusi ning oskusi, uurida andmeid põhjalikult ning igakülgselt. Juhul, kui on tuvastatud, et digitaalandmekandjalt on andmeid kustutatud või kompromiseeritud, viia läbi andmete taastamise protsess.
- Tuletatud andmete kriminalistiline uurimine ja järelduste tegemine.
- Juhtumi raporti koostamine. Etapp seisneb täieliku ning detailse raporti koostamisest, millest nähtub milliseid andmeid leiti ning milliste meetoditega.
- Andmete kritiseerimine. Üle vaadata leitud andmeid, tuvastamaks, kas kasutatud protseduurid ning meetodid olid õiged ja tehtud järeldused on piisavalt põhjendatud ning argumenteeritavad.

Nähtuvalt eeltoodust, hõlmab digitaalkriminalistikaline menetlusmudel endas kõiki varasemalt välja toodud digitaalkriminalistika põhiprintsiipe.[75]

[74] Vt. Peatükk 3.1.6.

2.3. DIGITAALKRIMINALISTIKA TÖÖVAHENDID

Käesoleva töö raames oleks liialt ressursikulukas üksikasjalikult välja tuua välja tarkvaraprogramme ning töömeetodeid, mida digitaalrkiminalistikas kasutatakse. Seetõttu toob autor järgnevalt välja peamised meetodid tõendite analüüsimiseks.

Digitaaltõendeid analüüsivad uurijatel on juurdepääs laialdastele töövahenditele, nii üldsusele avatud programmidele kui ka spetsiaalselt uurijate jaoks välja töötatud arvutirakendustele, mis aitavad digitaalseid tõendeid säilitada ning analüüsida.[76]

Eeltoodud töövahendid näevad ette erinevad abstraktsuse tasemed, võimaldades uurijal turvaliselt luua digitaalsete tõendite koopiaid ning sooritada muid rutiinseid uurimisülesandeid. See vähendab uurija vajadust süveneda pisidetailidesse, nt füüsilise kõvaketta organisatsiooni korraldamise protsessile või komplifitseeritud failitüüpide struktuuri mõistmisele, mis on aktuaalne eelkõige metaandmete analüüsimise puhul.[77]

2.3.1. Töövahendite efektiivsus arvuti tasandil

Tehnilisel tasandil on võimalik digitaalse uurimise protsessi kirjeldada järgnevalt: iga faili kohta mingis kindlas süsteemis tuleb teostada spetsiifilisi protseduure, nt failide indekseerimine, andmete otsing võtmesõnade abil, pisipiltide genereerimine jne.[78]

Digitaalkriminalistika otstarbeks on ettevõte AccessData poolt välja töötatud tarkvaraprogramm *Forensic Toolkit (*edaspidi *FTK).* See skanneerib kõvaketast otsimaks erinevat päringus sätestatud informatsiooni. Nt, suudab programm tuvastada kustutatud e-kirju, skanneerida kõvaketast päringus esitatud tekstiribade tuvastamiseks ning dekrüpteerida salasõnu.[79]

FTK eesmärk on vähendada uurija vajadust faili korduvaks lugemiseks. Selleks koostab programm eeltöödeldud faili, mille stuktureeritud loend lihtsustab uurija tööd failide leidmisel. Olgugi, et tegemist on äärmiselt efektiivse tarkvaralahendusega, on FTK kasutamine tehniliste võimaluste tõttu limiteeritud. Esiteks võib eeltöötletud pildi loomine

[75] Vt. Peatükk 3.1.
[76] G. G. Richard, V. Roussev. Digital Crime And Forensic Science in Cyberspace, Chapter IV: Digital Forensics Tools: The Next Generation. IGI Publishing Hershey, PA, USA, 2006, lk 76
[77] Samas, lk 76-77.
[78] Samas, lk 77.
[79] Samas, lk 79.

olla ajakulukas, vahel võib eeltöötletud pildi loomiseks mitmeid päevi. Teiseks, märgivad süsteemiindeksid vaid informatsiooni, mille programm arvab uurimises vajalikuks oleva, jättes tihtipeale tähelepanuta võõrkeelessed võtmesõnad. Viimaseks, indeksistruktuur, mida suuremahulise andmete korral luuakse, on mahult suur, mistõttu võib esineda eeltöödeldud failide hoiustamise probleeme.[80]

Seega, tuginedes eeltoodule on digitaalkriminalistiliste töövahendite efektiivsuse analüüsimise korral kaks erinevat probleemi. Esmalt, mida keerukama struktuuri ning suurema mahuga on analüüsitavad failid, seda keerulisemaid analüütilisi protsesse tuleb rakendada, eelkõige efektiivsemate algorütmide koostamist ning nende alusel programmide loomist. Teisalt, mida keerukam ja suurem on fail, seda võimsamat arvutisüsteemi see vajab digitaalse uurimise läbiviimiseks. Olukorras, mil analüüsitav kõvaketas sisaldab ühe terabaidi suuruses informatsiooni.[81]

2.3.2. Töövahendite efektiivsus inimese tasandil

Töövahendid uurija tasandil tähendavad uurija aja paremat kasutamist ning automatiseeritud, rutiinsete ülesannete hulga vähendamist. Üks eeliseid kasutamaks digitaalsete uurimiste puhul kõrgetehnoloogilisi arvutisüsteeme võimaldab luua vahendeid, mis on uurijale vastuvõtlikumad. See tähendab, et ajal, mil arvuti töötleb erinevaid andmeid, on uurijal võimalus keskenduda muudele uurimises kriitiliste elementide analüüsimsisele.[82] Taoline olukord võimaldab samaaegselt läbi viia rohkem toiminguid.

Teine tähtis punkt on, et arvutisüsteemide kasutamine võimaldab kasutada keerukamaid analüüsimismeetodeid, kui on inimese võimuses. Näiteks, tavaline arvutikasutaja omab reeglina mitimeid erinevaid multimeediaobjekte, näiteks pildi, video- ja helifaile. Olemasolevad tööriistad ei võimalda eeltoodud failide automatiseeritud töötlemist, mis tähendab, et need tuleb läbi viia manuaalselt.[83]

Seega, sisuliselt on digitaalkriminalistika töövahendiks ka uurija ise. Olgugi, et tehnika võimaldab vähendada analüüsitavate andmete hulka, ei välista tehniliste lahenduste olemasolu uurija rolli digitaalse analüüsi läbiviimisel.

[80] G. G. Richard, V. Roussev. Digital Crime And Forensic Science in Cyberspace, Chapter IV: Digital Forensics Tools: The Next Generation. IGI Publishing Hershey, PA, USA, 2006, lk 76.
[81] Samas, lk 77.
[82] Samas, lk 86.
[83] Samas, lk 87.

2.4. DIGITAALKRIMINALISTIKA TÖÖVAHENDITE TÕHUSUS

Olgugi, et digitaalsete tõendite tehnilised probleemid ei ole niivõrd tihedalt seotud õigusliku aspektiga, on tõendite lubatavuse regulatsiooniga tihedalt seotud. Kui tehnilised võimalused tõendite loomiseks on piiratud, raskendab tekkinud olukord kriminaalmenetluse seadustiku kohaselt lubatavate tõendite loomist. Seega on digitaaltõendite kasutamise perspektiivikuse määramisel oluline käsitleda ka digitaalkriminalistika tehnilisi võimalusi ning lahendusi tõendite fabritseerimiseks.

2.4.1. Fabritseeritud digitaalsed tõendid

Infotehnoloogia ning elektroonilised seadmed võivad olla kuriteo toimepanemise vahendiks ning sisaldada tõendeid kuritegude toimepanemise kohta. Küll aga võivad leitavad andmed viidata süüdistatava alibile. Nimisõna "alibi" tähendab ladina keeles "kusagil mujal".[84] Seega on alibi puhul tegemist sellise tõendi eriliigiga, mille eesmärk on veenda kedagi faktis, et isik, keda arvati kuriteopaigas viibivat, viibis samal ajahetkel mingis muus asukohas.

Võtmesõnad alibi määratlemisel on aeg ja koht. Kui isik sooritab arvuti või internetivõrgu vahendusel kuriteo, siis tihtipeale jääb jälg ajast ning kohast, genereerides digitaalse tõendi, mida saab alibi loomiseks või ümber lükkamiseks kasutada.. [85]

Seega on võimalik digitaalseid tõendeid kasutada ka kui alibisi tõendamaks, et isik ei saa olla süüdistusega seotud, kuivõrd kuriteo toimepanemise ajahetkel ei viibinud kahtlustatav kuriteopaigas. Sisuliselt iga tegevus, mis hõlmab arvutisüsteemi kasutamist, sh erinevate maksete tegemine, piletide soetamine või aktiveerimine, jätab endast digitaalse jälje, mida on võimalik uurimise käigus tõendina kasutada.

Fabritseeritud tõendite loomise peamine eesmärk on eksitada uurijat õigete jälgede või tõendite leidmisel või luua alibi tõendamaks mingite asjaolude olemasolu või ümberlükkamist.

[84] A. Castiglione, G. Cattaneo, G. De Maio, A. De Santis, G. Costabile, M. Epifani. The Forensic Analysis of a False Digital Alibi. 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Palermo, 2012, lk 115.
[85] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 323.

Protsessi eesmärgiks on simuleerida kasutaja tegevust nii reaalselt ja süvitsi, kui võimalik. Kõne alla tuleb nii internetilehekülgede külastamine, e-kirjade saatmine, kiirsõnumeid saatvate rakenduste kasutamine kui ka erinevat tüüpi dokumentide redigeerimine.[86]

Fabritseeritud tõendite loomisel rakendatakse eeldust, mille kohaselt on digitõend loodud digitaalset seadeldise abil. Lisaks seadmetele pakuvad paljud usaldusväärsed ettevõtted erinevaid teenuseid (nt sotsiaalmeediakanalid, meiliboksid), mis salvestavad kasutajate tegevust, näiteks juurdepääsu kuupäeva või külastamise sessiooni pikkust, mida on võimalik kohtumenetluses tõenditena kasutatada.[87]

Võltsitud tõendite tuvastamiseks või eelduste ümber lükkamiseks on kõige lihtsam tehniline võte esitada päring isikule või ettevõttele, kes on loodud tõenditega tihedalt seotud, olles selleks näiteks sotsiaalmeediaportaal Facebook või isik, kellele kahtlustatav sõnumeid edastas.[88]

Tõendite fabritseerimisel on võimalik välja tuua kaks peamist tõendite loomise viisi. Esmalt tuleb kõne alla tõendite fabritseerimine kaugjuhtimise vahendusel. Sisuliselt seisneb see meetod faktis, et võltstõendite loomiseks on vajalik luua ühendus mingi arvutisüsteemiga ajahetkel, mil soovitakse alibit luua. Selleks, et eeltoodu läbi viia, on vajalik kaugjuhtida mingit seadet internetiühenduse vahendusel, kasutades selleks vastavat tarkvara- või riistvaralahendust. Teiseks, saab rääkida automatiseeritud tegevusest, mis seisneb fabritseeritud tõendite loomises kasutades täielikult automatiseeritud tarkvaralahendusi. Eeltoodud vahend ei nõua kasutaja ja tõendi allikapoolset koostoimet.[89]

Tuginedes eeltoodule, on võimalik tõendite loomise protseduur jaotada kaheks:

1. Tõendite fabritseerimine kasutades kaugjuhtimisseadmeid

Isik, kes kasutab digitaalsete tõendite loomiseks KVM-lülitit[90], ei pea installeerima uurijatele kahtlust tekitavat tarkvara, millele tuginedes oleks võimalus tuvastada tõendite fabritseerimist. Sellest hoolimata peab indiviid kasutama ettevaatusabinõusid limiteerimaks tahtmatute jälgede arvu. Näiteks, KVM-lüliti tuleb konfigureerida staatilise IP aadressiga hoidumaks

[86] S. Beyer, M. Mulazzani, S. Schrittwieser, M. Huber and E. Weipp. Towards fully automated Digital Alibis with social interaction. Technical University of Vienna. Vienna, 2014, lk 67.
[87] A. De Santis, A. Castiglione, G. Cattaneo, G. De Maio, M. Ianulardo. Automated Construction of a False Digital Alibi. Springer, Berlin, Heidelberg. 2011, lk 1.
[88] Samas, lk 3.
[89] Samas, lk 3.
[90] Seade, mille vahendusel on võimalik ühe klaviatuuri, monitori ja hiire abil kontrollide mitmeid teisi ühendatud arvutisüsteeme.

kohalikku DHCP[91] (ingl. k. *Dynamic Host Configuration Protocol*) serverisse päringute salvestamisest. Eeldades, et tõendi looja on kasutusele võtnud kõik ettevaatusabinõud, on sellegipoolest internetiteenuse pakkujale päringu esitamise abil võimalik tuvastada ebaregulaarne IP-ühendus valetõendite loomise ajal.[92]

Kasutades tõendite loomiseks kaugjuhtimistarkvara, tuleb kahtluste limiteerimiseks luua tõendid kasutades mälupulgale installeeritud tarkvara (nt TeamViewer Portable). Sellest olenemata võib arvuti, millesse tõendid paigutati, jätta maha jälje tarkvara kasutamisest. Sellegipoolest on tegemist nö turvalisema meetodiga, kuivõrd see ei jäta interneti teenusepakkujale ega ruuteritsesse ühtegi jälge kaugjuhtimisseadmete kasutamisest.[93]

2. Tõendite automatiseeritud fabritseerimine

Tõendite automatiseeritud loomise puhul tuleb eelkõige kõne alla, milliseid vahendeid nende loomiseks kasutatakse, ning kuidas on eeltoodud tõendid eristatavad nö inimeste poolt loodud tõenditest. Tüüpilised inimkäitumise toimingud on iseloomustatavad hiireklikkide, klaviatuurivajutuste, tekstide kirjutamise, spetsiaalse tarkvara kasutamise juhusliku ajastamise kaudu. Taolist käitumist on võimalik simuleerida automatiseeritud programmide abil. Mõningad automatiseeritud programmid on võimelised sooritama lihtsamaid operatsioone, näiteks klaviatuurinuppude vajutamise ja hiireliigutuste simuleerimine, erinevate programmide avamine, sulgemine jne.[94]

Eeltoodud vahendid võimaldavad reeglina sooritama ka komplitseeritumaid, ent lihtsakoelised toimingud on piisavad loomaks fabritseeritud tõendeid. Näiteks on programmid võimelised navigeerima veebibrauserites, avama internetilehekülgi, logima sisse erinevatesse veebilehtedesse, postitama sotsiaalmeediasse jne. Lisaks on tarkvara võimeline töötlema nii erinevaid faile, kaustu kui ka videosid ja pilte, looma tekstifaile, sooritama telefonikõnesid jne.[95] Tuginedes eeltoodule, on sisuliselt võimalik automatiseeritud toimingute abil luua tõendeid igal ajahetkel ning igasuguses vormis.

Isik, kelle eesmärgiks on luua fabritseeritud alibi, peab identifitseerima alibi loomisel kasutatavate programmide poolt loodud tahtmatud tõendid ning seejärel implementeerima

[91] Andmevahetuse protokoll, mis võimaldab võrguhalduril lasta serveril või ruuteril dünaamiliselt hallata ja automatiseerida unikaalse IP-aadressi omistamist kohtvõrgu seadmetele ning võimaldab seda kasutada määratud ajavahemikul.
[92] A. De Santis, A. Castiglione, G. Cattaneo, G. De Maio, M. Ianulardo. Automated Construction of a False Digital Alibi. Springer, Berlin, Heidelberg. 2011, lk 3-4.
[93] Samas, lk 4.
[94] Samas, lk 4-5.
[95] A. De Santis, A. Castiglione, G. Cattaneo, G. De Maio, M. Ianulardo. Automated Construction of a False Digital Alibi. Springer, Berlin, Heidelberg. 2011, lk 5.

tehnika, kuidas need elimineerida või neist hoiduda. Eeltoodud tahtmatute tõendite loomise risk sõltub sellest, millist tarkvara ja operatsioonisüsteemi kasutatakse. [96]

Esmalt, jäävad maha toimingute sooritamise jäljed. Igasuguse operatsiooni puhul nimetatakse protsessiks igasuguste programmide käivitamist ning eeltoodud protsesside kohta salvestatakse failisüsteemis vastavad andmeid, näiteks programmi nimi, algusaeg jne.[97]

Teiseks, lisaks eeltoodule, jätavad operatsioonisüsteemidesse sisselogimised jälgi sellest, kuna ning kes on süsteemi sisse loginud. Reeglina luuakse salvestused süsteemi sisse-välja logimise hetkel ning süsteem teeb kindlaks, millal sisse ja/või välja logiti, sisselogija identifitseerimiseks vajalikud andmed. Salvestisi on võimalik modifitseerida, ent enamus digitaalkriminalistika meetodeid võimaldavad muudatuste tegemise tuvastada.[98]

3. Fabritseeritud tõendite tuvastamine

Tehnilistest probleemidest on kahtlemata oluline võltstõendite loomise tuvastamine. Kuivõrd digitaalseid andmeid on lihtne manipuleerida ning tehislikult luua, tuleb igasse tõendisse suhtuda teatava kahtlusega ning tagada kõik tehnilised lahendused tegemaks kindlaks tõendi usaldusväärsust.

