ŠARŪNAS GRIGALIŪNAS

NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE EKSPERTINIO TYRIMO METODAS

DAKTARO DISERTACIJOS SANTRAUKA

TECHNOLOGIJOS MOKSLAI, INFORMATIKOS INŽINERIJA (T 007)

Kaunas
2020

KAUNO TECHNOLOGIJOS UNIVERSITETAS
VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

ŠARŪNAS GRIGALIŪNAS

NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE EKSPERTINIO TYRIMO METODAS

Daktaro disertacijos santrauka
Technologijos mokslai, informatikos inžinerija (T 007)

2020, Kaunas

Disertacija rengta 2015–2019 m. Kauno technologijos universiteto Informatikos fakultete, Kompiuterių katedroje.

Mokslinis vadovas:
Prof. dr. Jevgenijus TOLDINAS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija, T 007).

Redagavo: Aurelija Gražina Rukšaitė (leidykla „Technologija“)

Informatikos inžinerijos mokslo krypties disertacijos gynimo taryba:
prof. dr. Rimantas BUTLERIS (Kauno technologijos universitetas, technologijos mokslai, informatikos inžinerija, T 007) – **pirmininkas**;
prof. habil. dr. Gintautas DZEMYDA (Vilniaus universitetas, informatikos inžinerija, T 007),
doc. dr. Nikolaj GORANIN (Vilniaus Gedimino technikos universitetas, informatikos inžinerija, T 007),
prof. dr. Rytis MASKELIŪNAS (Kauno technologijos universitetas, informatikos inžinerija, T 007),
doc. dr. Raimundas MATULEVIČIUS (Tartu universitetas, Estija, technologijos mokslai, informatikos inžinerija, T 007).

Disertacija bus ginama viešame Informatikos inžinerijos mokslo krypties disertacijos gynimo tarybos posėdyje 2020 m. rugpjūčio 28 d. 10 val. Kauno technologijos universiteto disertacijų gynymo salėje.

Adresas: K. Donelaičio g. 73-403, 44249 Kaunas, Lietuva.
Tel. (370) 37 30 00 42; faks. (370) 37 32 41 44; el. paštas doktorantura@ktu.lt.

Disertacijos santrauka išsiųsta 2020 m. liepos 31 d.
Kauno technologijos universiteto (K. Donelaičio g. 20, Kaunas), Vilniaus Gedimino technikos universiteto (Saulėtekio al. 14, Vilnius) bibliotekose bei internete (http://ktu.edu).

ĮVADAS

Problemos formulavimas

Kompiuteriuose saugomų duomenų kiekis kasmet sparčiai auga, dėl to nusikaltimų elektroninėje erdvėje skaitmeninių įkalčių ekspertinis tyrimas reikalauja daug laiko, nes reikia ištirti didelį duomenų kiekį ir iš jų išskirti nusikaltimų įkalčius. Ekspertinis tyrimas prasideda nuo kiekvieno skaitmeninėje laikmenoje esančio turinio rinkimo, kopijavimo ir autentifikavimo. Paskesniuose žingsniuose nagrinėjami gauti duomenys ir iš jų, taikant įvairius metodus bei įrankius, išskiriami nusikaltimo įkalčiai. Moksliniuose darbuose nagrinėjami nusikaltimų elektroninėje erdvėje skaitmeninių įkalčių paieškos karkasai, metodai bei modeliai. Tačiau specializuoto metodo bei įrankio, padedančio ekspertui sumažinti tiriamų duomenų imtį bei spręsti nusikaltimų elektroninėje erdvėje skaitmeninių įkalčių paieškos ir identifikavimo problemas, kol kas nėra, nes nėra pakankamai specializuotų įrankių bei metodų, skirtų ekspertiniam tyrimui automatizuoti.

Lietuvos Respublikos terminų bankas teikia aprobuotą termino ekspertinis tyrimas (angl. *Forensic investigation*) apibrėžtį: „Proceso įstatymų ir Lietuvos Respublikos teismo ekspertizės įstatymo nustatyta tvarka teismo eksperto ar specialisto atliekamas tyrimas, kuriam reikia specialių žinių (teismo ekspertizė, objektų tyrimas ir konsultacija)“. Lietuvos Respublikos teismo ekspertizės įstatyme Nr. IX-1161 eksperto specialios žinios apibūdinamos kaip „išsilavinimo ir specialaus pasirengimo arba profesinės veiklos dėka įgytos išsamios mokslo, technikos, meno ar bet kokios kitos žmonių veiklos srities žinios, reikalingos ekspertizei atlikti“. Nusikaltimai elektroninėje erdvėje (angl. *Computer crime*) atliekami pasitelkus kompiuterius, kompiuterinius tinklus, šiuolaikines informacines technologijas. Šių nusikaltimų skaitmeninių įkalčių (angl. *Digital evidence*) paieškai atlikti reikalingos specifinės eksperto žinios bei techninės priemonės, nes neteisėto veiksmo įrankiu tampa kompiuteris (jame esantys duomenys) arba kompiuterinės technologijos naudojamos informacijai rinkti, nusikalstamai veiklai planuoti ir vykdyti bei neteisėtiems duomenų mainams.

Darbo aktualumas

Nusikaltimų elektroninėje erdvėje tyrimas kelia daug iššūkių teisėsaugai ir asmenims, atsakingiems už informacijos saugumo

užtikrinimą. Pagrindiniai yra šie: supratimas apie nagrinėjamų objektų specifiką ir galimybė juos tinkamai išanalizuoti; įstatymų, reglamentuojančių bendruosius nusikaltimų tyrimo procesus, žinojimas, naujų teisinių dokumentų, reglamentuojančių elektroninę erdvę, žinojimas; gebėjimas įvertinti įvairias rizikas. Aukščiau išvardyti iššūkiai paskatino nusikaltimų elektroninėje erdvėje skaitmeninių įkalčių tyrimo priemonių, modelių ir metodų tobulėjimą, o tai lėmė vis didėjančius reikalavimus ekspertams. Tačiau nusikaltėliai taip pat tapo atsargesni ir supranta, kad jų veiksmus galima sekti, o palikti skaitmeniniai pėdsakai vėliau gali tapti įkalčiais teisme. Naujausios tendencijos rodo, kad nusikaltėliai imasi priemonių apsunkinti ekspertų darbą, taikydami duomenų šifravimo metodus, naudodami automatizuotas priemones skaitmeniniams įkalčiams slėpti ir vengdami tiesiogiai naudoti savo kompiuterius nusikaltimams daryti.

Specializuoti metodai ir įrankiai gali sumažinti skaitmeninių įkalčių paieškai analizuojamų duomenų imtį, padėti ekspertui išskirti skaitmeninius įkalčius bei sutrumpinti ekspertizės atlikimo laiką.

Tyrimo objektas

Šios disertacijos tyrimo objektas – nusikaltimų elektroninėje erdvėje tyrimo metodai, skirti ekspertinio tyrimo procesui pagerinti, sutrumpinant skaitmeninių įkalčių paieškos laiką.

Darbo tikslas

Pagrindinis disertacijos tikslas yra pagerinti nusikaltimų elektroninėje erdvėje ekspertinio tyrimo procesą, pasiūlant ekspertinio tyrimo metodą, kuris padėtų ekspertui surasti skaitmeninius įkalčius, leistų sumažinti ekspertinio tyrimo duomenų imtį bei sutrumpintų skaitmeninių įkalčių paieškos laiką.

Darbo uždaviniai

Disertacijos tikslui pasiekti ir mokslinei problemai spręsti darbe iškelti šie uždaviniai:

1. Išanalizuoti egzistuojančius metodus, modelius ir priemones, skirtus nusikaltimų elektroninėje erdvėje ekspertiniam tyrimui.
2. Sukurti naują metodą, kuris apimtų naudotojų įpročių profiliavimo ir skaitmeninių įkalčių objekto modelius;
3. Eksperimentiškai patikrinti ir įvertinti sukurtą įrankį, atliekant nusikaltimų elektroninėje erdvėje skaitmeninių įkalčių paiešką.

Mokslinių tyrimų metodika

Darbo tikslui pasiekti buvo naudojami šie tyrimo metodai:

1. Egzistuojančių nusikaltimų elektroninėje erdvėje ekspertinio tyrimo metodų, modelių ir įrankių lyginamosios literatūros lyginamosios analizės metodai.
2. Pasiūlytam metodui bei ontologija pagrįstos skaitmeninės nusikaltimų tyrimo srities transformacijos, naudotojų įpročių profiliavimo, skaitmeninių įkalčių objekto modeliams pagrįsti ir įvertinti atliktas eksperimentinis tyrimas, naudojant sukurtą įrankį.
3. Tyrimų ir analizės rezultatų struktūrizuoto įvertinimo ir apibendrinimo metodas.