Tuginedes sellele, on uurijatel võimalik tuvastada, kas tõend on artifitsiaalselt loodud või mitte. Eelkõige, kõikidel juhtudel, mil tõend luuakse kaugjuhtimisseadeldise abil, jätab arvutisse sisselogimine internetiteenuse pakkuja serveritesse andmeid, täpsemalt IP-aadressi, millelt arvutisse pääseti. Sisuliselt peavad uurijad olema kursis sellega, milliseid jälgi kaugjuhtimisseadeldised jätavad ning limiteerima võimalused tuvastamaks asjaolud, kas tegemist on legitiimse tõendiga või mitte. Eeldades, et kurjategija on infotehnoloogia valdkonnas pädev, võib jälgede leidmine olla uurija jaoks väga keerukas – kurjategija on endale teatavaks teinud kõik potentsiaalsed riskid ning need minimiseerinud. Sellisel juhul saab määrava tähtsusega asjaoluks uurija tähelepanelikkus ning detailide leidmise oskus, mis tähendab, et võltstõendite puhul tuleb enam kui kindla teadmisega piiritleda asjaolu, et tõend ei ole tehislikult loodud.

Automatiseeritud tõendite loomise puhul on tegemist keerukama protsessiga. Ainsad jäljed, mis võivad arvutisse programmi kasutamisest jääda, on programmi olemasolu, selle

[96] Samas, lk 6.
[97] Samas, lk 6.
[98] Samas, lk 6.

käivitamise aeg ning programmi sisu. Programmid, mida luuakse on äärmiselt kompleksed, võimaldamaks sooritada pea inimtegevuse lähedaseid toiminguid, alustades hiire liigutamise ja klaviatuurinuppude vajutamisega, lõpetades sotsiaalmeedia postituste tegemise või audio- või videofailide töötlemisega. Seega on keeruline välistada niivõrd keerukate operatsioonide läbiviimisel reaalset inimtegevust. Automatiseeritud võltstõendite tuvastamisel on vaja suunduda sügavamale, st esmalt välistada võimaluse, et keegi võib olla neid loonud eesmärgiga eksitada uurijaid.

Kokkuvõtteks, tõendite fabritseerimine ehk võltsalibite loomine, on digitaalsete tõendite puhul suur risk. Mida rohkem areneb infotehnoloogia valdkonnana, seda suurem on võimalus, et sellega kaasnevad uued meetodid peitmaks mingeid tegevusi ning võimaldamaks luua faile või tõendeid eksitamaks uurijaid mingite asjaolude või sündmuste kulgemise kohta. Selleks, et taolisi olukordi tuvastada ning elimineerida, tuleb asjasse kaasata oma ala eksperdid ning uurimist läbi viia äärmiselt suure hoolega. Digitaalne tõend on usaldusväärne vaid juhul, kui uurija on kindlaks teinud andmete tõendusliku väärtuse tehniliste lahenduste abil.

2.4.2. Digitaalsete koopiate valiidsus

Digitaalse koopia loomise üks peamisi eesmärke on saavutada digitaalse tõendi valiidsus, usaldusväärsus ning võimalusel taasesitada tõendi loomise protseduuri.

Teises peatükis käsitlesime tõendi valiidisuse tuvastamiseks digitaalsetele failidele kontrollväärtuse omistamist kui võimalust tagada tõendi valiidsus. Eeltoodud räsifunktsioonide efektiivsuse kontrollimiseks, viisid teadlased läbi uurimuse MD5 ja SHA-1 tulemuslikkuse tuvastamiseks.

Matemaatiliselt võimaldavad MD5 ja SHA-1 kalkulatsioonid tuvastada isegi ühe baidi suuruse muudatuse algfailis, väljastamaks originaalist erinevuse korral teistsuguse kontrollväärtuse. Kõnealuses uurimuses koosnes valim 6175 andmefailist, milleks olid erinevat liiki digitaalsed tõendid.[99]

Kõigile eeltoodud originaalfailidele loodiesialgne kontrollväärtus nii MD5 kui ka SHA-1 räsifunktsioonide abil, mis dokumenteeriti. Pärast esmaste kontrollväärtuste loomist

[99] V. Schmitt, J. Jordaan. Establishing the Validity of MD5 and SHA-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in these Algorithms. International Journal of Computer Applications (0975 – 8887) Volume 68– No.23. 2013, lk 42-43.

modifitseeriti iga faili esimest baiti kasutades tarkvararakendust *hex editori.*[100] Seejärel koostati iga modifitseeritud faili kohta uus MD5 ja SHA-1 kontrollväärtus. Failide modifitseerimise järel kontrollväärtuse taastati failide algväärtuses, mille alusel genereeriti uued kontrollväärtused.[101]

Uurimistöö tulemusena leiti, et esimese muudatuse järel erinesid originaalfailide ja modifitseeritud kontrollväärtused üksteisest olulisel määral. See näitas, et kasvõi ühe baidi suuruse muudatuse tulemusena muutub faili algstruktuur sellisel suurel määral, et räsifunktsioonide abil väljastatakse originaalist erinev kontrollväärtus.[102]

Kui muudetud fail taastati algsesse seisu ning muudetud failidele kalkuleeriti uued kontrollväärtused, vastasid muudetud failidele genereeritud kontrollväärtused nendega, millised olid digitaalsete tõendite originaal kontrollväärtused. [103]

Võttes arvesse, et eeltoodud eksperimendi valimiks oli 6175 faili ning eksimisprotsent originaal ning- duplikaatfailide kontrollväärtuste loomisel oli olematu, võib kindlal teadmisel põhineva kindlusega väita, et tegemist on teaduslikult valiidsete vahenditega tuvastamaks digitaalsete tõendite terviklikkust.

Seega, digitaalsete tõendite kasutamisel tõendite terviklikkuse säilitamise puhul on räsifunktsioonide SHA-1 ja MD5 kasutamine efektiivne ning usaldusväärne vahend. Räsifunktsioonide kasutamisel on hõlpsasti tuvastatav olukord, mil uurija või keegi kolmas isik on algtõendeid manipuleerinud. Tuginedes eeltoodule, võimaldavad räsifunktsioonid nii uurimise kui ka kohtumenetluse käigus tuvastada, kas tegemist on samade failidega, mis varasemalt on tuvastatud ning töödeldud.

2.4.3. Digitaalsete andmete taastamine

Andmete taastamisele viidatakse kui protsessile taastamaks andmeid osaliselt või täielikult hävinud, rikutud või juurdepääsmatult andmekandjal. Protseduur võib olla vajalik põhjustatud

[100] Programm, mis võimaldab manipuleerida arvutifailide binaarandmeid.
[101] V. Schmitt, J. Jordaan. Establishing the Validity of MD5 and SHA-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in these Algorithms. International Journal of Computer Applications (0975 – 8887) Volume 68– No.23. 2013, lk 42-43.
[102] Samas, lk 43.
[103] Samas, lk 43.

andmekandja füüsilisest kahjustatusest, nt CD-plaat on kriimustatud või kõvaketaste mehaanilised kahjud või failidele tuginevale kahjule.[104]

Digitaalkriminalistikas erineb andmete taastamine võrreldes tavaliste arvutiteadustega eelkõige kahe aspekti poolest. Esmalt, andmete taastamise eesmärk on luua digitaalsed tõendid, mida kasutatakse kohtumenetluses. Seega peavad kõik toimingud olema läbi viidud valideeritud ja kinnitatud töövahenditega ning kõik protseduurid peavad olema dokumenteeritud. Teiseks, digitaalkriminalistika on andmete taastamise valdkond oluliselt laiem ning problemaatilisem, hõlmates ka peidetud andmeid ning andmeid jälgede kohta.[105]

2.5. DIGITAALKRIMINALISTIKA EESTIS

2.5.1. Digitõendite kogumine kohtueelses menetluses

Prokuratuuriseaduse [106] (edaspidi ProkS) § 1 järgi on prokuratuur Justiitsministeeriumi valitsemisalas olev valitsusasutus, mis tegeleb kuritegude tõkestamiseks ja avastamiseks vajaliku jälitustegevuse planeerimises, juhib kohtueelset kriminaalmenetlust, tagades selle seaduslikkuse ja tulemuslikkuse, esindab riiklikku süüdistust ning täidab muid seadusega prokuratuurile pandud ülesandeid.

Tuginedes eeltoodud sättele, on prokuratuuri ülesandeks mh kohtueelse kriminaalmenetluse juhtimine. KrMS[107] § 211 lg 1 järgi on kohtueelse menetluse eesmärk koguda tõendusteavet ja luua kohtumenetluseks muud tingimused. Sama õigusakti § 213 sätestab prokuratuurile kohtueelse menetluse juhtimise kohustuse, mis mh hõlmab endas ka järelvalvet uurimisasutuste üle ning vajadusel menetlustoimingute tegemist.

Seega tegelevad digitaalsete tõendite kogumise ning uurimisega algastmes prokuratuur, sh uurimismenetlust läbi viivad uurijad. Eestis puudub uurimisasutuse tasandil regulatsioon spetsiaalselt digitaalsete tõendite, kui tõendite eriliigi, uurimiseks ja kogumiseks loodud stuktuuriüksuste või erialaspetsialistide väljaõppe kohta.

[104] Guo Y., Slay J. (2010) Data Recovery Function Testing for Digital Forensic Tools. In: Chow KP., Shenoi S. (eds) Advances in Digital Forensics VI. DigitalForensics. IFIP Advances in Information and Communication Technology, vol 337. Springer, Berlin, Heidelberg. 2010, lk 299-300.
[105] Samas, lk 300.
[106] Prokuratuuriseadus – RT I, 28.12.2017, 13
[107] Kriminaalmenetluseseadustik – RT I,05.12.2017, 8

2.5.2. Eesti Kohtuekspertiisi Instituudi Infotehnoloogia osakond

Eestis tegeleb digitaalsete tõendite analüüsimise ning ekspertiisi läbiviimisega Eesti Kohtuekspertiisi Instituut (edaspidi EKEI). Eesti Kohtuekspertiisi Instituudi põhimäärus[108] (edaspidi EKEI määrus) on kehtestatud kohtuekspertiisiseaduse[109] (edaspidi KES) § 8 lõike 1^1 alusel. Magistritöö kirjutamise hetkel kehtiv redaktsioon jõustus 01.07.2016. a.

EKEI määruse § 8 punkti 1 järgi teeb instituut kohtu, prokuratuuri, uurimisasutuste ja väärteo kohtuvälise menetleja määruse alusel või haldusorgani taotlusel kohtuarstlikke, kohtubioloogia-, kohtukeemia-, kohtupsühhiaatria-, ja kriminalistikaekspertiise ning seaduse või riigiasutustevahelise kokkuleppe alusel oma pädevusvaldkonnas muid ekspertiisivaldkondadega seonduvaid uuringuid, mida võimaldavad instituudi personali eriteadmised ning tema käsutuses olevad seadmed ja vahendid.

Õigusakti § 9 p-s 5 sätestatakse mh kriminalistikaekspertiiside läbiviimise võimalus. EKEI määruse[110] § 10 punkti 8 järgi teostab instituut infotehnoloogiauuringuid.

Eesti Kohtuekspertiisi Instituudil jaotatakse strukturaalselt osakondadeks ning talitusteks, tulenevalt EKEI määruse § 11 lõikest 1, lõike 3 kohaselt kuulub instituudi koosseisu mh ka dokumendi-, ja infotehnoloogiatalitlused. Määruse § 12 lõike 1 p 3^1 alusel on infotehnoloogiaosakonna põhiülesandeks kujutise töötluse, infotenhnoloogia- ja hääleekspertiiside ning –uuringute tegemine.

Justiitsministri määruse „Riiklikus ekspertiisisasutuses tehtavate ekspertiiside loetelu[111] § 5 lg 3 p 1 ja 2 alusel on infotehnoloogiaekspertiisi alaliigid alaealiste seksuaalse väärkohtlemisega seonduva materjali infotehnoloogiakspertiis ning radaridetektoriiekspertiis.

EKEI infotehnoloogia osakonda kuulub 01.02.2018. a. kinnitatud määruse alusel 1 osakonnajuhataja, 8 eksperti ning 1 juhtivspetsialist. [112] Võttes arvesse asjaolu, et kohtuekspertiisi läbiviimiseks on vajalik menetleja määrus tuginedes tõendamisvajadusest[113], on autori hinnangul EKEI Infotehnoloogia osakonna koosseis piisavalt suur digitõendite efektiivseks menetlemiseks.

[108] Eesti Kohtuekspertiisi Instituudi põhimäärus – RT I, 06.02.2015, 3
[109] Kohtuekspertiisiseadus – RT I,30.12.2015, 21
[110] Eesti Kohtuekspertiisi Instituudi põhimäärus – RT I, 06.02.2015, 3
[111] Justiitsministri määrus „Riiklikus ekspertiisiasutuses tehtavate ekspertiiside loetelu“ – RTL 2008, 9, 112.
[112] Eesti Kohtuekspertiisi koosseis, 01.02.2018. kinnitatud. Kättesaadav veebiaadressil: http://www.ekei.ee/sites/www.ekei.ee/files/elfinder/dokumendid/ekei_koosseis_01.02.2018.pdf
[113] KrMS § 105 lg 1 järgi korraldatakse ekspertiis tõendamisvajadusest lähtudes menetleja määruse alusel.

Eesti Kohtuekspertiisi Instituut on väljastanud infovoldiku [114], milles mh sätestatakse organisatsiooni ajalugu, eesmärgid, ülesanded ning spetsiifiliste osakondade põhiülesanded.

Infotehnoloogia osakonnas on võimalik teostada menetleja poolt ette antud märksõna-, kirjavahetuse-, dokumendi- ja failiotsinguid uuringuks esitatud arvutitest ning nendega seotud andmekandjatest (kõvakettad, CD/DVD-plaadid, flopikettad, mälupulgad ja –kaardid). Lisaks eeltoodule on võimalik uurida ka muid, menetlusasjas olulist infot sisaldada võivaid digitaalseid- või elektroonikaseadmeid.[115]

Infotehnoloogia uuringute ja ekspertiiside peamine uurimisobjekt on andmekandjad, millest levinumad on kõvakettad, mis paikenevad personaalarvutites ja sülearvutites, aga ka paljudes eriotstarbelistes seadmetes (arvutites) nagu turvavideo salvestusseadmed, kõvakettaga DVD-salvestud, mängukonsoolid jne.[116]

Ekspertiisi seisukohast on EKEI jaoks esmatähtis seadme mälus olev informatsioon. Lisaks andmekandjate uurimisele tegeleb infotehnoloogia osakond ka videosalvestiste või digitaalkujutistega seotud küsimustes kujutiseekspertiisi teostamise vormis. Kujutiseekspertiis sisaldab endas näiteks eriformaadis videosalvestiste konvertimist, töötlemist ja kvaliteediparandust, videosalvestiste mahamängimisega seotud probleemide lahendamist, kaadrite väljavõtmist, digitaalkujutistega seotud küsimustele vastamist, menetlusasjaga seotud pildi- ja videofailide otsingut esitatud andmekandjatest ja seadmetest.[117]

Teise eriliigina teostab organisatsioon hääleekspertiisi (erandjuhtudel ka uuringuid). Ekspertiisiliik tegeleb salvestise autentsuse uurimisega, salvestiste kvaliteedi „parandamisega“, st taustamüra, telefonihäirete, raadiohäirete, isegi aeglase muusika, tänavamüra jhms eemaldamist eesmärgiga muuta salvestisel kostuv kõne võimalikult kuulajasõbralikuks ja arusaadavamaks ning teksti transkribeerimisega ehk salvestise üleskirjutusega ja kõneleja tuvastamisega.[118]

---

[114] Eesti Kohtuekspertiisi Instituudi infovoldik, lk 4. Arvutivõrgus kättesaadav: https://www.google.ee/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0ahUKEwi8npTouvPZAhVlM5oKHSBdBnEQFghKMAM&url=http%3A%2F%2Fwww.ekei.ee%2Fsites%2Fwww.ekei.ee%2Ffiles%2Felfinder%2Fdokumendid%2Fekei_voldik_0.pdf&usg=AOvVaw2TJEm-2nvoHc0xf-cOp1iP (viimati külastatud: 23.04.2018).