Darbo mokslinis naujumas

Darbo mokslinis naujumas pagrįstas šiais rezultatais:

1. Pasiūlytas įpročių atributų profiliavimo metodas, skirtas nusikaltimų elektroninėje erdvėje skaitmeninių įkalčių paieškai;
2. Pasiūlytas dviejų pakopų ontologija pagrįstas transformacijos modelis ir ontologija pagrįsta transformacijos sistema, leidžianti parinkti tinkamą nusikaltimų elektroninėje erdvėje skaitmeninių įkalčių paieškos įrankį;
3. Pasiūlytas nusikaltimų elektroninėje erdvėje skaitmeninių įkalčių objekto modeliu grįstas metodas.

Disertacijos rezultatų praktinė vertė

Sukurtas ir eksperimentiškai ištirtas nusikaltimų elektroninėje erdvėje skaitmeninių įkalčių paieškos įrankis, kuris:

1. Leidžia sumažinti ekspertinio tyrimo duomenų imtį;
2. Remiantis įpročių atributų profiliavimo ir skaitmeninių įkalčių objekto modeliais, sudaro ekspertui sąlygas greičiau įvertinti įrankio pateiktus rezultatus ir iš jų išskirti skaitmeninius įkalčius;
3. Gali būti panaudotas, kai reikia operatyviai įvertinti nusikaltimų elektroninėje erdvėje skaitmeninius įkalčius.

Ginamieji teiginiai

1. Įpročių atributų profiliavimo metodas leidžia sumažinti ekspertinio tyrimo duomenų imtį, skirtą nusikaltimų elektroninėje erdvėje skaitmeninių įkalčių paieškai.
2. Skaitmeninio įkalčio objekto modelis leidžia atrinkti orientuotą į

galimai nusikaltimą padariusį asmenį sumažintą reprezentacinių duomenų imtį, taip padedant ekspertui priimti sprendimą bei sumažinti ekspertinio tyrimo laiką.

3. Įpročių atributų profiliavimo ir skaitmeninio įkalčio objekto modeliais grįstą metodą galima taikyti nusikaltimų elektroninėje erdvėje ekspertinio atvejo analizei atlikti, taip pat ir pritaikius automatizuotą įrankį.

Darbo rezultatų aprobavimas

Disertacijos rezultatai aprobuoti trijose tarptautinėse mokslinėse konferencijose. Paskelbti du straipsniai su citavimo indeksu „Clarivate Analytics Web of Science“ duomenų bazių recenzuojamuose žurnaluose:

1. Grigaliūnas, Šarūnas; Toldinas, Jevgenijus; Venčkauskas, Algimantas. An ontology-based transformation model for the digital forensics domain // Elektronika ir elektrotechnika. Kaunas: KTU. ISSN 1392-1215. eISSN 2029-5731. 2017, vol. 23, iss. 3, p. 78-82. DOI: 10.5755/j01.eie.23.3.18337.
2. Šarūnas Grigaliūnas, Jevgenijus Toldinas. „Habits Attribution and Digital Evidence Object Models Based Tool for Cybercrime Investigation“. Baltic J. Modern Computing, Vol. 8 (2020), No. 2, 275-292. DOI: 10.22364/bjmc.2020.8.2.05.

Disertacijos struktūra

Mokslinį darbą sudaro disertacijos įvadas, penki skyriai, bendros išvados, literatūros sąrašas, autoriaus publikacijų sąrašas ir priedai. Bendra disertacijos apimtis – 98 puslapiai, be priedų. Tekste yra 31 paveikslas ir 23 lentelės. Disertacijos tekste buvo panaudotos 208 nuorodos.

1. NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE EKSPERTINIO TYRIMO METODAI

Tendencijos rodo, kad smarkiai padidėja išpuolių mastas, rafinuotumas, skaičius ir rūšys, aukų skaičius ir ekonominė žala. Kai kuriose interneto dalyse naudojami anoniminimo metodai, kurie leidžia vartotojams laisvai bendrauti, nerizikuojant būti atsektiems. Tai yra visiškai teisėtos priemonės piliečiams apsaugoti savo privatumą. Tačiau šių privatumo tinklų ypatybės taip pat ypač domina nusikaltėlius, kurie masiškai piktnaudžiauja tokiu anonimiškumu neteisėtai prekybai narkotikais, ginklais, pavogtomis prekėmis, neteisėtu skaitmeninio turinio platinimu ir naudojimu, neteisėtos informacijos ir anoniminių tekstų platinimu, suklastotais asmens tapatybės dokumentais, vaikų seksualiniu išnaudojimu ir kt. Šiame skyriuje analizuojami egzistuojantys nusikaltimų elektroninėje erdvėje ekspertinio tyrimo metodai ir jų taikymo galimybės skaitmeninių įkalčių paieškai.

1.1. Nusikaltimų elektroninėje erdvėje skaitmeniniai įkalčiai

Europos Tarybos Konvencijoje dėl kibernetinių nusikaltimų *Cybercrime* terminas vartojamas plačiam nusikalstamų veikų, atliekamų prieš duomenis ir turinį, įskaitant autorinių teisių pažeidimą, spektrui apibūdinti. Jungtinių Tautų Žinyne dėl kompiuterinių nusikaltimų prevencijos ir kontrolės į kibernetinių nusikaltimų apibrėžimą įtraukti ir sukčiavimas, klastojimas bei nepageidaujama prieiga. Plačiausiai kibernetinius nusikaltimus apibrėžia (Nance ir Ryan, 2011) kaip „bet kokį nusikaltimą, kuris yra įvykdomas arba kuriam palengvinti naudojamas kompiuteris, kompiuterių tinklas arba techninis įtaisas“.

Apibendrintas apibrėžimas lietuvių kalba ir jo motyvacija pateikta (Goranin ir Mažeika, 2011): „NEE (Nusikaltimai elektroninėje erdvėje) *plačiąja prasme* apibrėžiami kaip bet kokie nusikaltimai, kuriems įvykdyti vienaip ar kitaip buvo panaudotos kompiuterinės technologijos, o nusikaltimo faktui įrodyti turi būti taikomos specifinės NEE tyrimo priemonės.“

Europos Tarybos Konvencija dėl kibernetinių nusikaltimų skiria 4 skirtingus nusikalstamų veiksmų tipus:

1) nusikaltimai prieš kompiuterinių duomenų ir sistemų konfidencialumą, vientisumą ir pasiekiamumą;
2) su kompiuteriu susiję nusikaltimai;
3) su turiniu susiję nusikaltimai;

4) su autorinėmis teisėmis susiję nusikaltimai.

Taigi, nusikaltimai elektroninėje erdvėje yra tradicinių nusikaltimų kaip technologinio proceso pasekmė. Tai išplėtė tradicinių nusikaltimų erdvę naujomis galingesnėmis priemonėmis, galimybėmis ir naujais nusikalstamų veikų tikslais ir siekiais. Analizuojant nusikaltimų elektroninėje erdvėje priemones, informacijos ir ryšių technologijos (IRT) padidina nusikalstamų veikų greitį ir imtį.

Didėjant kibernetinių nusikaltimų mastui, sudėtingumui ir išmanumui, reikia naujų metodų nusikaltimams elektroninėje erdvėje aptikti, skaitmeniniams įkalčiams išskirti, atliekant informacinių sistemų duomenų analizę. Plečiantis socialiniams tinklams, socialinis kibernetinių nusikaltimų mastas ir galimas poveikis ypač išaugo. Atsižvelgiant į dabartines kibernetinių nusikaltimų vystymosi tendencijas, ateityje numatomas ryškus su autorinių teisių pažeidimu susijusių kibernetinių nusikaltimų skaičiaus augimas. Šią grėsmę tinkamai atremti galima tik kuriant ir plėtojant tinkamus nusikaltimų elektroninėje erdvėje skaitmeninių pėdsakų aptikimo metodus, kurie ne tik padėtų aptikti sukčius, bet ir galėtų padėti atskleisti pedofilijos, autorių teisių, tapatybės (t. y. asmenis, nelegaliai platinančius legaliai įsigytą skaitmeninį turinį) nusikaltimus. Kiekvieną paminėtą nusikaltimą reikia ištirti ir tai padaryti kaip galima greičiau ir tiksliau. Lietuvos teismo ekspertizės centro (LTEC) informacinių technologijų ekspertizės išvadų pateikimas klasifikuojamas taip:

1. Kategoriška teigiama išvada: formuluojama, kai yra pakankama požymių visuma.
2. Tikėtina: trūksta požymių kategoriškai išvadai formuluoti.
3. Nustatyti negalima: nepateikti visi būtini tyrimui objektai arba ne visos tyrimo objektų dalys, tyrimo objektai sugadinti, neveikiantys, LTEC nėra techninių priemonių.

Ekspertinių tyrimų eilės Lietuvos policijos kriminalistinių tyrimų centre (LPKTC) ir Lietuvos teismo ekspertizės centre (LTEC, 2016) sudaro nuo 9 iki 12 mėnesių (1.1 1.1 lentelė. Ekspertinių tyrimų eilės Lietuvos policijos kriminalistinių tyrimų centre (LPKTC) ir Lietuvos teismo ekspertizės centre (LTEC)**.**).