[115] Samas, lk 4.

[116] Samas, lk 4.

[117] Samas, lk 4.

[118] Samas, lk 4.

3. DIGITÕENDID KUI METAANDMED JA VAHETUD TÕENDID

3.1. METAANDMED ARVUTISÜSTEEMIDES

Metaandmed on andmed, mis sisaldavad teavet muude andmete kohta. See on teave, mis tekib siis, kui kasutatakse erinevaid infotehnilisi lahendusi ja -süsteeme ning mis annab teada, kes, mida, kus, millal ja kuidas tegi. Metaandmed tekivad ja talletatakse teenuste tarbimisel ja IT-protsesside käivitamisel mitmes erinevas punktis ning erinevatel tehnilistel tasemetel: a) kasutaja enda arvuti; b) organisatsiooni kohtvõrgu administreerija; c) andmesides osalevad võrguseadmed; ning d) internetiteenuste osutaja jpt.[119]

Metaandmeid nimetatakse enamasti teabeks elektroonilise või digitaalse salvestise kohta, ent metaandmete mõiste on kahtlemata laiem. Näiteks on metaandmete töötlemine (st talletamine ja analüüsimine) vajalik ka infoturbe seisukohast, võimaldades tuvastada ründeid andmesidevõrgu ja selle kasutajate vastu.[120]

Metaandmetena on käsitetavad eelkõige faili asukoht, suurus, loomise aeg ning juurdepääsukontroll, mida salvestatakse metaandmetena. Eeltoodud andmed võimaldavad teha kindlaks mitmeid erinevaid kuriteos kriitilisi tehiolusid, näiteks motiiv, kuriteo toimepanemise aeg, dokumentide loomise aeg, autor, ajalugu ja eesmärk.[121]

3.1.1. Failisüsteemid

Failisüsteem on meetod hoiustamaks ning organiseerimaks arvutifaile ja andmeid, mida need sisaldavad, tehes failide leidmise ning juurdepääsu kasutajale lihtsamaks.[122] Failisüsteemid pakuvad võimalust juurde pääseda spetsiifilisetele andmete, mida mingil konkreetselt kõvakettal hoiustatakse. Fail on nimetatud kollektsioon seostuvatest andmetest, mille abil organiseeritakse sekundaarset teavet ehk metaandmeid.[123]

[119] Andmekaitse Inspektsioon. Metaandmed ja privaatsus. Juhis organisatsioonidele ja kodukasutjatele seaduse rakendamisel. 28.10.2015, lk 4.
[120] Samas, lk 4.
[121] K. L. Rusbarsky. A Forensic Comparison of NTFS and FAT 32 File Systems. Marshall University Forensic Science Center. Kansas City, 2012, lk 3.
[122] Lucio D. Jasio. Programming 16-bit PIC Microcontrollers in C: Learning to Fly the PIC 24. Newnes. Burlington, MA. 2007, lk 284.
[123] Association of Cerfitied Fraud Examiners. Investigating by Computer. Second edition. 2002, lk 159.

Microsoft Windowsi operatsioonisüsteemi puhul on populaarsemateks failisüsteemideks FAT failisüsteemid (ingl k. *file allocation table)*: FAT 12, FAT 16 ja FAT 32. Olgugi, et tegemist on võrdlemisi vanade failisüsteemidega, kasutatakse neid siiski paljude andmekandjate korral, nt digikaamerate mälukaartides ja mobiiliseadmetes. Tegemist on äärmiselt levinud ning struktuurilt lihtsate failisüsteemidega, mistõttu on FAT-failisüsteemid digitaalkriminalistide jaoks heaks alguspunktiks failisüsteemide ning kustutatud andmete analüüsimiseks.[124] Teiseks levinud failisüsteemiks on NTFS failisüsteemid (ingl. k. *New Technology File System)*, mis omadustel on keerulisem kui FAT failisüsteem ning oluliselt komplitseerituma struktuuriga.[125]

1. FAT failisüsteemid

FAT failisüsteemid kasutavad failide ja kaustade organiseerimiseks loendeid ning failijaotustabeleid. Tüvifail (näiteks C:\) on failisüsteemis kindlaks määratud asukohas, seega operatsioonisüsteem teab, kust seda leida. Kaust sisaldab endas nimekirja failidest ja alamkataloogidest, mis süsteemis asetsevad.[126]

FAT failissüsteem koosneb neljast erinevat sektorist. Esiteks reserveeritud sektor, mis hõlmab ala, mida kutsutakse BIOS [127] parameetri blokiks ja tavaliselt sisaldab endast operatsioonissüsteemi laadurkoodi. Teiseks, FAT regioon, mis ladustab reeglina kahte koopiat FAT tabelitest. Kolmas osa koosneb juurkataloogi regioonist, mis ladustab informatsiooni andmete ja kataloogide kohta. Viimane osa on andmete regioon, kus hoiustatakse failissüsteemis leiduvaid metaandmeid. [128]

Tuginedes FAT failisüsteemide struktuurile on kõige enam metaandmeid võimalik leida just juurkataloogi ning metaandmete regioonist.

2. NTFS failisüsteemid

[124] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 514.
[125] Samas, lk 519.
[126] Samas, lk 514-515.
[127] Baasvahetussüsteem (BIOS) on personaalarvuti riistvara kontrollimiseks mõeldud madala taseme tarkvara, mis toimib liidesena riistvara ja operatsioonisüsteemi vahel.
[128] Association of Cerfitied Fraud Examiners. Investigating by Computer. Second edition. 2002, lk 160

NTFS failisüsteemid, nagu eelnevalt mainitud, on oluliselt erinevad FAT failissüsteemidest, säilitades failisüsteemi informatsiooni mitmete erinevate süsteemide abil, näiteks kasutades peamist failitabelit (ingl keeles *Master File Table ehk $MFT),* mis toetab paremini suuremahulisi kettaid. Lisaks võimaldab failisüsteem efektiivsemat andmete kaitsmise meetodit, kasutades juurdepääsu kontrollnimekirja (ingl. k. *Access Control List* ehk *ACLs*).[129] Teiseks, võimaldavad NTFS failisüsteemid paremat toetust metaandmete kogumisele ning edasiarenenumat andmete struktuuri, tõstes failisüsteemi jõudlust, usaldusväärsust ning kõvaketta ruumi kokkuhoidu.[130]

NTFS on disainitud pidades silmas kõige halvemaid stsenaariume, eelkõige olukorda, mil failisüsteemi on vaja taastada.. Eeltoodu rakendamiseks luuakse failisüsteemist mitu koopiat, mida on võimalik taastada.[131]

NTFS-failisüsteemid, analoogselt FAT-failisüsteemidele sisaldavad hulganisti metaandmeid, ent tuginedes keerukamale struktuurile võib digitaalkriminalistidel olla komplitseeritum eeltoodud andmeid tuvastada, koguda ning fikseerida. Võttes arvesse NTFS-failisüsteemide ettevaatusabinõusid, võimaldab failisüsteem uurijatel lihtsamalt taastada ning tuvastada kustutatud andmeid.

3.1.2. Logifailid

Logifailid suudavad salvestada andmeid selle kohta, milline konkreetne kasutaja omas ligipääsu mingiste süsteemi konkreetsel ajal. Operatsioonisüsteemide kasutajatele kõvakettale juurde pääsemiseks kaks meetodit - interaktiivne juurdepääs ning juurdepääs arvutisüsteemi avatud ressurssidele. Mõlema puhul on tõenäoline kahtlusaluste ring märkimisväärselt suurendatud. Juhul, kui arvutist leitakse illegaalset materjali, on indiviidid, kellel oli juurdepääs arvutile, kaheldamatult konkreetses uurimises kahtlusalune. Reaalsuses eksisteerib võimalus, et tegelikkuses omandas keegi kolmas isik autoriseerimata juurdepääsu arvutisüsteemile ning ladustas illegaalsed materjalid kõvakettale.[132]

Süsteemilogid omavad informatsiooni selle kohta, milline arvuti kasutaja oli süsteemi sisse loginud hetkel, mil kuritegu sooritati, mh asjaolu, kas kasutajale omandas loata juurdepääsu

[129] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 519.
[130] Association of Cerfitied Fraud Examiners. Investigating by Computer. Second edition. 2002, lk 161.
[131] Samas, lk 519.
[132] Samas, lk, 535

keegi kolmas isik. Lisaks sisaldavad süsteemilogid informatsiooni selle kohta, kas arvutis olevat informatsiooni on salvestatud CD-le või DVD-le, arvutisse on sisestatnud eemaldatavat USB-seadet või manipuleeritud süsteemi sisse ehitatud ajaseadet.[133]

3.1.3. Registrifailid

Windowsi süsteemiregister on tsentraalne andmebaas, mis hoiustab sätteid ja konfiguratsioone, mis on vajalik operatsioonisüsteemi ning programmide opereerimiseks mingis konkreetses arvutissüsteemis. Süsteem ja selle kasutavad rakendused ja riistvara kasutavad registrifaile ladustamaks konkreetseid sättedetaile. Registrifailidest võib leida andmeid kasutaja e-maili, veebilehtede ja programmide salasõnade ja kasutajatunnuste kohta, külastatud internetilehekülgi koos külastuse ajaga, otsingumootoritesse sisestatud otsinguid, hiljutist failitegevust, loetelu arvutisse installeeritud tarkvarast, viimaseid õnnestunud ja ebaõnnestunud süsteemi sisselogimisi, eemaldatavate andmekandjate loetelu jne.[134]

Windowsi operatsioonisüsteemid kasutavad süsteemiregistrit (ingl. k. *system registry),* ladustamaks süsteemi konfiguratsione ning kasutamise detaile, mida kutsutakse võtmeteks (ingl. k. *keys).* Registrifailid ehk tarud Windowsi 95 ja Windowsi 98 puhul asetsevad Windowsi installatsioonikaustas ning kannavad nime "system.dat" ja "user.dat".[135]

Registrifaile, mis süsteemist taastatakse tõendusmaterjali tarbeks, on võimalik vaadata kasutades spetsiaalset *regedt32* käsklust süsteemi registrimenüüst. Registrifaile on võimalik töödelda kasutades erinevaid tarkvaraprogramme, nt EnCase ja FTK.[136]

Registrifailidest on uurijatel võimalik omandada oluliselt suures koguses informatsiooni, mis võivad omandada digitaalse tõendi väärtuse.

[133] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 536
[134] Association of Cerfitied Fraud Examiners. Investigating by Computer. Second edition. 2002, lk 167
[135] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 537
[136] Samas, lk 518.

3.2. METAANDMED INTERNETIS

Asjade internet (ingl. k. *Internet of Things)* kirjeldab maailma, kus paljud tavapärased seadeldised on unikaalselt identifitseeritavad, adresseeritavad ning ühendatavad läbi interneti. Sellised „asjad“ võivad olla rohkem kui sensori või täiturmehhanismiga uuendatud.[137]

Interneti kasutamine jätab arvutisse ning teenusepakkujatele hulganisti informatsiooni, sh külastatud veebilehed, sisu, mida kuvati ja uudistegrupid. Muuhulgas salvestavad mõningad operatsioonisüsteemid logi sellest, kuna ja milline arvutikasutaja internetti on kasutanud, arenenumad operatsioonisüsteemid logivad ka seda, millal on modemi või sissehelistamissüsteemi abil internetti sisse logitud.[138]

3.2.1. Veebibrauserid

Olukorras, mil isik külastab esimest korda mingit veebilehte, salvestab veebribrauser kõvakettale nii külastatud lehe kui sellega seonduvad kriitilised elemendid. Lisaks eeltoodudule registreeritakse salvestise loomise aeg ja muudatuste logi. Juhul, kui sama veebilehte külastatakse uuesti, kasutab arvutisüsteem juba salvestatud vahemälu salvestist. Mõningad veebibrauserid salvestavad konkreetsete veebilehtede külastamise arvu, luues brauserisisese andmebaasi. [139]

Firefox 3 säilitab databaasi külastatud veebilehtedest *SQLite*[140] abil faili, mille nimi on „Places.sqlite. Internet Explorer kasutab andmete hoiustamiseks faili nimega „index.dat“. Andmebaas sisaldab endas hulganisti informatsiooni, mh loetelu veebilehtedest, mida külastati ning otsingumootori ajalugu ning -detaile. Informatsiooni ekstraheerimiseks „index.dat“ ja muudest logifailidest on loodud mitmeid avatud lähtekoodidega programme.[141]

Veebribrauserid ladustavad ajutisi internetifaile vahemälu kaustas (ingl. k. *cache*), mis võimaldavad kasutajale lihtsama juurdepääsu tihedalt külastatud veebilehtedele. Vahemälu kaustad sisaldavad fragmente veebilehtedest, mida on hiljuti vaadatud, sisaldades

[137] D. Ryan and G. Shpantzer. Legal aspects of Digital Forensics. The George Washington University. Washington, D.C., USA. 2002, lk 3.
[138] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 538.
[139] Samas, lk 540-541
[140] SQlite on relaktsioonandmebaasi süsteem, mis salvestab külastatud veebilehtede andmeid.
[141] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 540-541

informatsiooni nii teksti- kui ka pildiformaadis.[142] Ajutised internetifailid laetakse alla koheselt, kui kasutaja külastab mingit veebilehte. Kustutatud internetifaile on võimalik taastada jaotamata ruumi sektsioonist kõvaketta failisüsteemist.[143]

Isegi kui ajutised failid on kustutatud, on neid võimalik taastada paljastamaks märkimisväärset informatsiooni, sh veebipõhised e-mailid (nt *Hushmail.com*), interneti ostude ajalugu (nt *Ebay.com* ja *Amazon.com*), finantstehingud (nt online-pangandus ja *Paypal.com*), reisimarsuudid (nt *Expedia.com*) jpm.[144]

Mõned veebibrauserid salvestavad indiviidi veebilehtede külastused ja huvid luues „küpsiste" faili. Näiteks, *Amazon.com* kasutab küpsistefaile selleks, et jälgida indiviivi ostude ajalugu ja luua parema mõistmise sellest, millised on tema huvid, võimaldamaks veebilehel soovitada muid tooteid, mis võiks talle huvi pakkuda. Netscape salvestab küpsised faili „cookies.txt" ja Internet Explorer säilitab küpsiseid „Windows\Cookies" kaustas. Iga salvestus sisaldab informatsiooni selle kohta, mis võib tulla uurimisel kasuks. Näiteks, võimaldavad „küpsisefailid" tuvastada indiviidi otsinguajalugu.[145]

Märkimist on väärt, et küpsisefaili olemasolu ei ole iseenesest tõend selle kohta, et indiviid tahtlikult veebilehele juurde pääääses. Näiteks, kasutavad mõned reklaamid küpsistefaile, luues viiteid reklaamitavale lehele juurde pääsemisest isegi siis, kui tegelikkuses eeltoodud veebilehtede ei külastanud. Lisaks, võib mõningatel juhtudel veebibrauser automaatselt kasutaja ümber suunata mitmetele veebilehtedele, luues kettale küpsisefaile ja sissekandeid veebilehekülje andmebaasi , isegi kui isik eesmärgiks ei olnud veebilehekülgi külastada.[146]

3.2.2. Uudisteserverid

Lisaks kõikide juurde pääsetud internetilehtede aadressidele salvestavad veebibrauserid andmeid selle kohta, milliseid uudisteservereid on indiviid külastanud. Näiteks salvestab Netscape´i uudistelugeja informatsiooni faile „.rc" laiendiga, näiteks „news.rc". [147]

[142] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 541.
[143] Association of Cerfitied Fraud Examiners. Investigating by Computer. Second edition. 2002, lk 167
[144] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 541.
[145] Samas, lk 541.
[146] Samas, lk 542.
[147] Samas, lk 542.