1.1 lentelė. Ekspertinių tyrimų eilės Lietuvos policijos kriminalistinių tyrimų centre (LPKTC) ir Lietuvos teismo ekspertizės centre (LTEC)

Ekspertinio tyrimo rūšis	**Eilė LPKTC (mėnesiais)**	**Eilė LTEC (mėnesiais)**
Informacinių technologijų tyrimai	9	12

Toks oficialus tyrimo laikas formuluoja užduotį mokslui prisidėti sprendžiant kriminalistinių tyrimų problemą – sutrumpinti skaitmeninių įkalčių surinkimo ir pateikimo laiką.

Skaitmeninių įkalčių tyrimas – tai mokslo ir technologijų naudojimas faktams, kurie patiekiami kriminaliniuose ar civiliniuose teismuose, nustatyti. Terminas „skaitmeninis kriminalistinis tyrimas“ žymi teismo ekspertizės procesą, kuris taiko ekspertinius principus ir procesus skaitmeninei informacijai analizuoti, turint tikslą nustatyti įvykių seką, kuri suformavo tiriamą incidentą. Skaitmeninė informacija yra svarbiausia, norint sėkmingai ištirti tokius incidentus. Jeigu organizacija nėra tinkamai pasiruošusi tokiems incidentams, tai labai tikėtina, kad galimi įkalčiai nebus pasiekiami.

Literatūroje (Kävrestad, 2018) autoriai sugrupavo pasirengimą skaitmeniniam kriminalistiniam tyrimui į tokias tematines kategorijas: strategija, politika ir procedūros, technologija, skaitmeninės teisinės ekspertizės atsakymas, laikymasis ir stebėjimas. Sprendimas įgyvendinti organizacijos pasirengimo skaitmeniniams kriminalistiniams tyrimams programą turi būti strateginis organizacijos sprendimas. Kiekviena organizacija turi turėti tam tikrą politikos ir procedūrų formą, kad nurodytų organizacijos nariams jų veiksmus ir veiklas. Ypač svarbu, kad organizacija, kuri įgyvendina pasirengimo skaitmeninių įkalčių teisinei ekspertizei programą, įsigytų tinkamą aparatinę ir programinę įrangą skaitmeniniams įkalčiams surinkti ir saugoti. Įgyvendinus pasirengimo skaitmeninei teisinei ekspertizei programą, reikia stebėti jos tolimesnę eigą.

Jei organizacija įgyvendino pasirengimo skaitmeniniams kriminalistiniams tyrimams programą, ji gali taikyti skaitmeninių teisinių tyrimų procesus, norėdama atsakyti į saugumo incidentą.

Labiausiai darbui imlus yra skaitmeninės teisinės ekspertizės tyrimo procesas. Mokslininkai šiam etapui taip pat skiria daugiausia dėmesio. NIST (Nacionalinis standartų ir technologijų institutas) apibrėžė keturis

skaitmeninių kriminalistinių tyrimų proceso etapus: surinkimas, tyrimas, analizė ir ataskaita. Nepriklausomai nuo situacijos, skaitmeninių įkalčių ekspertizės procesą sudaro šie keturi pagrindiniai etapai:

Surinkimas. Pirmasis proceso etapas yra skirtas identifikuoti, suklasifikuoti, užrašyti ir išgauti duomenis iš galimų duomenų šaltinių, laikantis nustatytų procedūrų duomenų vientisumui užtikrinti. Surinkimas paprastai atliekamas iškart, atsižvelgiant į tikimybę prarasti laikinuosius duomenis (tinklo prisijungimai, akumuliatoriais maitinama įranga, mobilieji telefonai, IoT, prieglobos tarnybinės stotys ir pan.).

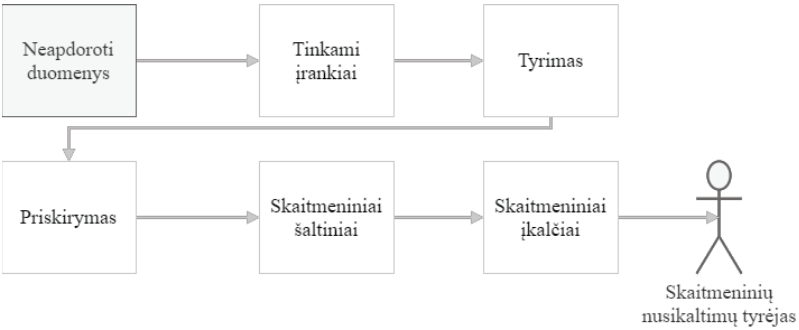
Tyrimas. Tyrimą sudaro didelių informacijos kiekių ekspertinis apdorojimas, taikant automatizuotus arba rankinius metodus dominančiai informacijai surinkti ir įvertinti, tuo pat metu užtikrinant duomenų vientisumą. Šioje fazėje labai svarbu tinkamai pasirinkti įrankį, kuriuo bus atkuriama informacija.

Analizė. Kitas analizės etapas yra skirtas, panaudojant teisiškai priimtinus metodus ir modelius, tyrimo rezultatams išanalizuoti ir išgauti naudingą informaciją, kuri atsakytų į tyrimui svarbius klausimus. Šioje fazėje daugiausia užtrunkama laiko (1.1 1.1 lentelė. Ekspertinių tyrimų eilės Lietuvos policijos kriminalistinių tyrimų centre (LPKTC) ir Lietuvos teismo ekspertizės centre (LTEC).).

Ataskaita. Galutinis proceso etapas yra rezultatų pateikimas, kuris gali apimti atliktus veiksmus, paaiškinimus, kaip ir kokie įrankiai bei metodai (modeliai) buvo pasirinkti tolimesnių veiksmų nustatymams atlikti, bei rekomendacijos įrankiams ir kitiems ekspertizės aspektams. Pateikimo formalumas gali kisti priklausomai nuo situacijos (teismo byla, privatus tyrimas).

Skaitmeninių pėdsakų paieškos išlaidos tam tikram tikėtinam skaitmeniniam įkalčiui atkurti yra įvertinamos kaip numatomas (paprastai vidutinis) tyrėjo darbo valandų skaičius, padaugintas iš apytikslio (paprastai vidutinio) tyrėjo valandos įkainio (įskaitant pridėtines išlaidas), pridedant valandines bet kurio specialisto naudojimo išlaidas.

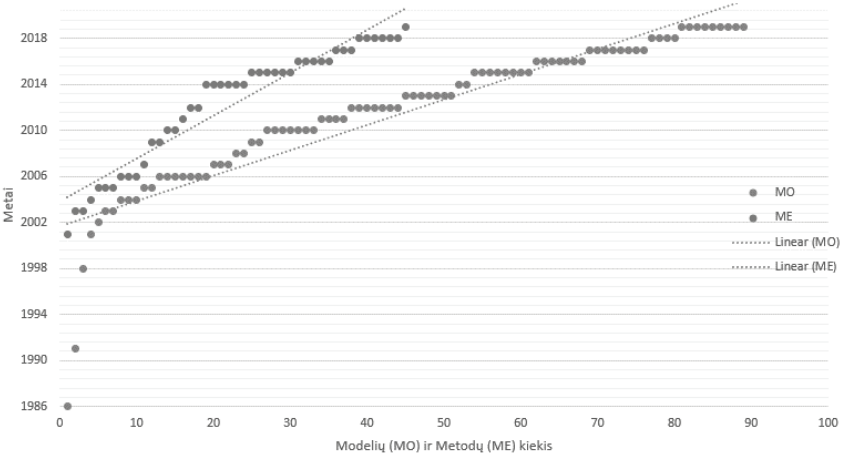
Šešių skaitmeninių įkalčių gavimo veiksmų apžvalga pateikta paveiksle (1.1 1.1 pav. Įkalčių gavimo veiksmų tyrimo procesas).



1.1 pav. Įkalčių gavimo veiksmų tyrimo procesas

Tikėtinų įkalčių pėdsakų svorius ar įrodomąsias vertes suderina, normalizuoja ir įvertina patyrę ekspertai. Skaitmeninių įkalčių kriminalistikos iššūkis, atkuriant tikėtinų įkalčių pėdsakus, – sukurti modelius ir metodus, kurie pateiktų pagrįstus rezultatus, kartu apsaugodami realius skaitmeninius įkalčius ir jų informaciją nuo sunaikinimo. Būtent tokia eiga panaudota šiame darbe. Pirmoje eilėje bet kokių skaitmeninių įkalčių atkūrimas pasirenkant tinkamiausią įrankį. Toliau seka tyrimas ir atributų klasifikavimas taikant modelius. Vėliau metodo taikymas juos priskiriant prie skaitmeninių nusikaltimų pėdsakų, o pačioje pabaigoje – prie skaitmeninių nusikaltimo įkalčių. Taikant modelius ir metodą atributų kiekio sumažinimas gali pasitarnauti ekspertui taupant laiko sąnaudas ir priimant sprendimą.