Uudisteserverid (ingl. k. *usenet*) on seletatavad kui globaalsed, detsentraliseeritud ning jaotatud interneti arutelusüsteemid, mis utiliseerivad kommunikeerimiseks võrguaja protokolli ehk NNTP protokolli (ingl. k. *Network Time Protocol*). [148]

Kasutades UUCP protokolli [149] (ingl. k. *Unix to Unix Copy Protocol)* ja modemiülest ühendust, leiab enamus võrguaja vahendusel toimuvat suhtlemist aset internetis. Võrguaja protokolli kasutatakse uudisteartiklite jagamiseks, päringute tegemiseks, leidmiseks ja postitamiseks. Põhimõtteliselt on tegemist „lae üles ja edasta" tüüpi süsteemiga, mis on sarnane standardsele e-mailide edastamise meetodile. Lihtne meiliedastusprotokoll ehk SMTP (ingl. k. *Simple Mail Transfer Protocol*) sisaldab endas ühte või mitut unikaalset e-maili aadressi, spetsifitseerib võrguaja protokoll mingi kindla uudiste sihtgrupi. Seega, üks konkreetne sõnum postitatakse ühe serveri vahendusel ning seda on võimalik kopeerida tuhandetesse erinevatesse sihtserveritesse.[150]

Nagu ka tavaliste e-mailide puhul, on ka võrguaja protokolli abil võimalik edastada saadetud sõnumitega erinevaid binaarseid manuseid (nt ZIP failid, MP3 muusikafailid, GIF ja JPG fotofailid). [151]

Levinud meetod uudisteserverite süsteemidest andmete leidmiseks on kasutada NZB faile. NZB fail on XML-baseeruv failiformaat tuletamaks informatsiooni võrguaja protokollide serveritest. Formaat loodi *Newzbin.com* veebilehe loojate poolt ning on efektiivne, kui andmeid otsitakse otsingupõhistest veebilehekülgedelt. Taolised veebilehed võimaldavad teha väljavõtteid erinevate failide allalaadimisi, luues NZB faile. [152]

Uudisteserverite iseloomust tulenevalt on võimalik välja tuua järgmised problemaatilised aspektid:[153]

- Interneti anonüümsus. Tuginedes faktile, et identifikatsiooni andmeid (näiteks väljavõtte päis) on väga lihtne muuta, on tõenäoliselt vajalik esitada päring uudisteserveri võõrustajale, omandamaks logifaile konkreetse postituse autori kohta. Sealjuures pole kindel, kas eeltoodud logifailid on säilitatud või mitte. Paljudel juhtudel on uudisteserverite loojad kohustatud andmekaitse regulatsioonidest tulenevalt salastama või mitte hoiustama eeltoodud informatsiooni, sh ei ole

[148] M. Lachiniet, C. Hornat. A forensic Primer for Usenet Evidence. SANS Institute, 2006, lk 5.
[149] UUCP protokoll tähendab Unixist Unixisse kopeerimise protokolli. Eelkõige kasutatakse protokolli e-kirjade ja uudisegruppide jutulõimekirjade liigutamiseks.
[150] M. Lachiniet, C. Hornat. A forensic Primer for Usenet Evidence. SANS Institute, 2006, lk 5.
[151] Samas, lk 5.
[152] Samas, lk 21.
[153] Samas, lk 27-28.

kohustatud teostama järelvalvet selle üle, kas kasutajad edastavad legaalset või illegaalset materjali.

- Volatiilsus. Uudisteserverite andmed, eriti binaarsed allalaadimised, on suuremahulised. Paljusid logisid hoiustatakse vaid ajutiselt, kuivõrd eeltoodud hõlmavad suure osa serverite mahust.
- Andmete leidmise problemaatika. Paljud andmed, ilma eksisteeriva failisüsteemi metaandmete olemasoluta, on äärmiselt raskesti leitavad, kuivõrd failide päised ei ole järjepidavad. Sisuliselt on võimalik luua andmete leidmiseks tarkvaraprogramm, mis võib analüüsida postituste pealkirja ning sisu[154], ent taolise programmi loomine võib olla infotehnoloogiliselt äärmiselt keeruline.
- Andmete analüüsimise problemaatika. Uudisteserverites leiduvad andmed võivad olla peidetud ja uurijale tundmatus failiformaadis. Näiteks, lihtne filmifail võib olla konventeeritud mitmeosalisse *.rar* failformaati, mis omakorda on teisendatud *.par* failiks, mis omakorda teisendatud *yEnc* formaati. See tähendab uurijatele täiendavat lisatööd saamaks aru, kokku sobitama ning seletama leitud informatsiooni sidusal moel.

Eeltoodud põhjuste tõttu on uudisteserverite kasutamisest tulenevaid seaduserikkumisi on digitaalsetel uurijatel väga keeruline tuvastada, mistõttu on uudisteserverite kasutamine väga populaarne vahend edastamaks illegaalseid faile.[155]

3.2.3. E-mailid

Internetis kujutavad e-mailid endast ühte kõige tavalisemat kommunikatsioonivahendit. Uuringute kohaselt koostatakse ja saadetakse iga päevaga rohkem e-kirju, kui inimesed teevad telefonikõnesid või koostavad paberdokumente. E-mailide ning neid edastavate programmide analüüs on olnud digitaalse uurimise keskseks nii tsiviil- kui ka kriminaalasjades. Tihtipeale tulenevad just e-mailidest tõendid, mis omavad kriminaalasjas süüdistavat funktsiooni ning uurimine ei ole täielik ilma e-mailide leidmiseks päringute esitamise, meilibokse läbi otsimata ega organiseerimata.[156]

[154] Vt. Peatükk 3.1.
[155] M. Lachiniet, C. Hornat. A forensic Primer for Usenet Evidence. SANS Institute, 2006, lk 27.
[156] L.Qian, F. Höglin, P. A. Diaz. Computer Forensics. Uppsala University, 2007, lk 5.

Tähtis on välja tuua, et käesoleva töö raames on võimalik e-mailidest tuletada ka digitõendeid nende standardtähenduses, st olukorda, mil e-mail ise sisaldab informatsiooni, mis on kriminaalmenetluses kriitiliste asjaolude tuvastamiseks oluline. Eelkõige on silmas peetud e-kirjas või selle manuses seisnevat informatsiooni, olgu selleks sõnumi sisu või manustatud illegaalne foto. Käesolev alapeatükk keskendub informatsioonile, mida on võimalik tuletada andmetest andmete kohta ehk e-mailide metaandmete kohta.

E-mailidest on võimalik tuletada palju erinevat informatsiooni, alustades selle saatjast, vastuvõtjast, saatmise ajast, manustest ning sellest, kuna e-maili on loetud. E-maile on võimalik leida nii arvutist, kust see väljastati, arvutist, mille kaudu see vastu võeti ja erinevatest serveritest, mis e-maili vahendasid, ning samuti serverist, mis koostas saadetud e-mailist koopiaid.[157]

E-maile edastavad ja vastu võtvad programmid sisaldavad sõnumeid, mis on saadetud ja vastu võetud konkreetsest arvutist. Netscape ja Eudora veebibrauserid ladustavad e-maile tavaliste tekstifailidena, Microsoft Outlook, Outlook Express, IBM Lotus notes, Novel GroupWise ja America Online (AOL) kasutavad patendeeritud spetsiaalseid failiformaate, mis nõuavad juurdepääsemiseks eriomaseid programme. Isegi, kui e-mail on salvestatud tavalise tekstifailina, on sellele juurde pääsemiseks vaja dekodeerida šifreeritud sõnumite manuseid.[158]

Levinud on arvamus, et kustutatud e-kirju ei ole võimalik taastada. Küll aga on enamus juhtudel võimalik digitaalkriminalistiliste võtetega taastada kasutajate e-maili programmide ning e-maili serverite abil kustutatud e-kirju. E-mailid võivad jätkuvalt paikneda vahendusserverites või tagavarakoopiatena teenusepakkuja serverites. Lisaks on võimalik e-kirju taastada kõvakettalt või serverist.[159]

Samu võimalusi pakuvad ka erinevad veebirakendustel põhinevad e-kirjade postkastid nagu näiteks Hotmail, Gmail ja Yahoo Mail. Programmid kasutavad veebibrauserid võimaldamaks kasutajal suhelda vahendusserverite abil. Brauser edastab informatsiooni süsteemisisesele kõvakettale, mis salvestab e-kirjast koopia. Digitaalkriminalistikaliste võtetega on võimalik välja võtta HTML failiformaadil baseeruv e-mail, mis on salvestatud kõvakettale.[160]

[157] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 543.
[158] L.Qian, F. Höglin, P. A. Diaz. Computer Forensics. Uppsala University, 2007, lk 5.
[159] Samas, lk 5.
[160] Samas, lk 5.

3.2.4. Muud rakendused

Yahhoo Pager, AOIM ja muud kiirsõnumi saatmise rakendused ei hoiusta vaikimisi saadetud sõnumite arhiivi, kuid neid on võimalik seadistada logimaks vestluste seansse. Erinevad failijagamisprogrammid võivad hoiustada nimekirja võõrustajatest, kes on jaganud või juurde pääsenud jagatud failidele, ent eeltoodud teave sisaldab võrreldes muude tõenditega vähe informatsiooni.[161]

IRC ja muud internetipõhised vestluskanalite rakendused sisaldavad reeglina rohkem logisid, kuid vaid juhul, mil kasutaja otsustab need salvestada. Seega, jäljed muudest rakendustest on tõenäolisemalt inimese andmekandjate kõvakettal kui internetis. Parim informatsiooni kogumise viis muude rakenduste puhul on otsida faile meediakandjatelt, kuhu andmed on ajutiselt hoiustatud või jälgida internetikasutust ajal, mil ta neid programme kasutab.[162]

3.2.5. Internetis failide hoiustamine

Oluline osa kriminalistilisest ekspertiisist on identifitseerida erinevaid ebatõenäolisi asukohti, kus digitõendeid võib leida. Kannatanu võis võõrustada veebilehte või kurjategija võis üle kanda süüdistatavat informatsiooni ühest arvutist teise interneti vahendusel. [163]

Üks tavalisemaid kaugladusatamise asukohti on indiviidi internetipakkuja (ingl. k. *Internet Service Provider ehk ISP*) poolt pakutavates hoiustamisruumides. Lisaks e-mailide ladustamisele, võimaldavad mõningad ISP-d täiendavat ladustamisruumi veebilehtede ja muude andmete jaoks. Faile saab üle kanda eeltoodud andmesüsteemidesse kasutades erinevaid programme nagu näiteks FTP, SecureCRT ja Secure Shell (SHH).[164]

Näiteks, loob WS-FTP logifaile iga kord, kui seda kasutatakse failide ülekandmiseks, luues andmed selle kohta, kus fail asub, märkides lisaks FTP serveri nime ja ülekande kellaaja. SecureCRT ja Secure Shell funktsioone on võimalik konfigureerida säilitamaks isiku konfiguratsioonifaile iga erineva arvuti puhul, mida ta kasutab failide ladustamiseks. Nimekiri süsteemidest, millele on juurde pääsetud, võib olla avalik, kui inimene on valinud võimaluse

[161] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 544
[162] Samas, lk 544.
[163] Samas, lk 544.
[164] Samas, lk 544.

salvestada koopia igast avalikust krüpteerimisvõtmest. Teised programmid kasutavad registrit selleks, et salvestada arvutite nimesid või IP-aadresse. [165]

Lisaks eeltoodule on ladustatakse andmeid jagatud võrgukettal. Paljud Windowsi operatsioonisüsteemi kasutavad arvutid on võimelised tegema kogu kõvaketta või osa sellest saadavaks ka võrgus. Paljud organisatsioonid kasutavad Windowsi failiservereid selleks, et pakkuda kasutajatele sellist tüüpi andmete ladustamise võimalus. Ka personaalarvutid on võimelised eeltoodud funktsiooni kasutama. Rakenduse abil saavad inimesed andmeid ühest arvutist teise kasutada ilma eemaldatavate mälupulkade kasutamiseta.[166]

Loetelu aktiivsetest võrkudes on võimalik leida *HKEY-USERS\sid\Network\Registry* funktsiooni kasutades. Märkimisväärselt, võrgujagamisest lubamine arvutis ei viita ilmtingimata sellele, et kasutajal on võimalik juurde pääseda jagatava kõvaketta andmetele. Seega, juurdepääsuandmete alusel on võimalik tuvastada, kas kasutaja üleüldse on lubatud andmeid kirjutama või isegi lugema antud võrgujagamise funktsiooni sätete kohaselt.[167]

Eeltoodu ei ole kindlasti ammendav loetelu andmete hoiustamiseks. Esineb muid täiendavaid võimalusi andmete ladustamiseks, mis sisaldavad tasuta ruumi mingil kettal. Eeltoodu on võimalik ka internetis, paljud leheküljed pakuvad võimalust andmeid tasuta ladestada. [168]

Enamus andmeladustamise viise on kaitstud salasõna abil. Digitaalkriminalistil ei ole soovitatav andmeladustamise serverisse sisse logida ilma loata, isegi juhul, kui nad teavad salasõna. Näiteks, võib arvuti olla konfigureeritud süsteemi käivitamisel automaatselt ühendama võrguserveriga. Kuigi sellisel viisil on võimalik andmetele juurde pääseda, võib olla tegemist tõendite muutmisega ja väljuda väljastatud loa piiridest.[169]

[165] E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011, lk 544.
[166] Samas, lk 544-545.
[167] Samas, lk 545.
[168] Samas, lk 546.
[169] Samas, lk 547.

3.3. ANDMEKANDJATELT LEITAVAD DIGITAALSED TÕENDID

Andmekandja on igasugune riistvara, mis võimaldab hoiustada või ekstraheerida andmefaile või objekte. See võimaldab hoiustada informatsiooni nii ajutiselt kui ka jäädavalt ning võib olla arvutisse integreeritud- või väline kõvaketas, server või muu sarnane seadeldis.[170]

Esimeses peatükis sätestasime, et digitaalsete tõendite puhul omab tõendusväärtust nii andmekandjatel leitavad andmed kui ka andmetest tuletatavad metaandmed. Käesolev alapeatükk peab silmas andmeid, mis on otseselt tuletatavad digitaalsetest meediaseadmetest.

Juhul, kui digitaalselt andmekandjalt leitavad andmed iseenesest omavad kriminaalasjas tõenduslikku väärtust, puudub vajadus nende edasiseks analüüsimiseks. Näiteks olukorras, mil kahtlustatava arvutist leitakse illegaalset video- või pildimaterjali, on tõendiks kõnealused failid. Sellisel juhul puudub vajadus metaandmete ekstraheerimiseks ning analüüsimiseks ja tõendina on kasutavad failid iseseisvalt.

Eeltoodud tõendite omandamiseks on vajalik saavutada juurdepääs objektiks olevale andmekandjale ning tõendina kasutatav fail ekstraheerida. Tõendi fikseerimise protseduuri kestel on äärmiselt oluline järgida digitaalkriminalistika põhiprintsiipe, omandamaks tõendit kriminaalmenetluse seadustiku tähenduses.