Analizės skyrelyje buvo apžvelgti 88 modeliai ir 45 metodai. Per pastaruosius penkerius metus pastebėta, kad pasiūlytų naujų metodų skaičius sumažėjo (2 pav.). Pastebėta tendencija parodo, kad, augant ekspertizės duomenų kiekiui, kurį reikia apdoroti, naujai sukuriamų metodų skaičius smarkiai atsilieka.



1.2 pav. Skaitmeninių įkalčių tyrimo modelių ir metodų kiekio augimo tendencija

Išanalizuoti metodai supaprastina užduotį, bet neatsako į pagrindinį tyrėjo klausimą: kas padarė nusikaltimą elektroninėje erdvėje? Skaitmeniniai įkalčiai turėtų kuo tiksliau identifikuoti įtariamąjį. Skaitmeninių įkalčių teismo ekspertizė yra labai svarbus sektorius pasaulyje. Esamų tradicinių skaitmeninių įkalčių paieškos priemonių nepakanka kibernetiniams nusikaltimams tirti. Norint ištirti nusikaltimus elektroninėje erdvėje, reikia sukurti novatoriškus skaitmeninės teismo ekspertizės parengties tyrimo metodus.

Taigi, kalbant apie metodus ir modelius, aiškiai matomas pasiūlytų metodų, kurie palengvina kibernetinių nusikaltimų tyrimus ir sumažina laiko sąnaudas, skaičiaus mažėjimas ateityje.

1.2. Pirmojo skyriaus išvados ir darbo tikslų formulavimas

Pirmajame šio darbo skyriuje apžvelgiami skaitmeniniai įrodymai, ekspertinio tyrimo procesas ir šioje srityje atlikti tyrimai. Didesnis dėmesys skirtas esamų įrankių, metodų, karkasų ir modelių, naudojamų skaitmeniniams įrodymams tirti, analizei. Buvo padarytos šios išvados:

1. Atlikus sisteminę mokslinių dokumentų kibernetinių nusikaltimų teismo ekspertizės srityje analizę, paaiškėjo, kad dauguma 2002–2009 m. darbų buvo parašyti naudojant bendruosius skaitmeninio tyrimo metodus

ir modelius. Šių problemų temų nagrinėjimo svarba mokslo visuomenėje rodo, kad tai yra aktualu. Tačiau vis dar trūksta metodų, kurie suvienodintų skaitmeninių įrodymų objektus ir teiktų pirmenybę įrodymams, sumažindami skaitmeninio tyrimo laiką ir išlaidas.

2. Yra daugybė prieinamų ekspertinio tyrimo priemonių – nuo atskirų paketų iki sudėtingų integruotų priemonių, sukurtų plačiam nusikaltimų tyrimui atlikti. Pirmas klausimas (prieš pradedant tyrimą) – kaip pasirinkti tinkamą tyrimo įrankį, kuris konkrečiu atveju bus tinkamas. Tinkamo įrankio pasirinkimas jau šiame etape gali smarkiai sutrumpinti tyrimo laiką.

3. Palyginti esami elektroninių nusikaltimų ekspertinio tyrimo metodai, modeliai ir sistemos. Palyginimas įrodė, kad nėra vieno pranašesnio metodo, modelio ar sistemos, galinčių padengti eksponentinio skaitmeninės informacijos augimo apimtį pagrindinėmis su elektroniniais nusikaltimais susijusiomis sritimis. Taigi, norint sutelkti dėmesį į ekspertizės laiko ir išlaidų sumažinimą, reikia naujo, holistinio elektroninio nusikalstamumo ekspertinio tyrimo metodo. Palyginimo metu pažymėjome, kad dažniausiai naudojami vertinimai yra priminimas, tikslumas, f-matas, kuris pagrįstas TP, TN, FP. Be to, atvejo analizė yra dažniausiai naudojama eksperimentų strategija.

4. Kita problema, su kuria susiduria šiuolaikiniai skaitmeninių nusikaltimų tyrėjai, yra poreikis kurti veiksmingas metodikas ir kurti efektyvias priemones. Rezultatai parodė, kad dauguma analizuotų priemonių yra tinkamos kompiuterinių sistemų kriminalistiniam tyrimui ir orientuotos į informacijos poėmį iš kompiuterinės sistemos plataus spektro neapdorotų duomenų. Tai patvirtina idėją, kad trūksta priemonių, kurios turėtų galimybę padėti ekspertams skaitmeninių įrodymų tyrimo procese.

Remiantis išvadomis tikslui pasiekti suformuluoti šie uždaviniai:

1. Pasiūlyti naują nusikaltimų skaitmeninių įkalčių ekspertinio tyrimo pertvarkymo sistemą, kuri padėtų ir palengvintų skaitmeninių įrodymų tyrimo ekspertinį darbą.

2. Pasiūlyti naują skaitmeninių įrodymų tyrimo modelį, naudojant įpročių priskyrimo profiliavimo metodą per savybių profiliavimo ir įpročių sričių analizę, siekiant sumažinti skaitmeninių naudotojo rinkinio objektų skaičių paieškos seką.

3. Pasiūlyti naują skaitmeninių įrodymų objekto modelį, kuriame būtų informatyviai sujungtas nusikaltimo tyrimo procesas su objektyvaus

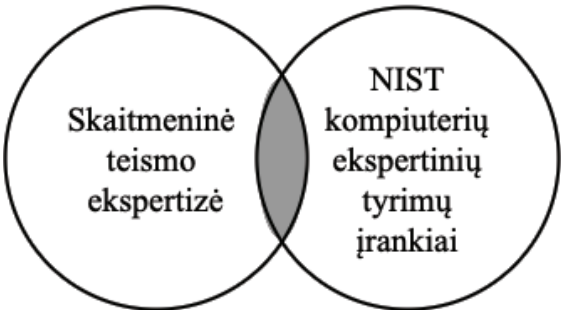
programavimo modeliu, siekiant sumažinti analizei reikalingų duomenų kiekį ekspertui ir padėti ekspertui priimti sprendimus, kai reikia atsakyti į klausimą, kas padarė nusikaltimą.

2. SIŪLOMAS DVIEJŲ PAKOPŲ ONTOLOGIJA PAGRĮSTAS TRANSFORMACIJOS MODELIS, SKIRTAS EKSPERTINIAM TYRIMUI ATLIKTI

Šio skyriaus objektas yra skaitmeninių įkalčių atkūrimas ir įrankių naudojimas, siekiant rasti naudotojų nusikaltimų elektroninėje erdvėje skaitmeninius įkalčius: įrenginyje, profilyje, namų kataloge ir kt. Siūlomas modelis koncentruojasi į skaitmeninių įkalčių tyrimą, kuriame naudojami du domenai:

1. Kibernetinės ekspertizės ontologija – CFO (*Cyber Forensics Ontology* (Brinson, Robinson, & Rogers, 2006);
2. NIST kompiuterinių ekspertinių tyrimo įrankių katalogas – NIST CFTC (NIST, 2019) N*NIST Computer Forensic Toll Catalog* – Forensic Tool.

Ontologijų CFO ir CFTCO bendra aibė tarp kibernetinės teismo ekspertizės ir NIST kompiuterių ekspertinių tyrimo įrankių domenų pavaizduota 2.1 paveiksle.



2.1 pav. Santykis tarp skaitmeninės teismo ekspertizės ir NIST kompiuterių ekspertinių tyrimo įrankių

Nors abi ontologijos priklauso tai pačiai skaitmeninės kriminalistikos sričiai, jos skiriasi iš esmės. Kaip įprasta, teismo ekspertas arba skaitmeninių įkalčio ekspertas dirba naudodamas CFO domeną. Kita

vertus, skaitmeninių įkalčių tyrimo priemonių NIST taksonomija pateikiama naudojant CFTC domeną.

Formaliai ontologija apibrėžiama kaip pora $O = (D, R)$, čia D domenas ir R sąryšių tarp domeno D ir $R \subseteq D^n$ elementų rinkinys.

Siekiant aprašyti siūlomą ontologija pagrįstą transformacijos modelį, suformuluotas aksiomų rinkinys:

Aksioma A1: Jeigu O_{cf} yra kompiuterių ekspertizės domeno ontologija ir E_{xcf} – atitinkantis CFO domenui XML elementas, tai egzistuoja funkcija $f_{cf}: O_{cf} \to E_{xcf}$.

Aksioma A2: Jeigu O_{cftc} yra kompiuterinių ekspertinių tyrimo įrankių katalogo domeno ontologija ir E_{xcftc} – atitinkantis CFTCO domeną XML elementas, tai egzistuoja funkcija $f_{cftc}: O_{cftc} \to E_{xcftc}$.

Aksioma A3: Jeigu E_{xcf} yra atitinkantis CFO domeną XML elementas ir O_{cftc} yra CFTC domeno ontologija, tai egzistuoja funkcija $g_{cf} \circ f_{cf}: E_{xcf} \to O_{cftc}$.

Aksioma A4: Jeigu E_{xcftc} yra atitinkantis CFTCO domeną XML elementas ir O_{cf} yra CFO ontologija, tai egzistuoja funkcija $g_{cftc} \circ f_{cftc}: E_{xcftc} \to O_{cf}$.

Remiantis aksiomų rinkiniu, pasiūlytas ontologija pagrįstas transformacijos modelis, skirtas ekspertiniam tyrimui atlikti, aprašomas taip:

$$TM(O) = \left(O_{cf}, f_{cf}, E_{xcf}, O_{cftc}, f_{cftc}, E_{xcftc}, g_{cf}, g_{cftc}\right). \quad (1)$$

Ontologija pagrįsto transformacijos modelio pagrindu pasiūlyta daugiasluoksnė OBTS (angl. *ontology-based transformation model system*) sistema, kuri naudoja XML dokumentų transformacijas CFO ir CFTCO ontologijų atspindžiams vienos į kitą ir atvirkščiai.

2.1. Antrojo skyriaus išvados

1. Išanalizavus elektroninių nusikaltimų elektroninėje erdvėje ekspertinio tyrimo įrankius paaiškėjo, kad yra daugybė kompiuterinių teismo ekspertizės priemonių ir nėra sprendimų, kaip pasirinkti tinkamą įrankį. CFO ir CFTCO sukūrė bendrus apibrėžimus skaitmeninių įkalčių

ekspertinio tyrimo ekspertizės srityje. Nors abu priklauso tai pačiai ekspertizės sričiai, jie yra labai skirtingi ir susikerta tik dideliu skaičiumi artefaktų, išreikštų per ontologijas. Paprastai kriminalistikos ekspertai veikia atsižvelgdami į CFO, tačiau NIST taksonomija kriminalistikos priemonėms, skirtoms skaitmeniniams įrodymams tirti, pateikiama CFTC terminais.

2. Siūlomas dviejų pakopų pertvarkymo modelis suteikia sinerginį požiūrį atliekant nusikaltimų elektroninėje erdvėje ekspertinio tyrimo srities (CFO) ir NIST taksonomijos kriminalistikos priemonių srities (CFCTO) skaitmeninių įrodymų tyrimą, keičiant ontologijas iš CFO į CFTCO ir atvirkščiai. Modelyje siūloma sukurti CFML ir CFCTO ontologijų XML, kuris užtikrintų labai lankstų pusiau struktūruotą dokumentą su žymės pagrindu sukurta struktūra, pritaikytą duomenų struktūrai universalizuoti. Siūlomas modelis pritaikytas XML dokumentų transformavimo taisyklėms (XDT) aprėpti, kad būtų galima susieti CFO ir CFTCO XML vienas su kitomis.

3. Siūloma daugiasluoksnė architektūra ir ontologija pagrįsta transformavimo sistema (OBTS), kur realizuojamas siūlomas modelis ir XDT, gali pasitarnauti ekspertams, dirbantiems nusikaltimų elektroninėje erdvėje ekspertinio tyrimo srityje, sutrumpinti laiką atliekant tyrimo įrodymų atranką pagal NIST priemonių katalogą, reikalingą tinkamam įrankiui pasirinkti. Atvejo analizėje buvo sukurtas pertvarkymo taisyklių rinkinys ir pademonstruota, kad OBTS paverčia CFO į NIST priemonių sąrašą ir gali padėti ekspertams parinkti tinkamą įrankį tolesniam skaitmeninių įrodymų tyrimui atlikti.

4. Daugiasluoksnė transformacijos sistema ir dviejų pakopų nusikaltimų elektroninėje erdvėje ekspertinio tyrimo srities transformacijos modelis nuo esamų sprendimų išsiskiria tuo, kad turi svarbių CFO ir CFCTO sričių ontologijų integraciją ir apibrėžtas XDT transformacijas tarp jų.

3. SIŪLOMAS ĮPROČIŲ ATRIBUTŲ PROFILIAVIMO MODELIS

HiD (angl. *Habbit Attribution*) modelis pagrįstas metodu, kuris apima naudotojo vietos (pvz., namų katalogas) skaitmeninių profilių gavimą, palyginimą ir atpažinimą. Identifikavimas atliekamas lyginant skaitmeninį pirmąjį profilį, gautą iš kompiuterio ar primontuoto atvaizdo, pridedant prie žinomo objekto profilius, gautus iš kitų skaitmeninių

prietaisų, su kuriais šie nusikaltimai galimai buvo padaryti, tačiau su šiuo prietaisu nėra patikimai susiję. Pažymėtina, kad principas, kuriuo grindžiamas modelis, yra dvipusis, t. y. jis taip pat gali prasidėti nuo vartotojo skaitmeninio „anoniminio“ profilio, kad būtų galima palyginti su kitų prietaisų profiliais (kurie taip pat nėra tiesiogiai susiję su nusikalstama veika), kurie buvo priskirti tam tikriems atvejams ar naudotojams (Schultz ir Shumway, 2002).

Uždavinio formalizavimas buvo adaptuotas iš (Štuikys, Burbaitė ir Bespalova, 2015). Turime keturis rinkinius: (*E*) – skaitmeninių įkalčių rinkinį, (*S*) – paieškos taisyklių rinkinį, (*P*) – aparatūros profilio atributų rinkinį, (*D*) – vartotojo prietaisų rinkinį. Kiekvienas rinkinys turi savo variantus. Panaudodami įvestus rinkinius, siūlome tokią skaitmeninių įkalčių tyrimo seką:

$$\begin{Bmatrix} e_1 \\ \dots \\ e_i \\ \dots \\ e_n \end{Bmatrix} \rightarrow \begin{Bmatrix} s_1 \\ \dots \\ s_i \\ \dots \\ s_m \end{Bmatrix} \rightarrow \begin{Bmatrix} p_1 \\ \dots \\ p_i \\ \dots \\ p_k \end{Bmatrix} \rightarrow \begin{Bmatrix} d_1 \\ \dots \\ d_i \\ \dots \\ d_l \end{Bmatrix}. \quad (2)$$

Įvertinę (2), turėsime bendrą sekų skaičių $|E|\times|S|\times|P|\times|D|$. Sekos turi apribojimų, tokių kaip tyrėjo įkalčių pirmenybė arba paieškos taisyklė, kuri gali turėti įtakos pasirinkus D variantus. Pavyzdžiui, ekspertas įkalčių gali ieškoti tarp tam tikrų tipų failų ar aplankų.

HiD metodo pagrindu įvedame įpročių rinkinį $H = \{h_i\},\ i = [1, m]$, iš tų pačių HiD, įpročių atributų rinkinį $A = \{a_j\},\ j = [1, q]$ ir paieškos taisyklių kūrimo funkciją *f(SR)* (3).

$$f(SR) = H \cup A. \quad (3)$$

Paieškos taisyklių funkcijai $f(SR)$ sukurti yra remiamasi šiomis prielaidomis:

- kompiuterio vartotojas yra žmogus, linkęs pritaikyti visas aplinkybes, su kuriomis bendrauja pagal savo įpročius;
- įpročio atpažinimo būdui gali būti taikomi atributai;
- Priskirtų įpročių profilį galima naudoti paieškos taisyklėms kurti.

Tuomet paieškos taisyklių rinkinį $\{s_1, \dots, s_i, \dots, s_m\}$ pakeičiame suskaičiuotu funkcijų rinkiniu (4):

$$\begin{Bmatrix} e_1 \\ \dots \\ e_i \\ \dots \\ e_n \end{Bmatrix} \rightarrow \begin{Bmatrix} f(sr_1) \\ \dots \\ f(sr_i) \\ \dots \\ f(sr_m) \end{Bmatrix} \rightarrow \begin{Bmatrix} p_1 \\ \dots \\ p_i \\ \dots \\ p_k \end{Bmatrix} \rightarrow \begin{Bmatrix} d_1 \\ \dots \\ d_i \\ \dots \\ d_l \end{Bmatrix}. \quad (4)$$

Įvertinę (4), turėsime seką $|E|\times|F(SR)|\times|P|\times|D|$. Sekos turi apribojimų, tokių kaip tyrėjo įkalčių pirmenybė arba paieškos taisyklė, kuri gali turėti įtakos pasirinkus D variantus. Pavyzdžiui, ekspertas įkalčių gali ieškoti tarp tam tikrų tipų failų ar aplankų (3).

Tolesniam formalizavimui atlikti naudosime pasiūlytą rinkinį (4). Darome prielaidą, kad šiuos apribojimus galima išreikšti naudojant suvaržymo operatorius ir pogrupį (angl. *requires_any_of*, *excludes* and *subset*).

Jei turime įkalčių rinkinius iš naudotojo įrangos $E\{e_1, e_2\}$, paieškos taisyklių rinkinio funkcijos $F(SR)\{sr_1, sr_2, sr_3, sr_4\}$, profilių rinkinio funkcijos $P\{p_1, p_2\}$, naudotojo skaitmeninių įkalčių rinkinio funkcijos $D\{d_1, \dots, d_i, \dots d_l\}$, tai darome prielaidą, kad tyrėjas ieškos dviejų įrodymų. Turimose keturiose paieškos taisyklių reikšmėse, apskaičiuotose pagal rinkinį (4), bus tiriami du profiliai (du įrenginiai, paimti tyrimui), o konfiskuotuose įrenginiuose gali būti daugybė failų ir aplankų bei įrodymai.