[170] Definition – What does Storage Device mean? Arvutivõrgus kättesaadav: https://www.techopedia.com/definition/1119/storage-device (viimati külastatud: 23.04.2018)

4. DIGITAALSETE TÕENDITE KASUTAMISE PERSPEKTIIVIKUS KOHTUMENETLUSES

4.1. DIGITÕENDITE LUBATAVUS

KrMS on rajatud rangele tõendamismenetlusele ehk lubatud tõendiliikide ammendavale loetelule seaduses (KrMS § 63 lg 1). Iseenesest ei takista eeltoodud säte ka digitaalsete tõendite kasutamist kriminaalmenetluses, kuivõrd kõikvõimalikud tõendamisväärtusega digitaalsed andmed ja vastavad andmekandjad on kvalifitseeritavad mõne antud normis loetletud tõendi liigi alla.[171] Seda seisukohta kinnitab ka Riigikohus, ent reservatsiooniga, mille kohaselt üksnes menetlusliku sisuga asjaolude tõendamiseks on võimalik tugineda täiendavalt erinevatele lubatavatele tõendiliikidele (nn vabatõend).[172]

Seega, et digitaalseid tõendeid oleks üleüldse võimalik kohtumenetluses kasutada, on oluline tuvastada nende lubatavus tuginedes kriminaalmenetluse seadustikule. Eeltoodud seisukohta kinnitab ka Riigikohus[173] leides, et juhul, kui tõendit käsitletetakse kriminaalseadustiku § 63 lg-s 1, on tõend lubatav juhul, kui selle tõendi kogumisel ei ole rikutud menetlusõigust.[174]

Eelmises peatükis sätestatud digitaalsete tõendite liikidest tulenevalt on oluline analüüsida, kas eeltoodud tõendite liigid kvalifitseeruvad KrMS § 63 lg 1 koosseisu, kuivõrd vastasel juhul ei ole nende kasutamine kohtumenetluses lubatud.

Kõigi eeltoodud tõendi liikide puhul ei ole tegemist iseseisvate tõenditega, st digitaalsete tõendite puhul ei pruugi omada tõenduslikku väärtust see objekt ise, vaid tõendi analüüsimisest tulenev informatsiooni. Näiteks, arvutikõvakettal leiduvad metaandmed omandavad tõendi väärtuse juhul, kui analüüside pinnalt tekib põhjendatud kahtlus mingi kuriteo aspektist kriitilise elemendi ilmnemise kohta. Lisaks eeltoodule on oluline, et andmed on fikseeritud tõendi vormis. Erandina võib välja tuua e-kirjad ning andmekandjatel leiduvad tõendid, milles seisnev sisu võib iseseisvalt omandada informatsiooni kuriteo kriitiliste asjaolude kinnitamiseks või ümber lükkamiseks.

---

[171] J. Tehver. Digitaalsete tõendite kasutamise võimaldamine. Mai 2016, lk 2. Arvutivõrgus kättesaadav: https://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf (viimati külastatud: 23.04.2018)
[172] RKKKO 3-1-1-142-05, p 10.
[173] Kõnealuses kohtuasjas arutles RK kõne salvestiste lubatavuse küsimust, mis on kvalifitseeritav muu teabetalletuse liigi alla.
[174] RKKKO, 3-1-1-33-11, p 9

4.1.1 Andmekandjatel asuvad tõendid

Tuginedes andmete kogumise viisile ning analüüsimise meetoditele, on võimalik andmekandjatel asuvad digitaalsed tõendid paigutada eelkõige asitõendi mõiste alla, tuginedes KrMS § 63 lg-le 1.

Eesti õiguskirjanduses on võimalik asitõendi mõiste kokku võtta kui tõendamiseseme asjaolude selgitamisel kasutatav mis tahes asendamatu ese, mis on võetud kriminaalasja juurde.[175] Kriminaalmenetluse seadustiku § 124 lg 1 järgi on asitõend kuriteo objektiks olnud asi, kuriteo toimepanemise vahend, kuriteojäljega asi, kuriteojäljest valmistatud jäljend või tõmmis või kuriteosündmusega seotud muu asendamatu objekt mis on kasutatav tõendamiseseme asjaolude selgitamisel.

Riigikohus on leidnud, et nt isiku arvuti on käsitatav kuriteo toimepanemise vahendina, kuivõrd selle abil on süüdimõistetul võimalik temale kuuluvas sülearvutis talletada ja taasesitada lapspornot sisaldavaid pildifaile.[176] Autor ei näe põhjust, miks ei ole võimalik analoogia korras rakendada eeltoodud seisukohta ka muudele digitaalse meedia allikatele, sh mobiiltelefonidele, tahvelarvutitele ja muudele digitaalsetele andmekandjatele. Põhimõtteliselt on kõik eeltoodud andmekandjad võimelised talletama ning taasesitama kuriteo asjaolude väljaselgitamiseks vajalikke andmeid.

Seega olukorras, mil digitaalne tõend asetseb mingil andmekandjal, võib olla asitõendiks andmekandja kui kuriteo toimepanemise vahend. Kõne alla tulevad digitaalsed tõendid kõige lihtsamalt avalduvates vormides, st tõendid, mille fikseerimiseks ei ole vajalik täiendavalt menetlustoiminguid läbi viia. Tõendamisväärtust omab eelkõige informatsioon, mis on otse andmekandjalt tuletatav, olgu selleks kuriteo asjaolusid kirjeldav või kuriteo toimepanemiseks vahetult kasutatud andmefail.

Tuginedes kehtiva seaduse redaktsioonile on võimalik andmekandjatel leitavaid digitaalseid tõendeid kriminaalmenetluses kasutada asitõenditena.

4.1.2. Arvutisüsteemides ning internetis leiduvad metaandmed

[175] E. Kergandberg, P. Pikamäe (koost). Kriminaalmenetluse seadustik. Kommenteeritud väljaanne. Juura, 2012. § 63 komm 4, E. Kergandberg, lk 190.
[176] RKKKm, 3-1-1-57-12, p 13.

Metaandmete puhul on regulatsioon mõniti teistsugune. Metaandmed, olles andmed andmete kohta, ei kujuta olemuselt otsest tõendit, vaid kaudset teavet mingi kuriteo kriitiliste elementide ehk tehiolude kohta.

Kriminaalmenetluse seadustiku § 63 lg 1 sätestab muuhulgas kinnises loetelus teabe liigina muu teabetalletuse. KrMS § 63 lg 1 ei sätesta muu teabetalletuse legaaldefinitsiooni.

Muu teabetalletuse määratlemisel võib põhimõtteliselt olla tegu ka nn muu dokumendi või asitõendi kvaliteeti omava tõendi liigiga. Eelkõige peetakse silmas uurimistoimingu käigus tehtavaid tehnilisi teabesalvestusi. [177] Eeltooduks võib olla näiteks sündmuskoha läbivaatamisel koostatud videosalvestis.

Metaandmed on tuletatavad nii isiku personaalarvutist kui muudest andmekandjatest, mis sisaldavad failisüsteeme või registreid, ning internetiteenuse pakkujale päringu esitamise vahendusel. Sisuliselt omab tõenduslikku informatsiooni mingi omandatud teabe fikseerimine tõendina. See protsess võib olla loodud viies läbi metaandmete uurimist kasutades digitaalkriminalistika printsiipe, sh digitaalse koopia loomist ning analüüsimist dokumenteerimise abil.

Tõendamisväärtust ei oma metaandmed iseseisvalt, vaid nende seostamine tehioludega. Metaandmed on omadustelt kaudsed tõendid. Seega, dokumenteerides menetlusreeglite kohaselt mingi metaandmetest tuleneva teabe, on seda võimalik siduda kuriteo asjaolude ning tuvastust leidnud faktidega. See võimaldab kinnitada või ümber lükata konkreetset kuriteo asjaolusid, olgu selleks teo toimepanemise või tahtluse tuvastamise fakt.

Tuginedes eeltoodule võib digitaalkriminalistide poolt koostatud informatsioon omandada muu teabetalletuse mõiste. Sisuliselt on tegemist uurimistoimingu käigus tehtava teabetalletusega, mis on dokumenteeritud protokolli vormis. Kriminaalmenetluse seadustik sätestab iga menetlustoimingu protokollimise nõude, mis omavad tõendi väärtust.

KrMS § 63 lg 1 alusel on mh tõendiks ka ekspertiisiakt. Juhul, kui kohtumenetluse või uurimise käigus otsustatakse, et kriminaalasja menetluses oleva digitaalse teabe tõendusväärtuse selgitamiseks on vajalik läbi viia ekspertiis KrMS § 95 lg 1 alusel, võib digitaalne tõend tekkida ka ekspertiisiakti alusel.

Kokkuvõtlikult võivad digitaalsed metaandmed, mis tulenevad arvutisüsteemidest ning interneti vahendusel, olla kriminaalmenetluses lubatavad tõendid, kui need on

[177] E. Kergandberg, P. Pikamäe (koost). Kriminaalmenetluse seadustik. Kommenteeritud väljaanne. Juura, 2012. § 63 komm 4, E. Kergandberg, lk 196

menetlustoimingute tulemusena nõuetekohaselt protokollitud. Täiendavalt on uurimisasutusel võimalus kogutud metaandmete alusel taotleda ekspertiisi läbiviimist. Ekspertiisi tulemusena koostatakse ekspertiisiakt, mis on iseseisev tõend. Kriminaalmenetluses käsitletakse tõendina ka eksperdi ütlusi ekspertiisiakti selgitamisel.

4.2. DIGITÕENDITE KOGUMINE

Viies läbi arvutialast uurimist tuvastamaks potentsiaalselt kuriteotunnustega tegu, tuleb järgida kohaliku riigi kohtumenetluse reegleid, tavasid ning tõenduspõhimõtteid. Reeglina koosnevad kriminaalasjad kolmest etapist. Esmalt kuriteokaebuse või kuriteole viitava informatsiooni edastamine uurimisasutusele, teiseks, uurimisprotsess tervikuna ning viimaks kohtumenetlus. [178] Käesoleva magistritöö raames on põhirõhk viimasel kahel ehk uurimisprotsessi legitiimsuse tagamisel ning digitaalsete tõendite kohtumenetluses kasutamisel.

Digitaalseid tõendeid on võimalik koguda kriminaalmenetluse seadustikus sätestatud tingimustel ning korras. Digitaalsete tõendite kogumisel tulevad eelkõige kõne alla KrMS § 83 järgi vaatlus, KrMS § 90^1 kohaselt päring sideettevõtjatele (nt internetiteenuse pakkujad), KrMS § 91 järgi läbiotsimine ning KrMS § 126^1 alusel jälitustoimingute vahendusel. Eeltoodud tõendite kogumise meetodid kokku võttes kogutakse digitaalseid tõendeid uurimis- ning menetlustoimingute abil.

Eesti Vabariigi põhiseaduse[179] § 32 lg 1 esimese lause järgi on igaühe omand puutumatu ning võrdselt kaitstud. Vara arestimine kahtlemata riivab inimeste põhiõigusi, kuna sellega piiratakse inimese õigust enda vara käsitleda.[180] Arvutiandmete läbiotsimisel ja arestimisel proportsionaalsuse põhimõttega arvestamine tähendab, et ära võtta või arestida võib vaid sellises ulatuses andmeid ja andmekandjaid, mis on menetluse läbiviimiseks ja tõendamiseseme asjaolude selgitamiseks vajalikud. Võimaluse korral tuleks asjassepuutuvad andmed kopeerida, kahtlustatava arvutist kustutada või talle kättesaamatuks muuta, mitte aga arvutit, arvutisüsteemi või andmekandjat tervikuna ära võtta.[181]

[178] B. Nelson, A. Phillips, C. Steuart. Guide to Computer Forensics and Investigations. Third edition. Course Technology, Cengage Learning, 2010, lk 12.
[179] Eesti Vabariigi Põhiseadus – RT I, 15.05.2015, 1
[180] RKKKm, 3-1-1-1-12, p 16
[181] RKKKm, 3-1-1-57-12, p 16

Eeltoodud sätted sisaldavad üldist regulatsiooni tõendite omandamiseks, st eriregulatsiooni digitaalsetele tõenditele, tulenevalt nende iseloomust, ei sätestata. Nagu varasemalt mainitud, on digitaalkriminalistika üks põhiprintsiipideks kriminalistilise koopia loomine. See tähendab, et andmekandjaid tuleks arestida vaid juhul, kui eeltoodud koopia loomine pole objektiivsetel kaalutlustel võimalik.

Põhiõiguste kaitsmisele viitab ka kriminaalmenetluse seadustiku § 64 lg 1, mille alusel ei tohi riivata tõendite kogumisel osaleja au ja väärikust, ei ohusta tema elu või tervist ega põhjusta põhjendamatut varalist kahju.

Teine põhiõiguslik garantii, mida digitaaltõendite kogumisel võidakse oluliselt rikkuda on PS § 26 tulenev eraelu puutumatuse õigus. Reeglina sisaldavad digitaalse meedia seadeldised hulganisti informatsiooni inimeste eraelu kohta ning taolise materjali uurimine on oluline riive inimeste põhiõigustele.

Tuginedes eeltoodule on oluline, et ka digitaalsete tõendite kogumine oleks seaduse alusel lubatud ning inimeste põhiõigusi võimalikult vähe riivav.

4.2.1. Arvutikuritegevusvastane konventsioon

Digitaalsete tõendite kogumise regulatsiooni sätestab Arvutikuritegevusvastane konventsioon (edaspidi Konventsioon)[182], millega Eesti on liitunud. Eeltoodud õigusaktiga liitumiseks on 12.02.2003 vastu võetud arvutitegevusvastase konventsiooni ratifitseerimise seadus.[183]

Sisuliselt on Konventsiooni puhul tegemist rahvusvahelise tunnustusega luua digitaalsete tõendite kogumiseks ning kasutamiseks eriregulatsioon. Konventsiooni preambulis on sätestatud, et välislepingu koostamisel ollakse teadlikud sügavatest muutustest, mille on kaasa toonud arvutivõrkude digiteerimine, vastastikune lähenemine ning jätkuv globaliseerumine. Täiendavalt avaldatakse muret selle kohta, et arvutivõrke ja elektroonilist teavet võidakse kasutada ka kuritegude toimepanemiseks ning et selliste kuritegudega seotud tõendeid võidakse salvestada ja edastada nende võrkude kaudu.

Õigusakti peamine eesmärk on sätestada välislepingu tasemel konventsiooniga liitunud riikidele minimaalsed materiaal- ning menetlusõiguslikud nõuded võitlemaks küberkuritegevusega ning menetlemaks digitaaltõendeid sisaldavaid kuritegusid.

[182] Arvutikuritegevusvastane konventsioon – RT II 2003,9,32
[183] Arvutikuritegevusvastane konventsiooni ratifitseerimise seadus – RT II 2003,9,32

Eeltoodud Konventsioon sätestab baasregulatsiooni digitaalsete tõendite kogumise suhtes. Konventsiooni artikli 14 lõike 2 punkti b) alusel tuleb sätestada arvutisüsteemi abil toimepandud muude kuritegude kohta elektrooniliste tõendite kogumise suhtes võtta seadusandlikud ja muud meetmed. Sama artikli lõige 2 punkt c) laiendab sätte kohaldamisala ka teiste kuritegude kohta elektrooniliste tõendite kogumise suhtes.

Konventsiooni seletuskirja punktist 141[184] johtuvalt on iga liikmesriik kohustatud artikli 14 rakendamisel võtma kasutusele meetmed nii a) konventsiooni 1. peatükis sätestatud kuritegude menetlemisel; b) teiste kuritegude menetlemisel, mis on toime pandud arvutisüsteemi vahendusel ning c) elektroonilises vormis kogutavate tõendite kasutamisel kriminaalmenetluses.

Seega kohustab õigusakt liikmesriikme töötlema välja menetlusõiguslikud võimalused eeltoodud meetmete rakendamiseks ka muude karistusseadustiku eriosas sätestatud kuritegude tõendamiseks digitaalsete tõendite kogumiseks. Konventsioon ei piirdu, nagu tuleneb õigusakti nimest, vaid arvutikuritegevuste menetlemiseks materiaal- ning menetlusõigusliku raamistiku loomisega.

Digitaalsete tõendite puhul on oluline art 16, mis võimaldab konventsiooniosalistele arvutiteandmete kiirsalvestamise juhul, kui on alust arvata, et arvutiandmed on kadumamineku või muutmise suhtes kaitsetud. Konventsiooni seletuskirja punkt 159[185] sätestab, et artikel teadlikult ei defineeri andmete säilitamise meetodit ning sobivad meetodid tuleb liikmesriikidel endil kaasusepõhiselt lahendada.