Mes turime *Nv* =16 variacijų pagal (5), kurios kiekviena turės pogrupius iš *D*:

$$N_v = |E| \times |F(SR)| \times |P| . \quad (5)$$

Darome prielaidą, kad ekspertas naudos paieškos įkalčius $\{e_1, e_2\}$, apibrėžiamus taisyklėmis (6–9), kur $\{e_1\}$ nustatomas pagal $f(sr_2)$ ir $f(sr_3)$ paieškos taisyklių kūrimo funkcijos reikšmes (7), o $\{e_2\}$ – pagal $f(sr_1), f(sr_2), f(sr_3)$ paieškos taisyklių kūrimo funkcijos reikšmes (9).

Pasirinktos paieškos taisyklės kūrimo funkcija $f(sr_1)$ reikalauja $\{p_2\}$ profilio (12) ir paieškos taisyklės kūrimo funkcijos reikšmių $f(sr_2), f(sr_3)$, kurioms reikia bent vieno $\{p_1, p_2\}$ profilio (13). Pagal pasirinktus profilius failai ir aplankai bus tiriami kaip skaitmeniniai įkalčiai (10,11).

$$\{e_1\}\ excludes\ \{f(sr_1), f(sr_4)\}; \quad ((6)$$

$\{e_1\}\, requires\_any\_of\, \{f(sr_2), f(sr_3)\}$; ((7)
$\{e_2\}\, excludes\, \{f(sr_4)\}$; ((8)
$\{e_2\}\, requires\_any\_of\, \{f(sr_1), f(sr_2), f(sr_3)\}$; ((9)
$\{p_1\}\ requires\, \{d_1, \dots, d_i, \dots d_l\}$; ((10)
$\{p_2\}\ requires\, \{d_1, \dots, d_i, \dots d_l\}$; ((11)
$\{f(sr_1)\}\, requires\, \{p_2\}$; ((12)
$\{f(sr_2), f(sr_3)\}\, requires\ any\ of \{p_1, p_2\}$. ((13)

Tarkime, $SD = subset\{d_1, \dots, d_i, \dots d_l\}$, ir mes užrašysime įkalčių tyrimo sekas taip:

$e_1 \rightarrow f(sr_2) \rightarrow p_1 \rightarrow SD;\ e_1 \rightarrow f(sr_2) \rightarrow p_2 \rightarrow SD;$ (14)
$e_1 \rightarrow f(sr_3) \rightarrow p_1 \rightarrow SD;\ e_1 \rightarrow f(sr_3) \rightarrow p_2 \rightarrow SD;$ (15)
$e_2 \rightarrow f(sr_1) \rightarrow p_2 \rightarrow SD;$ (16)
$e_2 \rightarrow f(sr_2) \rightarrow p_1 \rightarrow SD;\ e_2 \rightarrow f(sr_2) \rightarrow p_2 \rightarrow SD;$ (17)
$e_2 \rightarrow f(sr_3) \rightarrow p_1 \rightarrow SD;\ e_2 \rightarrow f(sr_3) \rightarrow p_2 \rightarrow SD.$ (18)

Naudodamiesi siūlomu modeliu, kai paieškos taisyklės kūrimo funkcija įvertina įpročių rinkinius ir jų atributus, galime sumažinti D sekos rinkinio skaičių (kaip pateikta mūsų pavyzdyje, nuo *šešiolikos iki devynių*).

3.1. Pasiūlyto skaitmeninių įkalčių tyrimo modelio naudojant įpročių profiliavimo metodą atvejo analizė

Norint pademonstruoti skaitmeninių įkalčių tyrimo modelio profiliavimo metodo galimybes, buvo atlikti du bandymai.

1 bandymas. Įkalčiai e_1 surinkti iš naudotojo standžiojo disko failų. Paieškos rezultatas su reikšmėmis $f(sr_2)$ ir $f(sr_3)$ – atrinkta 60 failų, kuriuose yra įkalčių artefaktų.

2 bandymas. Įkalčiai e_2 surinkti iš naudotojo standžiojo disko failų momentinės kopijos. Paieškos rezultatas su reikšmėmis $f(sr_1)$, $f(sr_2)$ ir $f(sr_3)$ – atrinkta 30 failų, kuriuose yra įkalčių artefaktų.

Kiekybinis bandymų rezultatų vertinimas pateiktas žemiau (3.1 lentelė).

3.1 lentelė. Skaitmeninių įkalčių tyrimo bandymų rezultatai naudojant įpročius

	Įkalčiai e_1, surinkti iš naudotojo kietojo disko		**Įkalčiai e_2, surinkti iš naudotojo kietojo disko momentinės kopijos**	
	Failų skaičius	Išeiga (efektyvumas)	Failų skaičius	Išeiga (efektyvumas)
Prieš testavimą	15429	0%	15097	2,2%
Pašalinta po $f(sr_1)$ pritaikymo	Netaikoma		332	
Tyrimas po $f(sr_1)$ pritaikymo	15429		14765	
Failų, kuriuose yra įkalčių, skaičius	125	48%	250	12%
Failų, kuriuose yra įkalčių, skaičius, pritaikius $f(sr_2), f(sr_3)$	60		30	

Po to, kai buvo pritaikytos $f(sr_2)$ ir $f(sr_3)$, kurios naudojamos kaip paieškos taisyklės, susijusios su įkalčiais e_1, surinktais iš naudotojo standžiojo disko failų, bandymo rezultatai rodo 48% išeigos efektyvumą. O tada, kai buvo pritaikytos $f(sr_1)$, $f(sr_2)$ ir $f(sr_3)$, kurios naudojamos kaip paieškos taisyklės, susijusios su įkalčiais e_2, surinktais iš naudotojo standžiojo disko momentinės kopijos failų, bandymo rezultatai rodo 2,2% ir 12% išeigos efektyvumą.

Priskirtų įpročių profilio kūrimas prasideda nuo visos informacijos, kuri gali būti surinkta iš skaitmeninio įrenginio naudotojo paliktos skaitmeninės liekanos, tyrimo ir analizės. Kompiuterio naudotojas yra žmogus, linkęs pritaikyti aplinką, su kuria jis sąveikauja. Toks aprašytas metodas tinka skaitmeniniams įrenginiams tirti. Tai galima taikyti asmeniniams kompiuteriams, planšetiniams kompiuteriams, išmaniesiems telefonams, daiktų interneto įrenginiams ir pan.

3.2. Trečiojo skyriaus išvados

1. Atlikta priskyrimo, profiliavimo ir įpročių sričių analizė parodė, kad nusikaltimų elektroninėje erdvėje ekspertinis tyrimas, siekiant surasti skaitmeninius nusikaltimo įrodymus skaitmeninėse naudotojų vietose (prietaisas, profilis, namų katalogas ir kt.), yra daug platesnės apimties nei kitose analogiškose srityse. Metaduomenys ir kiti žurnaliniai įrašai gali būti naudojami siekiant priskirti veiksmus įtariamajam nustatyti. Siūlomas sisteminis požiūris į nagrinėjamų analizuojamų sričių problemą naudojant ypatybių diagramos modelį. Siūlomame įpročių identifikavimo srities (HiD) modelyje nagrinėjamas profiliavimo metodas, kuris remiasi priskiriamais įpročiais ir orientuojasi į įpročių, jų požymių ir profilių specializaciją.

2. Siūlomu HiD modeliu pagrįstas metodas išskiria iš esamų sprendimų tuo, kad integruoja specifinius metodus, priimtus iš intelektinio ir tradicinio profiliavimo, kad būtų galima gauti informacijos, kuri padėtų sukurti skaitmeninį profilį su įtariamo naudotojo įpročių atributais, o tada į jį atsižvelgti tiriant įrodymus.

3. Priskiriamų įpročių profilio kūrimas prasideda tiriant ir analizuojant visą informaciją, kurią galima surinkti iš skaitmeninių pėdsakų, naudotojų paliktų skaitmeniniame įrenginyje. Kompiuterio naudotojai yra žmonės, linkę prisitaikyti visas aplinkas, su kuriomis sąveikauja. Taigi jie negali išvengti (net nesąmoningai) aptiktų ir palygintų su jų pačių įpročiais skaitmeninių įrodymų artefaktų.

4. Šiame skyriuje aprašytas modelis tinka skaitmeniniams įrenginiams, tokiems kaip asmeniniai kompiuteriai, planšetiniai kompiuteriai, išmanieji telefonai ir kt., tirti. Siūlomo skaitmeninių įrodymų tyrimo modelio, pagrįsto įpročių priskyrimo metodo testo rezultatais, analizė rodo 48% efektyvumą, kai išgaunami naudotojo standžiojo disko failai po bendrojo tyrimo, kuriame yra įrodymų objektai, su failais, turinčiais įrodymų objektų. Pritaikius siūlomas metodo funkcijas, kai įrodymai surinkti iš failų, esančių naudotojo standžiojo disko momentiniame atvaizde, išeigos efektyvumas yra 12%.

4. SIŪLOMAS NUSIKALTIMŲ ELEKTRONINĖJE ERDVĖJE SKAITMENINIŲ ĮKALČIŲ OBJEKTO MODELIU GRĮSTAS METODAS

Disertacijoje pasiūlytas skaitmeninio įkalčio objekto (*Digital Evidence Object – DEO*) modelis, pagrįstas tinkamos teismo ekspertizės proceso metu išgautos informacijos analize, naudojant kategorijų teorijos elementus (Delvenne, 2019), atsižvelgiant į 5W (***W**hy, **W**hen, **W**here, **W**hat, **W**ho*) (Miranda Lopez, Moon ir Park, 2016). Pasiūlytam DEO modeliui formalizuoti panaudota kategorijų teorija, nes ji yra gerai įsitvirtinusi kompiuterių mokslo srityje ir rado šalininkų keliose kitose srityse (Delvenne, 2019). Ji puikiai tinka atviroms, autonominėms ir tinklų dinaminėms sistemoms modeliuoti, todėl ji taip pat gali būti naudojami skaitmeniniams objektams apibūdinti.

Pasiūlyto DEO modelio tikslas – formalizuoti skaitmeninio teismo ekspertizės tyrimo proceso etapą, sumažinti analizuojamų duomenų kiekį iš kompiuterinės sistemos ar skaitmeninio prietaiso, kad būtų galima pagreitinti skaitmeninių įkalčių gavimą ir jų ištyrimą. Modelis atitinka JAV teisingumo departamento rekomendacijas, kuriose buvo apibrėžti keturi pagrindiniai teismo proceso etapai: rinkimas, nagrinėjimas, analizė ir ataskaitų teikimas. Tyrimo etapas suskirstytas į dvi dalis: dokumentų atrinkimas (dokumentai patvirtina jo turinį ir būklę) ir duomenų redukcija. Duomenų mažinimo dalis tyrimo fazėje yra labai svarbi dėl didžiulio kiekio duomenų ir informacijos, saugomos kompiuterinėse sistemose.

4.1. Skaitmeninių įkalčių objekto modelio pagrindimas

Nagrinėdami fizinį nusikaltimą, tyrėjai analizuoja įvykių objektus, kad nustatytų įkalčių objektus. Tyrimo tikslas – kuo daugiau sužinoti apie objektų istoriją nusikaltimo vietoje. Skaitmeninių įkalčių istorija apima kompiuterių sistemose įvykusius įvykius. Istorija apima visus vartotojus, taip pat ir programas, operacinę sistemą ir kitus procesus. Kitaip tariant, ekspertas turi rasti atsakymus į 5W klausimus: kodėl, kada, kur, ką ir galiausiai kas padarė nusikalstamo veiklą. Ekspertas turi daryti prielaidas apie ankstesnius ryšius tarp skaitmeninių objektų ir įvykių, paremtų galutine ir galbūt tarpine kompiuterinės sistemos būsenomis.

DEO modelis formaliai apibrėžiamas penkiais kintamaisiais:

$$DEO = (W_{hy}, W_{hen}, W_{here}, W_{hat}, W_{ho}). \quad (19)$$

W_{hy} apibrėžiamas penkių kintamųjų rinkiniu:

$$W_{hy} = \{CD, IE, FI, CPV, CA\}; \quad (20)$$

čia *CD* – nusikalstama žala, *IE* – pramoninis šnipinėjimas, *FI* – finansiniai tyrimai, *CPV* – organizacijos politikos pažeidimas, *CA* – piktnaudžiavimas vaikais.

W_{hen} apibrėžiamas trijų kintamųjų rinkiniu:

$$W_{hen} = \{BT_{inv}, ET_{inv}, \Delta T_{inv}\}; \quad (21)$$

čia BT_{inv} – pradžios laikas, nurodantis tyrimo laikotarpio pradžią, ET_{inv} – pabaigos laikas, nurodantis tyrimo laikotarpio pabaigą, ΔT_{inv} – laiko trukmė tarp tiriamojo laikotarpio laiko verčių.

W_{here} apibrėžiamas dviejų kintamųjų rinkiniu:

$$W_{here} = \{S, P\}; \quad (22)$$

čia *S* – tyrimo šaltinis, *P* – tyrimo vieta.

W_{hat} apibrėžiamas trijų kintamųjų rinkiniu:

$$W_{hat} = \{BT_{ev}, ET_{ev}, \Delta T_{ev}\}; \quad (23)$$

čia BT_{ev} – pradžios laikas, nurodantis, kad tuo metu buvo pradėtas tyrimas, ET_{ev} – pabaigos laikas, nurodantis tą laiką, kai baigėsi tyrimas, ΔT_{ev} – laiko trukmė tarp iš eilės tiriamų įvykių.

W_{ho} apibrėžiamas dviejų kintamųjų rinkiniu:

$$W_{ho} = \{U, E\}; \quad (24)$$

čia U – asmuo, vykdantis nusikalstamą veiklą, E – subjektas (procesas, byla, katalogas, registras ar sistemos įrašas ir kt.), kuris vyksta nusikalstamos veikos metu.

DEO modeliui suformuluotos šios prielaidos:

Jei $f_1 : W_{hy} \rightarrow W_{hen}$ ir jei $g_1 : W_{hen} \rightarrow W_{ho}$, tada egzistuoja kompozicija $h_1 = g_1 \circ f_1 : W_{hy} \rightarrow W_{ho}$.

Jei $f_2 : W_{hen} \rightarrow W_{here}$ ir jei $g_2 : W_{hhere} \rightarrow W_{ho}$ tada

egzistuoja kompozicija $h_2 = g_2 \circ f_2 : W_{hen} \rightarrow W_{ho}$.

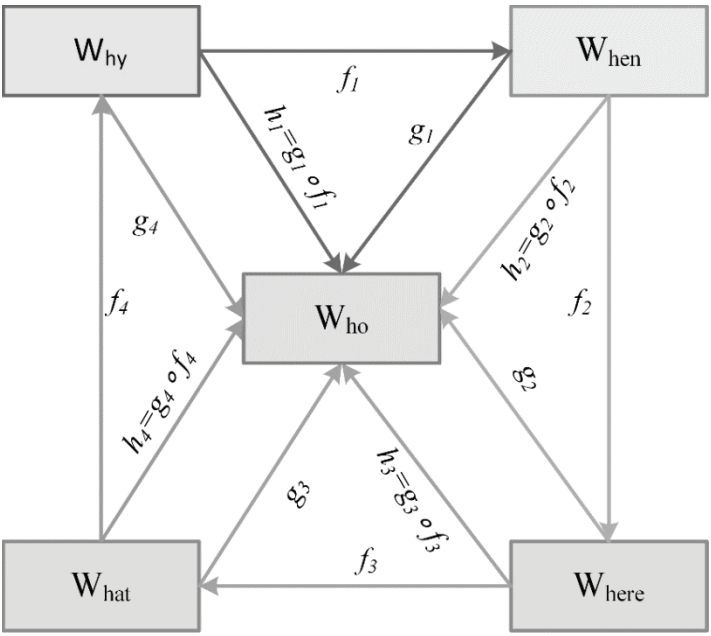
Jei $f_3 : W_{here} \rightarrow W_{hat}$ ir jei $g_3 : W_{hat} \rightarrow W_{ho,}$ tada egzistuoja kompozicija $h_3 = g_3 \circ f_3 : W_{here} \rightarrow W_{ho}$.

Jei $f_4 : W_{hat} \rightarrow W_{hy}$ ir jei $g_4 : W_{hy} \rightarrow W_{ho}$, tada egzistuoja kompozicija $h_4 = g_4 \circ f_4 : W_{hat} \rightarrow W_{ho}$.

Apibrėžimas. Galima nustatyti DEO objektų rinkinį tyrimui, apskaičiuojant visų galimų n-vektorių aibę, kurių i-toji koordinatė priklauso aibei H_i:

$$H_1, \cdots, H_n = \{(h_1, \cdots, h_n) \mid h_i \in H_i \; for \; every \; i \in \{i, \cdots, n\}\}. \quad (25)$$

DEO modelis pateiktas žemiau (4.1 pav.).



4.1 pav. DEO modelis

Rezultatams įvertinti panaudotos tipinės metrikos, naudojamos informacijos paieškos ir klasifikavimo vertinimo srityse (Tharwat, 2018).

Neteisingas teigiamasis koeficientas (FPR) yra nesusijusių objektų santykis išgautų objektų rinkinyje:

$$FPR = \frac{C}{C+D}; \quad (26)$$

čia C – neaktyvių objektų, kurie buvo gauti, skaičius, D – nesusijusių objektų, kurie nebuvo gauti, skaičius.