Konventsioon ei sätesta täpsemalt, millised on kiirsäilituse kohaldamise alused, mistõttu tuleb praktikast lähtuvalt pidada silmas konfiskeerimise regulatsioonile sarnaseid eeldusi, kuivõrd sisuliselt on tegemist arvutiandmeid edastava või säilitava teabekandja konfiskeerimisega.

Kahjuks tuleb möönda, et kriminaalmenetluses ei ole sätestatud tuginedes konventsioonile, menetlusõiguslikku raamistikku digitaaltõendite kogumise suhtes. Nagu eeltoodust leitud, kasutatakse digitaaltõendite uurimisel ning kohtumenetluses kasutamisel vaid kriminaalmenetluse seadustikus välja toodud üldnorme.

[184] Convention on Cybercrime. Details of Treaty No.185, lk 22. Arvutivõrgus kättesaadav: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (viimati külastatud: 23.04.2018)
[185] Samas, lk 26.

4.2.2. Digitaalsete tõendite kogumine vaatlusega

KrMS § 83 lg 1 järgi on vaatluse eesmärgiks koguda kriminaalasja lahendamiseks vajalikke andmeid, avastada kuriteojäljed ja võtta asitõenditena kasutatavad objektid ära. Lõike 2 p 3 alusel on vaatluse objektiks dokument, muu objekt või asitõend.

Vaatluse kohta tuleb koostada nõuetekohane protokoll järgides KrMS § 87 nõudeid. Tuginedes eeltoodud sättele on vaatluse abil digitaalsete tõendite kogumine võimalik kahel juhul, esiteks, kui digitaalsed tõendid asuvad sündmuskohal ning teisalt, kui vaatluse objektiks on lõige 2 p-s 3 sätestatud objekt. Kuivõrd muu objekti mõiste on väga avar, ei keela säte näiteks personaalarvuti vaatlust.

Vaatluse tulemusel võidakse vaadeldud objekti kasutada asitõendina või tuvastada kuriteojälgi. Kuriteojälgede fikseerimise korral on iseseisvaks tõendiks vaatlusprotokoll. Vaatluse tulemusena leitud asitõend omab kriminaalmenetluse seadustiku kohaselt iseseisvat tõenduslikku väärtust.

Tuginedes eeltoodule on vaatluse läbiviimisel võimalik tuvastada nii otseseid tõendeid kui ka kaudseid tõendeid. Otsesed tõendid fikseeritakse asitõendina. Kaudsete tõendite kogumise puhul vaatlusega tulevad kõne alla eelkõige varasemalt käsitletud metaandmed. Olukorras, mil uurija vaatluse objektiks on isiku personaalarvuti või muu andmekandja ning uurimistoimingu tulemusena fikseerib menetleja leitud metaandmed vaatlusprotokollis.

4.2.3. Digitõendite kogumine päringu esitamisega sideettevõtjale

KrMS § 90^1 lg 1 võimaldab menetlejal teha päringu elektroonilise side ettevõtjale üldkasutatava elektroonilise side võrgus kasutavate identifitseerimistunnustega seotud lõppkasutaja tuvastamiseks vajalike andmete kohta, välja arvatud sõnumi edastamise faktiga seotud andmete kohta. Lõike 2 järgi on uurijatel õigus taotleda ka elektroonilise side seaduses [186] sätestatud andmete kohta päringu esitamine prokuratuuri või kohtu loal kohtumenetluses esitada täiendav päring.

Seega sätestab sideettevõtjatele päringu esitamise regulatsioon uurijatele täiendava võimaluse digitaalsete tõendite omandamiseks tuginedes internetis levivatele metaandmetele, tuletamaks

[186] Elektroonilise side seadus – RT I, 01.07.2017, 2

digitaalseid tõendeid. Sideettevõtja on kohustatud säilitama isiku kohta seaduses loetletud informatsiooni ning päringu esitamise aluste olemasolul need uurimisasutusele väljastama. Seega on võimalik digitaalseid tõendeid koguda ka sideettevõtjale päringu esitamise abil.

4.2.4. Digitaalsete tõendite kogumine läbiotsimise kaudu

KrMS § 91 lg 1 järgi on läbiotsimise eesmärk leida hoonest, ruumist, sõidukist või piirdega alalt asitõendina kasutatav objekt, kriminaalasja lahendamiseks vajalik dokument, asi või isik või kriminaalmenetluses arestitav vara või laip või tabada tagaotsitav. Sätte sõnastusest ei tulene, et läbiotsimise raames oleks võimalik otsida arvutisüsteemist metaandmeid.

Peamiselt on läbiotsimise käigus võimalik otsida digitaalseid tõendeid neid edastavatelt või kandvatelt seadetelt, milleks on reeglina personaalarvutid, telefonid või muud igapäevaselt kasutatavad seadmed, ehk kriminaalmenetluse seadustiku § 63 lg 1 järgi asitõendeid.

Läbiotsimise puhul on oluline koostada läbiotsimisprotokoll, mis vastab KrMS § 92 lg 1 sätestatud protseduurinõuetele. Regulatsiooni kohaselt on võimalik asitõendina kasutatav objekt konfiskeerida. Digitaalsete tõendite puhul tuleks eelistada originaaltõendist koopia tegemist, kuivõrd tuginedes digitaalkriminalistika printsiipidele on see uurimise, menetlusökonoomia ning menetlusosaliste õiguse kaitsmiseks tõhusam vahend. Kriminaalmenetluse seadustik ei reguleeri läbiotsimise käigus asitõendina kasutatavast objektist koopia tegemist.

Juhul, kui läbiotsimise kahtlustatava käitumisest tulenevalt on võimalik eeldada, et tal on plaanis digitaalseid andmed kustutada, tuleb menetluse tulevase käigu huvides digitaalne tõend kahtlustatavale kättesaamatuks muuta või kustutada. Vastasel juhul võib kriminaalmenetluse lõppastmes tõusetuda vaidlus digitaalse tõendi usaldusväärsuse üle, st kui menetlusosalisel on jätkuvalt ligipääs eeltoodud failidele, ei ole välistatud andmete manipuleerimise võimalus.

Tuginedes digitaalsete tõendite allikate omadustele ei reguleeri kriminaalmenetluse seadustik läbiotsimise olulisi aspekte, milleks on näiteks parooliga kaitstud andmete läbiotsimine, st menetlusosaline ei ole kohustatud teatavaks tegema enda salasõna või võib väita, et ei ole sellest teadlik. Samuti võivad digitaalsed tõendid olla hoiustatud mõningatel internetihoiustamist pakkuvatel veebilehtedel või pilvesüsteemides.

Samas tekitab praktikas tihtipeale segadus läbiotsimise ning vaatluse kui menetlustoimingute piiritlemine. Sisuliselt võib vaatlus endas kujutada personaalarvuti läbiotsimist, mistõttu on oluline sätestada, milline on vaatluse ja läbiotsimise erinevus. Peamine erinevus regulatsioonis seisneb autori hinnangul selles, et läbiotsimise puhul on uurijatele teada objekt, mida otsitakse, st läbiotsimine peab olema tingitud mingile varasemale teabele digitaalse tõendi olemasolust. Vaatluse puhul on tegemist nö andmete juhuslikku laadi otsimisega, millal on eesmärgiks juhuslike tõendite leidmine.

4.2.5. Digitaalsete tõendite kogumine jälitustegevusega

KrMS § 126^1 kohaselt on jälitustoiming isikuandmete töötlemine seaduses sätestatud ülesande täitmiseks eesmärgiga varjata andmete töötlemise fakti ja sisu andmesubjekti eest.

Jälitustoimingute puhul on tegemist intensiivse põhiõiguste riivega, mistõttu sätestab kriminaalmenetluse seadustik täiendavad nõuded jälitustoimingute aluse ning korra suhtes. KrMS § 126 lg 4 järgi on jälitustoiminguga saadud teave tõend, kui jälitustoimingu loa taotlemisel ja andmisel ning jälitustoimingu tegemisel on järgitud seaduse nõudeid.

KrMS § 126^5 lg 1 järgi on isiku, asja või paikkonna varjatud jälgimiseks, võrdlusmaterjali varjatud kogumiseks ja esmauuringute tegemiseks ning asja varjatud läbivaatamiseks või asendamiseks annab prokuratuur loa kuni kaheks kuuks. Sama sätte lõike 2 kohaselt käesolevas paragrahvis nimetatud jälitustoimingu käigus vajaduse korral videosalvestatakse, pildistatakse või kopereritakse või talletatakse kogutud teave muul viisil.

Jälitustegevuse regulatsioon võimaldab, tuginedes KrMS § 126^3 lg-le 5 lubada varjatult siseneda ka andmesubjekti arvutisüsteemi juhul, kui see on vältimatult vajalik jälitustoimingu eesmärgi saavutamiseks. Tegemist on sisuliselt ainsa digitaalsete tõendite kogumise regulatsiooniga jälitustoimingute teostamisel ning ka see on üsna üldsõnaline, jättes reguleerimata menetlustoimingu ulatuse.

KrMS § 126^{10} lg 1 järgi tuleb jälitustoiminguga kogutud teabe alusel koostada jälitustoimingu teinud või jälitustoimingut taotlenud asutuse ametnikul koostada jälitustoimingu protokoll, kuhu kantakse p-des 1-6 sätestatud andmed. Mh tuleb jälitusprotokolli kanda jälitustoiminguga kogutud teave, mis on jälitustoimingu eesmärgi täitmiseks või kriminaalasja lahendamiseks vajalik.

Seega sisuliselt on uurijal kohustus dokumenteerida jälitustoiming kui tervik. Eeltoodud säte regulatsioonis on võimalik luua analooge digitaalkriminalistika põhimõtetega. Usaldusväärsete digitaalsete tõendite loomise meetod on range ning tuleb järgida teatud protseduurireegleid.

Kahtlemata on jälitustoimingute vahendusel digitaalsete tõendite kogumine kõige efektiivsem, kuivõrd subjekt ei ole sellest teadlik, mis tähendab, et andmete manipuleerimise võimalus on väiksem kui teiste menetlustoimingute puhul. Vastukaaluks on jälitustoimingute korral isikute põhiõiguste riive kõige olulisem, mistõttu on vajalik menetlustoimingu läbiviimisel analüüsida selle edukuse võimalust ning alternatiivseid lähenemisi.

Tõendusväärtuse omandab jälitustoimingute puhul informatsioon, mis toiminguga saadakse ja fikseeritakse jälitustoimingu protokollis. Uurimistoiming on efektiivseim vahend metaandmete kogumiseks. Kohtumenetluses kasutatakse tõendina jälitustoimingu protokolli, milles sisaldub metaandmete analüüsimisest või tuletamisest saadud informatsioon. Seega juhul, kui jälitustoimingu kohaselt uuritakse isiku postitusi sotsiaalmeedias, privaatvestlusi või e-kirjavahetust, tuleb tõendusväärtuse saamiseks jälitustoiming nõuetekohaselt protokollida.

4.2.6. Digitaalsete tõendite kogumise objektiivsed piirangud

Nagu eelpool välja toodud, on iga isiku põhiõigusi riivava menetlustoimingu tegemiseks vajalik prokuratuuri või eeluurimiskohtuniku luba. Kuivõrd digitaalsed tõendid on ajas kiiresti muutuvad ning immateriaalsed, võivad tihtipeale ajalised faktorid digitaalsete tõendite kogumise muuta võimatuks või seda raskendada olulisel määral.

Kuivõrd prokuratuuri või eeluurimiskohtuniku loa saamine võib võtta kaua aega, on oht, et uurijal ei ole võimalik tõendeid õigeaegselt koguda ning järgmiseks hetkeks võivad kõnealused tõendid olla kustutatud või muudetud.

Mõningad menetlustoimingud, näiteks läbiotsimine võimaldab KrMS § 91 lg p 6 järgi uurimistoimingu läbi viia ka ilma eeluurimiskohtuniku loata juhul, kui tegemist on edasilükkamatu juhuga. Digitaalsete tõendite puhul võib praktikas esineda mitmeid olukordi, mil eeltoodud sätet tuleb kasutada. Sarnane regulatsioon on kehtestatud ka läbiotsimise puhul (KrMS § 91 lg 3), mis võimaldab läbiotsimise läbi viia edasilükkamatutel juhtudel prokuratuuri loa alusel.

Tulenevalt jälitustoimingute iseloomust[187] ei ole prokuratuuri või eeluurimiskohtuniku loa õigeaegne saamine niivõrd problemaatiline. Jälitustoimingute puhul on alust eeldada, et andmesubjekt ei ole teadlik eelseisva menetlustoimingu läbiviimisest, mistõttu on andmete tahtliku hävitamise fakt ebatõenäoline.

Eelnevalt mainitud, sätestab ka arvutikuritegevusevastane konventsioon liiklusandmete ja muude arvutiandmete kiirsäilituse võimaluse. Kehtiv kriminaalmenetluse seadustik ei ole digitaalsete tõendite puhul eeltoodud eriregulatsiooni korporeerinud. Kõik reservatsioonid prokuratuuri või eeluurimiskohtuniku loa hilisemaks taotlemiseks on reguleeritud tuginedes menetlustoimingu edasilükkamatute tingimuste olemasolule. Eeltoodud sätted ei võta arvesse digitaalsete tõendite erilisi omadusi, vaid menetlustoimingu edasilükkamatust tervikuna.

Sellest hoolimata on kriminaalmenetluse seadustik loonud vastava regulatsioon edasilükkamatute menetlustoimingute sooritamiseks, mis võimaldab digitaalseid tõendeid omandada ka juhtudel, mis on oht, et menetlustoimingu tegemata jätmisel võivad tõendid muutuda või hävineda. Tegemist ei ole otsese regulatsiooniga muutmaks kättesaadavamaks digitaalsete tõendite kogumist, vaid sisuliselt üldregulatsiooniga võimaldada edasilükkamatute toimingute legaalne läbiviimine.

Eeltoodust johtuvalt on argumenteeritav, kas digitaalsetele tõenditele tuleks luua eriregulatsioon võttes arvesse arvutikuritegevusevastast konventsioonis sätestatut, kuivõrd välislepingu kohaselt ei vaja andmete kiirsäilitamine prokuratuuri või eeluurimiskohtuniku luba. Seega on konventsioonist tulenevalt arvutiandmete kiirsäilitamine menetlusökonoomilisem ning uurija jaoks vähem koormav. Sellest olenemata võimaldab kehtiv kriminaalmenetluse seadustik edasilükkamatutel juhtudel koguda tõendeid ilma eeluurimiskohtuniku loata.

4.3. Digitaalse koopia regulatsiooni vajadus

Kriminaalmenetluse seadustiku § 64 lg 1 sätestab tõendite kogumise üldpõhimõtted, mille kohaselt kogutakse tõendeid viisil, mis ei riiva kogumises osaleja au ja väärikust, ei ohusta tema elu või tervist ega tekita põhjendamatult varalist kahju. Regulatsioon on üldsõnaline ning ei sätesta tõendite kogumise üldprintsiipe, veel vähem digitaalsete tõendite kogumise

[187] Tegemist on isikuandmete töötlemisega eesmärgiga varjata andmete töötlemise fakti ja sisu andmesubjekti eest.

eritingimusi. Seega tuleb digitaalsete tõendite kogumisel lähtuda eelkõige digitaalkriminalistika põhiprintsiipidest.

Digitaalse koopia loomine on hädavajalik tõendamisväärtust omava tõendi loomisel. Tegemist on uurija võimalusega luua koopia tõendist, millest tulenevalt on võimalik tagada digitaalkriminalistika printsiipe. Digitaalse koopia loomisel on võimalik vähendada andmete manipuleeritavuse võimalust nii uurijate tegevuse kui ka tehniliste eksimuste tõttu. Digitaalse koopia loomine võimaldab muuhulgas vältida KrMS § 64 lg-s 1 sätestatud põhjendamatu varalise kahju tekkimist, kuivõrd digitaalse koopia loomisel ei ole uurija vahetult seotud digitaalset teavet omava seadmega, mis tähendab, et võimalus vara kahjustamiseks on väiksem, kui originaaltõendi vahetul fikseerimisel. Kahjuks tuleb möönda, et kriminaalmenetluse seadustik ei reguleeri digitaalse koopia tegemise võimalust või tingimusi.

Arvutikuritegevusvastase konventsiooni artikli 19 lõike 3 punkti b alusel on asutus volitatud tegema arvutiandmete koopia ja säilitama seda. Eeltoodud sätet ei ole Eesti seadusandlusesse otseselt üle võetud, ent tuginedes konventsioonile peavad liikmesriigid konventsiooni sätted siseriiklikesse õigusaktidesse korporeerima.

Autori hinnangul on oluline sätestada kriminaalmenetluse seadustikus eriregulatsiooni digitaalse koopia loomise võimaldamiseks, säilitamiseks ning kasutamiseks kohtumenetluses. Digitaalse koopia loomise võimaldamise regulatsioon aitaks muuta digitaalsete tõendite analüüsimise protseduuri oluliselt lihtsamaks. Samuti võimaldab digitaalne koopia hõlpsasti taasesitada digitaalse tõendi analüüsimisel omandatud teavet, tuvastada dokumendi terviklikkus ning tagada muid digitaalkriminalistika printsiipe.

KOKKUVÕTE

Käesoleva magistritöö eesmärk oli analüüsida, kas digitaalsete tõendite kogumine ja kasutamine kriminaalmenetluses on tuginedes kehtivale regulatsioonile võimalik. Eelkõige on silmas peetud, kas digitõendite kogumise protsess võimaldab fikseerida tõendid seaduses sätestatud menetlusõigust järgides ning lubatud vormis. Digitõendite kasutamine kohtumenetluses tähendab seda, tõendid peavad olema kriminaalmenetluses lubatud ehk vastama kriminaalmenetluse seadustikus sätestatud tõendi definitsioonile.

Digitaalsete tõendite kogumise, analüüsimise ning esitamisega tegeleb digitaalkriminalistika. Teadusharu efektiivsemaks rakendamiseks on praktikas välja töötatud hulk printsiipe, mis võimaldavad uurijatel luua kriminaalmenetluses lubatud tõendeid. Digitaalkriminalistika printsiipide ebapiisav rakendamine ning tehniliste lahenduste puudlikkus on olulises seoses tõendite kogumise protsessiga. Juhul, kui uurijatel puudub erialane väljaõpe või efektiivsed töövahendid, ei pruugi digitaalsete tõendite fikseerimine olla läbi viidud menetlusnormide kohaselt. Lõppastmes on selle tagajärjeks tõendi lubamatus kohtumenetluses.

Eestis ei ole digitaalkriminalistikale kui teadusharule olulist rõhku osutatud. Eesti Kohtuekspertiisi Instituudis on loodud Infotehnoloogia osakond, mis tegeleb digitaalsete tõendite analüüsimisega. Digitaalsete tõendite kogumine uurimisasutuste tasandil ei ole seadusandlikult fikseeritud, samuti ei ole valdkonna kohta kodumaist õiguskirjandust.

Magistritöös leidis kinnitust hüpotees, mille kohaselt on digitaalkriminalistika tehnilised võimalused Eesti kriminaalmenetluses ammendavad kogumaks, analüüsimaks, hoiustamaks ning esitamaks kriminaalmenetluses lubatavaid tõendeid. Olgugi, et hüpotees leidis kinnitust, esineb hulganisti tehnilisi probleeme, mis võivad digitõendite fikseerimisel osutuda komistuskiviks. Tõendite fabritseerimine võib aset leida ka füüsiliste tõendite puhul. Küll aga, tuginedes digitõendite muutuvusele, anonüümsusele ja manipuleeritavusele, on digitõendite fabritseerimist oluliselt keerulisem tuvastada. Täiendavalt, digitaalse koopia loomise regulatsioon võimaldab uurijatel digitõendeid analüüsida viisil, mis tagab digitõendite terviklikkuse ning autentsuse. Autentsuse kontrollimiseks on loodud matemaatilised räsifunktsioonid, mis võimaldavad tuvastada tõendite tahtliku või tahtmatu muutmise, veenmaks nii uurijaid kui ka kohut tõendi terviklikkuses ja autentsuses.

Eesti kriminaalmenetlus on üles ehitatud rangele tõendistruktuurile, mis tähendab, et tõendina on käsitletud vaid kriminaalmenetluse seadustiku §-s 63 loetletud tõendi liigid. Digitõendite puhul on tegemist füüsilistest tõenditest unikaalsema tõendi liigiga. Omadustelt on digitaalsed

digitõendid immateriaalsed ja implitsiitsed, mis muudavad nende fikseerimise füüsiliste tõendite fikseerimisest oluliselt keerulisemaks.

Digitaalseid tõendeid on sisuliselt võimalik jaotada kahte peamisesse gruppi. Esmalt digitõendid, mis iseenesest omavad tõenduslikku väärtust, nt e-kirja sisu või andmekandjalt leitavad fotod, ning mille eesmärgiks on tõendada kuriteo asjaolusid. Teisalt digitaalsetelt andmekandjatelt omandatavad metaandmed, mille fikseerimine on kriminaalmenetluse seadustiku kohaselt keerulisem. Eeltoodud andmete eesmärgiks on tõendada nii kuriteo asjaolusid kui ka digitõendite autentsust.

Kehtiv kriminaalmenetluse seadustik ei sätesta digitõendite kogumisele ning lubatavusele eriregulatsiooni. See tähendab, et digitaalseid tõendid on kohtumenetluses lubatud juhul, kui neid on võimalik paigutada tõendi üldregulatsioonis sätestatud liigituse raamesse. Kuivõrd seadusandja on tõendi mõistesse hõlmanud eraldi tõendiliigina mh asitõendid ning muud teabetalletused, võimaldab õiguskirjandus ning kohtupraktika eeltoodu alla paigutada ka digitaalseid tõendeid.

Sellised digitõendid, mis omavad iseenest tõenduslikku materjali, on reeglina salvestatud mingile andmekandjale, nt arvutisüsteemi kõvakettale või digitaalsele andmekandjale. Riigikohus on leidnud, et objekt, millele tõend on hoiustatud, on iseenesest kuriteo toimepanemise vahend ehk asitõend. Seega on andmekandjatel leitavad tõendid lubatud kohtumenetluses asitõenditena.

Metaandmete puhul on tõendite lubatavuse problemaatika erinev. Sisuliselt ei oma tõendusmaterjali metaandmed ise, vaid nende fikseerimisest tuletatud järeldused. Seega ei saa metaandmete puhul olla tegemist asitõenditega. Kriminaalmenetluse seisukohast pole oluline fakt, et kasutaja on süsteemi mingil ajahetkel sisse loginud, vaid tõenduslikku väärtust omab teave, kuidas on võimalik siduda metaandmed kuriteo tehioludega. Sisuliselt tähendab see, et metaandmeid on vaja lubataval moel fikseerida.

Reeglina fikseeritakse metaandmeid menetlustoimingute vahendusel, olgu selleks ekspertiisi teostamine, läbiotsimine või uurimiseksperiment. Sellisel juhul on tõendiks koostatud menetlustoimingu protokoll või ekspertiisiakt, mis on tõendina lubatud ning autentne ja usaldusväärne. Sellegipoolest on oluline, et tõendi fikseerimise protsess oleks kooskõlas digitaalkriminalistika printsiipidega.

Muu teabetalletuse mõiste määratlemisel võib sisuliselt tegemist olla muu dokumendi või asitõendi kvaliteeti omava tõendi liigiga, mh tuleb kõne alla ka uurimistoimingu käigus tehtavad tehnilised teabesalvestised.

Sarnaselt digitaalsete tõendite lubatavusele on problemaatiline digitõendite kogumise temaatika. Taaskord, ei sätesta kriminaalmenetluse seadustik eriregulatsiooni digitaalsete tõendite kogumiseks. Küll aga on Eesti ratifitseerinud arvutikuritegevusvastase konventsiooni. Eeltoodud välisleping kohustab liikmesriike siseriiklikku seadusandlusesse implementeerima hulganisti regulatsioone arvutikuritegevusega võitlemiseks. Erinormidena sätestatakse ka muude digitaalsete tõendite kogumise, mis on kuritegude tõendamisel olulised. Eeltoodud sätete rakendamine Eesti seadustes on puudulik.

Samas ei saa eitada, et käesolev regulatsioon on piisav digitõendite kogumiseks ning kasutamiseks kriminaalmenetluses. Kriminaalmenetluse seadustik sätestab hulganisti tõendite kogumise viise, mille abil on võimalik ka digitõendeid koguda. Muuhulgas võimaldab kehtiv seadusandlus koguda digitaalseid tõendeid erinevate menetlustoiminguga, nt vaatlusega või läbiotsimisega, päringuga sideettevõtjale, jälitustegevusega jne. Vajadusel on võimalik kogutud andmetele teha ekspertiis, mille tulemusel omandatud informatsioon omab samuti tõendi jõudu.

Käesoleva magistritöö raames on leidnud kinnitust hüpotees, mille kohaselt on digitaalseid tõendeid võimalik kriminaalmenetluses kasutada. Kehtiv seadusandlus ei sätesta eriregulatsiooni digitõendite kogumiseks. Tõendite kogumise üldnormide kohaselt on reguleeritud hulganisti menetlustoiminguid, mille vahendusel on võimalik ka digitõendeid fikseerida. Seega on digitõendid kehtiva kriminaalmenetluse seadustiku kohaselt kohtumenetluses lubatud.

Magistritöös on põhjalikult analüüsinud digitaalsete tõendite olemust, digitaalkriminalistikat kui teadusharu ning erinevaid allikad, milledest on võimalik digitaalseid tõendeid tuletada. Kahtlemata on digitaalkriminalistika iga aastaga kriminaalmenetluses suuremat rolli mängiv teadusharu, mistõttu tuleb Eesti spetsialistidel valdkonna rakendamisega põhjalikumalt tegeleda. Autori hinnangul on vajalik luua Eesti uurijatele digitaalkriminalistika käsiraamat, mis aitaks nii kogenud uurijatel kui ka teistel inimestel ennast kurssi viia teadusharu põhiprintsiipidega ning töömeetoditega.

Olgugi, et kriminaalmenetluse regulatsioon on digitõendite kasutamiseks ja kogumiseks piisav, tuleb kehtiv seadustik viia kooskõlla arvutikuritegevusvastase konventsiooniga, mis

sätestab digitaalsete tõendite eriregulatsiooni kehtestamise kohustuse. Eesti on välislepingu ratifitseerinud 2002. aastal ning käesolevaks aastaks ei ole seadustikus sätestatud ühtegi digitõendi eriregulatsiooni. Tuginedes eeltoodule ei ole Eesti täitnud konventsioonist tulenevaid kohustusi digitõendite kogumiseks vajaliku menetlusõiguse regulatsiooni kohaldamiseks.

Autori hinnangul ei ole niivõrd problemaatiline digitaalsete tõendite kui asitõendite regulatsiooni vajadus. Nii seadusandlus kui ka Riigikohus tunnustab andmekandjatelt leitavate digitaalsete tõendite fikseerimist asitõenditena, mistõttu eriregulatsioon ei ole vajalik. Küll aga tekitab hulganisti probleeme metaandmete fikseerimine. Käesoleval hetkel ei ole sätestatud kindlat standardit, mil viisil metaandmeid lubatava tõendina fikseerida. Seadus sätestab hulganisti menetlustoiminguid, mille alusel on võimalik andmeid tõendina kasutada, sh muu teabetalletuse mõiste. Sellest hoolimata on metaandmed tavapärastest füüsilistest tõenditest kõrgemal erinevad – nende leidmine, analüüsimine ja fikseerimine nõuab hulganisti eriteadmisi.

Käesolev magistritöö on avardanud digitaalkriminalistika kui teadusharu mõistet Eesti kriminaalmenetluses. Lisaks eeltoodule avas autor digitõendite olemuse ning eriliigid, millest tuleb kriminaalmenetluse kestel lähtuda. Tulenevalt digitõendite unikaalsetest omadustest, analüüsinud nende kohta kriminaalmenetluse ranges tõendistruktuuris ning kogumist ja fikseerimist tuginedes kehtivatele menetlusõiguse normidele.

ABSTRACT

Perspective of Acquiring and Using Digital Evidence in Criminal Proceedings

Modern society is vastly depending on different communication systems, internet of things, mobile devices and other forms of digital communication. The use of high-tech gadgets and technological advances have improved and benefited life of many people. On the other hand, with the growth of infotechnology, many legal problems arise. One of which is the formation and use of digital evidence in the Court of Justice.

In most cases, the use of digital evidence in the Court of Justice has been a success. It is important to note, that the forms of digital evidence may be used in any type of Court – administrative cases, criminal proceedings and even civil matters. This paper focuses on the use of digital evidence in Criminal Proceedings.

Digital evidence has been around for as long as computers have existed. Digital evidence are all around us, almost every person owns some form of digital media, which is feasible to store or create digital evidence. This is mainly caused by the wide accessibility of digital media devices.

Carrying out the analysis of the hypothesis, the main objective of this paper was to expand the definitions of digital evidence, digital forensics as a science of obtaining and analysing digital evidence and the types of digital evidence which can be found on various sources of digital media.

Characteristics of digital evidence include being hidden for the most of the times, latent, crossing the borders of jurisdiction, easily manipulated and destroyed and sensitive to time factors. It is very hard to identify the author of the digital evidence. Some authors say, that digital evidence and physical evidence do not have any fundamental differences. However, the characteristics of digital evidence make it harder to seize and analyize, on the other hand, they information and metadata, which has potential to be more valuable to the investigation. Digital evidence may be contained in open computer systems, also known as computers, in various communication systems, such as internet and in embedded computer systems.

Estonian legislation has not implemented any regulation for digital evidence in specific, which means, the use of digital evidence is regulated by the general provisions found in Code of Criminal Procedure. That rises alot of legal problems, starting from digital evidence being

admissibile in Court to having no regulation specifing the process of acquiring digital evidence.

The main purpose of this paper is to analyse whether digital evidence are admissible as evidence in the light of Code of Criminal Procedure. Furthermore, evidence can only be acquired by following the procedural provisions regulating the process. The hypothesis consists of digital evidence being admissable as evidence and being acquiriable in the lights of general rules found in Criminal Proceedings Act. Author deems the stipulated hypothesis to be approved.

Digital Forensics is the use scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations. In short, digital forensics is the science which analyses and acquires digital evidence.

The purpose of the science is not to prove someone guilty or innocent, but to provide digital evidence, which would be admissible in Court of Justice. The evidence gathered might be direct or indirect, depending on the data and information provided. Digital forensics addresses many cases of digital investigation, such as data recovery, identifying deleted data, alternation of data, crypting and decrypting data etc.

Digital forensics has developed a set of principles, which must be followed in order to create admissibile evidence. The principles include evidence exchange, evidence characteristics, forensic soundness, authentication, chainf of custody, evidence integrity, objectivity and repeatability.

In order to obtain a better understanding on the rules governing digital evidence, it must be settled, which sources and what types of digital evidence provide. Due to its nature, digital evidence can be classified as direct evidence, which derive from digital media and digital evidence, which come in the form of metadata.

The main difference between the classification of evidence is, that the metadata itself can not have evidentiary attributes. The information, which is obtained and documented with the use of digital forensics, can administer the admissibility of evidence. On the other hand, documents, pictures or other forms of data found on any sort of digital storage medium, might idependently have evidentiary characteristics. Such as a folder of child pornography or e-

mails providing information about a crime, itself may be evidence in a Criminal Proceedings. However, metadata containing information about when a file was created, has to be analysed further and documented in a suitable manner in order to be admissible in Court.

The abovementioned classification has an important aspect in the process of acquiring evidence and evidence being admissable in Court.

Criminal Proceedings Act § 63 (1) defines the list of admissibile types of evidence, which include physical evidence and other documents, photographs, films or other data recordings. It is debatable, where or if digital evidence may be classified in the light of this provision. The purpose of this paper was to find whether digital evidence are allowed and regulated in the abovementioned regulation.

Author of this paper found, that the digital evidence derived from a digital media source, can be classified as a physical evidence. Physical evidence may be defined as an object used to provide evidence about any details of the crime. Usually, physical evidence refers to an object, which can be confiscated. The Supereme Court has established, that a person's computer may be classified as a tool for commiting crime, since the system is able to preserve and reproduce picutre files containing child pornography. Using analogy, this can be adjusted to other digital media found on users digital media sources, such as USB-flash drives, digital camera memory card etc. According to above, digital evidence may be classified as physical evidence.

When it comes to metadata found on either a computing system or other digital sources or in Internet, the provision is not that unambiguous. Metadata can not be physical evidence, since by nature, it contains data about data. According to the Code of Criminal Procedure, an admissable evidence may be other documents, photographs, films or other data recordings. Metadata can obtain evidentary value only if it is documented or protocolled according to the procedual provisions. Metadata can not have evidentiary value on its own. There are two methods of documenting metadata, first of which, is to compose a procedural act, having information about collecting and analysing the information, as well as stating its importance to the case. The second method contains conducting an expertise of the acquired data, of which an expert's report must be drawn. According to the provision mentioned above, the report itself has evidentiary value, as well as the expert's statements concerning the expert's report.

So, to sum up, in the light of this paper, digital evidence derived from either digital media or obtained as metadata are admissiable in the Court of Justice. The general provisions are framed broad enough for digital evidence to be classified as evidence according to the Code of Criminal Procedure.

The second part of confirming the hypothesis requires analyising whether the current regulation in Code of Criminal Procedure provides enough grounds for investigators to gather digital evidence. Taking into account the special features of the digital evidence.

Evidence in general may be acquired only by following the regulations provided in law. Collection of evidence must not infrige the fundamental rights provided in the Constitution of the Republic of Estonia. According to the Constitution, property of every person is inviolable and equally protected, as well as everyone is entitled to inviolability of his or her private and family life. The Constution states, that every person's dignity, honour, life and health must be preserved. Forementioned constitutional guarantees are the most vulnerable to Criminal Proceedings.

Collecting of digital evidence has the potential to infridge the constitutional guarantees as much as physical evidence. However, taking into account the fact, that usually digital evidence is derived from a person's digital media device, which usually contains a lot of personal information, in most cases, those fundamental rights are being infridged on a larger scale.

In 2002, Estonia validated Convention on Cybercrime. The main purpose of the act is to establish a foundation for regulations concerning fighting cybercrime and collecting digital evidence. Drawing up the Convention, the parties were aware of the changes caused by digitalisation and globalisation of computer networks, as well as the fact that computer networks and electronic data might be used to commit crimes and may be saved and forwarded using computers and internet in general.

The Convention has set up minimum requirements for substantive and procedual provisions concerning the digital evidence. Such as, Article 14 (2) subsection b) and c) oblige parties to take precautions for collecting digital evidence for crimes being commited using computers and other crimes, which might have digital evidence derived. According to Article 16, parties must adopt such legilsative and other measures necessary to enable its competent authorities to preserve computer data, that is believed to be particularly vulnerable to loss or modification.

Unfortunately, comparing the abovementioned provisions in the Convention of Cybercrime and current regulations in the Code of Criminal Procedures, Estonia has failed to adapt regulations concerning obtaining and preserving digital evidence.

Nevertheless, it still must be analysed whether according to current law, it is possible to acquire digital evidence in an admissible manner. The main procedual acts for acquiring digital evidence are inspection, request to electronics communications undertakings to submit information, a search and taking of evidence by Surveillance Activities.

According to the Code of Criminal Procedures, the main goal of conduction an inspection, is to collect necessary information, data, detect evidentary traces and confiscate physical evidence. Evidence, derived from an inspection can be physical, such as a suspect's computer, or non-physical, mainly being protocol drawn about conduction an inspection. During an inspection, if physical evidence is found, it can be used as an evidence. In case evidentary traces are found, they must be protocolled, which itself serves as evidence in the Court of Law. In that case, concerning metadata, problem arises, however being of evidentary value, protocol about discovering metadata does not have any value. Further analysis must be drawn in order for meta data to serve purpose.

Electronics communications providers are required by law to maintain information about the user of the service. Electronics Communication providers might hold important metadata about the user's actions in the network. Therefore, investigators may use the regulation in order to obtain metadata found on Internet.

Search is a procedual act during which, the main purpose is to find physical evidence from either a building, a room, a vehicle or fenced area. Based on the idea of a search, the goal is supported by the knowledge of the object being searched. According to which, the search serves it's purpose of finding abovementioned physical evidence which contain digital evidence.

Surveillance activities are one of the most problematic procedual acts regulated in the Code of Criminal Proceedings. Due to its nature of having the most potential to infrige fundamental rights, surveillance activities must be carried out taking precautions. Regulation allows investigators to enter the subject's computer system when it is necessary for carrying out the purpose of the procedual act. Therefore, surveillance activities are excellent way to gather digital evidence – the fact of subject not knowing about the collection of evidence makes it

extremely difficult for him or her to manipulate or terminate data, that might acquire evidentiary powers in the investigation.

To sum it up, Code of Criminal Procedure regulates many ways for investigators to carry out procedual acts for collecting digital evidence. That confirms the papers hypothesis, according to which, current legislation allows investigators to acquire digital evidence. However, being member of Convention of Cybercrime, Estonia has failed to implement the minimum requirements set for substantive and procedual law to acquire digital evidence from subjects.

The work briefly analyses the term forensic copy, which is a tool for digital investigators to carry out analysis of digital evidence. Forensic copy is made of original piece of evidence, to maintain the original source of evidence and convince the Court of Justice that evidence has not been altered or manipulated. Based on this paper, author finds it necessary for Estonia to implement a provision governing the concept of forensic copy. With the correct precautions and analysis carried out on the copy, it has all the potential to serve as a special type of evidence. Provisions governing the creation, preserving and analysising forensic copy, have possibility to make use of it in criminal proceedings.

Furthermore, this paper concludes, that special provisions, concerning digital evidence, should be introduced to the Code of Criminal Procedure. Although, according to current provisions, digital evidence is admissibile and acquirable, special regulation must be established. The process of obtaining digital evidence must be drawn, in order for the investigators to acquire digital evidence without the danger of loss or manipulation of data. Secondly, the admissibility of digital evidence in criminal proceedings depends heavily on the procedural acts.

Despite the topical need for regulations concerning digital evidence, Estonia has failed to implement the minimum substantial and procedular regulations set out in the Convention of Cybercrime.

To conclude, this paper has thouroughly analysed the digital evidence as a special type evidentiary material in criminal proceedings and digital forensics as a science aimed to collect and analyse digital data. Furthermore, the methods of acquiring digital evidence and being admissable in Court, taking into account the different forms of digital evidence being found.

KASUTATUD LÜHENDID

Art - artikkel

EKEI – Eesti Kohtuekspertiisi Instituut

EKEI määrus – Eesti Kohtuekspertiisi Instituudi põhimäärus

FTK – Forensic Toolkit

KES – Kohtuekspertiisiseadus

Konventsioon – Arvutikuritegevusvastane konventsioon

KrMS – Kriminaalmenetluse seadustik

ProkS – prokuratuuriseadus

RKKKO – Riigikohtu Kriminaalkolleegiumi otsus

RKKKm – Riigikohtu Kriminaalkolleegiumi määrus

KASUTATUD KIRJANDUS

1. A. Castiglione, G. Cattaneo, G. De Maio, A. De Santis, G. Costabile and M. Epifani. The Forensic Analysis of a False Digital Alibi. 2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing. Palermo, 2012.
2. A. De Santis, A. Castiglione, G. Cattaneo, G. De Maio, M. Ianulardo. Automated Construction of a False Digital Alibi. Springer, Berlin, Heidelberg. 2011
3. A. Varol, Y. Ü. Sönmez. Review of Evidence Analysis and Reporting Phases in Digital Forensics Process. 2017 International Conference on Computer Science and Engineering (UBMK). Türgi, 2017
4. Association of Cerfitied Fraud Examiners. Investigating by Computer. Second edition. 2002.
5. Andmekaitse Inspektsioon. Metaandmed ja privaatsus. Juhis organisatsioonidele ja kodukasjatale seaduse rakendamisel. 28.10.2015. a.
6. B. Nelson, A. Phillips, C. Steuart. Guide to Computer Forensics and Investigations. Third edition. Cengage Learning, 2014.
7. C. Reed. Computer Law, Seventh Edition. Oxford University Press, 2008.
8. Collective work of all DFRWS attendees. A Road Map for Digital Forensic Research. DFRWS. Utica, New York, USA, 2001.
9. Convention on Cybercrime. Details of Treaty No.185. Kättesaadaval veebiaadressil: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
10. D. Ryan and G. Shpantzer. Legal aspects of Digital Forensics. The George Washington University. Washington, D.C., USA. 2002
11. E. Casey. Digital evidence and computer crime: Forensic Science, Computers, and the Internet, 3rd Edition. Academic Press, 2011.
12. E. Casey. Handbook of Digital Forensics and Investigation. Academic Press, 2009
13. E. Kergandberg, M. Sillaots. Kriminaalmenetlus. Kirjastus Juura. Tallinn, 2006.
14. E. Kergandberg, P. Pikamäe. Kriminaalmenetluse seadustik. Kommenteeritud väljaanne. Juura, 2012.

15. Eesti Kohtuekspertiisi Instituudi infovoldik. Kättesaadaval veebiaadressil: https://www.google.ee/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0ahUKEwi8npTouvPZAhVlM5oKHSBdBnEQFghKMAM&url=http%3A%2F%2Fwww.ekei.ee%2Fsites%2Fwww.ekei.ee%2Ffiles%2Felfinder%2Fdokumendid%2Fekei_voldik_0.pdf&usg=AOvVaw2TJEm-2nvoHc0xf-cOp1iP (viimati külastatud: 23.04.2018))

16. Eesti Kohtuekspertiisi koosseis, 01.02.2018. kinnitatud. Kättesaadav veebiaadressil: http://www.ekei.ee/sites/www.ekei.ee/files/elfinder/dokumendid/ekei_koosseis_01.02.2018.pdf (viimati külastatud: 23.04.2018)

17. G. G. Richard, V. Roussev. Digital Crime And Forensic Science in Cyberspace, Chapter V: Digital Forensics Tools: The Next Generation. IGI Publishing Hershey. Pennsylvania, USA, 2006

18. G. Peterson, S. Shenoi. Advances in Digital Forensics XIII. Springer. Orlando, FL, USA. 2017

19. J. Cosic, M. Baca. (Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. The 33rd International Convention MIPRO. Opatija, Croatia, 2010

20. J. Tehver. Digitaalsete tõendite kasutamise võimaldamine. Mai 2016. Arvutivõrgus kättesaadav: https://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf (viimati külastatud: 23.04.2018)

21. K. L. Rusbarsky. A Forensic Comparison of NTFS and FAT 32 File Systems. Marshall University Forensic Science Center. Kansas City, 2012.

22. K. Palm. Digitaalsed tõendid ja nende talletamine Põhja Prefektuuri näitel. Lõputöö, Sisekaitseakadeemia, Politsei- ja Piirivalvekolledž. Tallinn, 2013.

23. L. Caviglione, S. Wendzel, W. Mazurzcyk. The Future of Digital Forensics: Challenges and the Road Ahead. IEEE Security & Privacy (V: 15, Issue: 6), November/December 2017. IEE, 2017.

24. L.Qian, F. Höglin, P. A. Diaz. Computer Forensics. Uppsala University, 2007.

25. Lucio D. Jasio. Programming 16-bit PIC Microcontrollers in C: Learning to Fly the PIC 24. Newnes. Burlington, MA:, 2007.

26. M. B. Mukasey, J. L. Sedgwick, D. W. Hagy. Electronic Crime Scene investigation: A Guide for first responders, Second edition. U.S. Department of Justice Office of Justice Programs. 2008.

27. M. Lachiniet, C. Hornat. A forensic Primer for Usenet Evidence. SANS Institute, 2006.

28. M.G.Nagaraya. Investigators chain of custody in digital evidence recovery. Bureau of Police Research and Development, Indian Police Journal, 2006.

29. P. Craiger, M. Pollitt and J. Swauger, Law enforcement and digital evidence, in Handbook of Information Security, Volume 2, H. Bidgoli (Ed.), John Wiley, New York, pp. 739–777, 2006.

30. P. Gladyshev,. Formalising Event Reconstruction in Digital Investigations. Doktoritöö. Department of Computer Science, University College Dublin. 2004

31. P. Sommer. Emerging Problems in Digital Evidence. Presentation to Criminal Bar Association, 2007.

32. R. McKemmish. When is Digital Evidence Forensically Sound?. Ray I., Shenoi S. (eds) Advances in Digital Forensics IV. DigitalForensics 2008. IFIP — The International Federation for Information Processing, vol 285. Springer, Boston, MA, 2008.

33. S. Beyer, M. Mulazzani, S. Schrittwieser, M. Huber and E. Weipp. Towards fully automated Digital Alibis with social interaction. Technical University of Vienna. Vienna, 2014.

34. S. E. Goodison, R. C. Davis, B. A. Jackson. Digital Evidence and the U.S. Criminal Justice System. Identifying Technology and other Needs to more efficiently acquire and utilize Digital Evidence. National Institute of Justice. 2015

35. S. Garfinkel. Digital Forensics Research: The Next 10 Years. DFRWS. Portland, USA, 2010.

36. S. Saleem. Protecting the Integrity of Digital Evidence and Basic Human Rights during the Process of Digital Forensics. Stockholm University. 2015

37. S. Van Deusen Phillips. Legal Considerations for Electronic Evidence, Part 2: Relevance and authenticty. Word Press, 2010. Arvutivõrgus kättesaadav: https://crlgrn.wordpress.com/2010/04/26/legal-considerations-for-electronic-documentation-part-2-relevance-and-authenticity/ (viimati külastatud: 23.04.2018)

38. S. von Solms, C. Louwrens, C. Reekie and T. Grobler. A Control Framework for Digital Forensics. Olivier M.S., Shenoi S. (eds) Advances in Digital Forensics II. IFIP Advances in Information and Communication, vol 222. Springer, Boston, MA. 2006

39. V. Schmitt, J. Jordaan. Establishing the Validity of MD5 and SHA-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in these Algorithms. International Journal of Computer Applications (0975 – 8887) Volume 68– No.23. 2013

40. Guo Y., Slay J. Data Recovery Function Testing for Digital Forensic Tools. In: Chow KP., Shenoi S. (eds) Advances in Digital Forensics VI. DigitalForensics. IFIP Advances in Information and Communication Technology, vol 337. Springer, Berlin, Heidelberg. 2010

KASUTATUD ÕIGUSAKTID

41. Arvutikuritegevusvastane konventsioon – RT II 2003,9,32
42. Arvutikuritegevusvastane konventsiooni ratifitseerimise seadus – RT II 2003,9,32
43. Eesti Kohtuekspertiisi Instituudi põhimäärus – RT I, 06.02.2015, 3
44. Eesti Kohtuekspertiisi Instituudi põhimäärus – RT I, 06.02.2015, 3
45. Eesti Vabariigi põhiseadus – RT I, 15.05.2015,2
46. Elektroonilise side seadus – RT I, 01.07.2017,2
47. Justiitsministri määrus „Riiklikus ekspertiisiasutuses tehtavate ekspertiiside loetelu“ – RTL 2008, 9, 112.
48. Kohtuekspertiisiseadus – RT I,30.12.2015, 21
49. Kriminaalmenetluseseadustik – RT I,05.12.2017, 8
50. Prokuratuuriseadus – RT I, 28.12.2017, 13

KASUTATUD KOHTUPRAKTIKA

51. RKKKo 01.03.2006, 3-1-1-142-05
52. RKKKo 04.05.2011, 3-1-1-33-11
53. RKKKm 20.02.2012, 3-1-1-1-12
54. RKKKm 16.05.2012, 3-1-1-57-12

KASUTATUD MUUD ALLIKAD

55. https://www.am.ee/node/5287
56. http://kfst.ee/korduma-kippuvad-kusimused/
57. https://www.techopedia.com/definition/1119/storage-device

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Gerd Raudsepp (sünnikuupäev: 28.07.1993)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Infotehnoloogia ja digitaalsete tõendite omandamise ja kasutamise võimalikkus kriminaalmenetluses“, mille juhendaja on dr. iur. Mario Rosentau,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhviivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. Olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, 23.04.2018. a.