4.2. Ketvirtojo skyriaus išvados

1. Esamų nusikaltimų elektroninėje erdvėje ekspertinių tyrimų ekspertizės metodų, modelių ir karkasų analizė parodė, kad nėra vieno aukštesnio lygio metodo, modelio ar sistemos, galinčių padengti eksponentinės skaitmeninės informacijos augimo apimtis skaitmeninių nusikaltimų srityje. Siūlomas naujas nusikaltimų elektroninėje erdvėje ekspertizės tyrimo „Digital Evidence Object“ (DEO) modelis yra pagrįstas kategorijų teorijos principais ir yra naudojamas nusikaltimų skaitmeninių įkalčių tyrimų analizei, atsižvelgiant į 5W (kodėl, kada, kur, kas ir kas), atlikti.

2. Modelis išsiskiria iš esamų sprendimų tuo, kad gali padėti intelektualiai vertinti situaciją laiko kritinių sprendimų priėmimų atžvilgiu ir automatizuoti paiešką nusikaltimų elektroninėje erdvėje ekspertizės srityje.

3. Pristatytas realaus atvejo tyrimas, skirtas padėti nusikaltimų elektroninėje erdvėje ekspertinių tyrimų ekspertui skaitmeninių įrodymų tyrimo procese dėl sukčiavimo, siekiant paslėpti kogeneracinės jėgainėje pagamintos bendros energijos kiekį. Gauti rezultatai įrodo, kad siūlomas DEO modelis gali formalizuoti nusikaltimų elektroninėje erdvėje ekspertizės proceso tyrimo etapą, sumažinti duomenų kiekį, gautą iš kompiuterinės sistemos ar skaitmeninio įrenginio, pagreitinti skaitmeninių įrodymų rinkimą ir pagerinti supratimą apie kibernetinę situaciją.

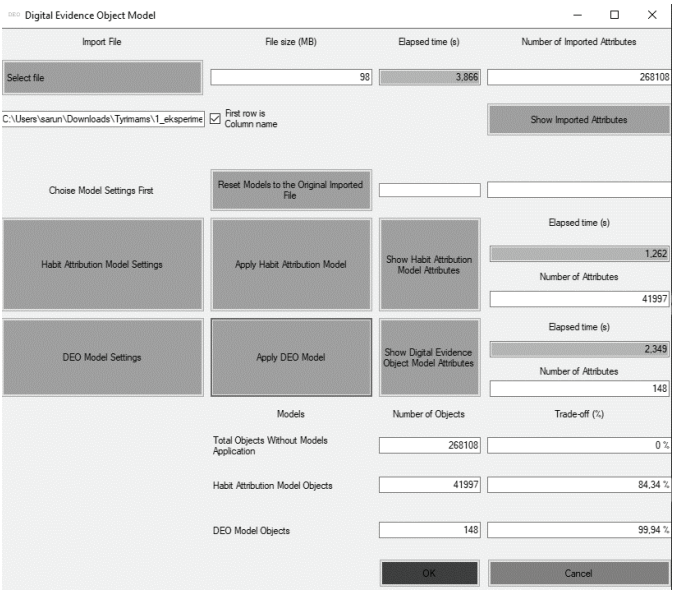
4. DEO modelis gali padėti nusikaltimų elektroninėje erdvėje tyrėjui sumažinti tiriamų duomenų kiekį. Vėliau analizuoti ir išgauti skaitmeninius įrodymus iš mažesnio informacijos kiekio ir mažesnio duomenų rinkinio. Ištyręs mažesnį informacijos ir duomenų kiekį iš kompiuterinės sistemos, nusikaltimų elektroninėje erdvėje ekspertas gali padidinti savo laiko efektyvumą ir sumažinti klaidų lygį. Gauti rezultatai rodo (TPR) 0,986, tikslumo (FPR) 0,001 ir F1 mato 0,002 vertes.

5. SIŪLOMŲ METODO EKSPERIMENTINIS TYRIMAS

Siūlomas metodas apima nusikaltimų tyrimo procesą su pasiūlytais modeliais ir tinkamas skaitmeninių įkalčių paieškas elektroninėje erdvėje. Jis leidžia kurti priemones elektroninių nusikaltimų tyrėjams, kurios sumažintų skaitmeninių pėdsakų tyrimų laiką ir pastangas.

NIST ir ISO / LEC teismo ekspertizės gairės (Ajijola, Zavarsky ir Ruhl, 2014) nurodo, kad teismo ekspertizė vykdoma penkiais etapais: (1) identifikavimas, (2) rinkimas ir (arba) įsigijimas, 3) išsaugojimas, (4) tyrimas ir analizė ir (5) ataskaitų rašymas. Pagrindinis darbo eksperimentinio tyrimo tikslas – pateikti pagrįstą ir patikimą DEO objektų visumą, kuri padėtų ekspertui surasti nusikaltimų elektroninėje erdvėje įkalčius.

Atliktas dviejų dalių eksperimentas. Eksperimentui atlikti sukurtas DEIC įrankis (5.1 pav.).



5.1 pav. Metodo įrankis kuriame realizuoti HiD ir DEO modeliai

Pirmojoje dalyje buvo naudojama dešimt skirtingų kompiuterių magnetinių diskų atvaizdų. Antrojoje buvo nagrinėjamas realus nusikaltimas. Išsamiau gautus rezultatus aprašome pagal antrąją dalį.

Eksperimentui pasirinkta informacinė sistema (IS), valdanti galios kogeneracinės jėgainės sistemą, sutrikusi dėl įtariamos įsilaužimo veiklos. Dėl šios priežasties 2016 m. kovo 22 d. elektrinės patalpa užsidegė, ir gamyklos savininkams buvo padaryta didelių nuostolių. Jėgainės draudimo bendrovė pradėjo tyrimą, kad nustatytų incidento priežastis. Buvo įtarta, kad IS žurnalai galėjo būti keičiami laikotarpiu nuo 2016 m. kovo 21 d. iki 2016 m. balandžio 1 d.

Tyrimo objektas. 40 GB „Samsung“ standusis diskas (HDD), kuris buvo konfiskuotas iš įtartinos kogeneracinės elektrinės tarnybinės stoties ir, laikantis nustatytos procedūros, padarytas šio standžiojo disko atvaizdas tolimesniam tyrimui atlikti. Atvaizdas primontuotas ekspertiniame kompiuteryje ir parengtas ketvirtajam teismo ekspertizės etapui – tyrimui ir analizei.

Tyrimo ir analizės prielaida. Teismo ekspertas žinojo apie sujungtą energetikos informacinę sistemą (CEIS), kuri buvo įdiegta konfiskuotame HDD. Pagrindinė įdiegtos CEIS užduotis yra kontroliuoti pagamintos kogeneruotos energijos kiekį. Dėl tam tikros priežasties (galbūt sukčiavimo, siekiant paslėpti pagamintos kogeneruotos energijos kiekį) sistema nepateikė realių duomenų arba tinkamai neveikė.

Eksperto iškeltos hipotezės. Įtariama, kad nusikalstamais veiksmais buvo modifikuota CEIS žurnalinių įrašų, informacija apie pagamintą elektros energiją (išeigą) buvo modifikuota ir galėjo būti pakeista. Galimas įtartinų veiksmų laikas – nuo 2016 m. kovo 21 d. iki 2016 m. balandžio 1 d. Ekspertas pasirinko tyrimo laikotarpį nuo 2016 m. sausio 1 d. iki 2016 m. balandžio 8 d., kad būtų nagrinėjama veiksmų seka prieš incidentą ir po jo.

Ekspertiniam tyrimui atlikti naudojami įrankiai. AutoPSY 4.9 (Basis Technology, 2019), Forensic Toolkit 5 (FTK) (AccessData, 2019) ir pasiūlytas DEIC įrankis (Grigaliūnas, 2019).

5.1. Eksperimentinio tyrimo rezultatai

Pagal nagrinėjamą disko atvaizdo rezultatą, naudodami DEIC programinę įrangą irtaikydami DEO modelį (5.1 lent.), darome šias išvadas (šis vaizdas paimtas iš tikrojo atvejo ir naudojamas antrojoje dalyje): pirmasis atvaizdas turi 268 108 atributus.

5.1 lentelė. Atributų skaičius DEO modelio panaudojimo atveju

Įkeltas įtariamojo magnetinio disko	Failo dydis (MB)	DEO užduoties atlikimo laikas (s)	Rastų atributų skaičius	DEO (Why)	DEO kelias iki Users (5W)	DEO kelias iki user (5W)	DEO Ext csv (5W)	DEO CAM (5W)
1	98	5,164	268108	38658	13401	10182	19924	153
2	89	4,175	245581	18495	10765	7749	3903	166
3	93	8,665	257531	37513	12691	9727	19926	127
4	196	16,066	536216	68679	18121	1522	39848	332
5	160	10,673	804324	115974	40137	30477	59778	39
6	297	14,835	804324	115974	40137	30477	59772	498
7	93	3,427	255989	36212	12591	9726	19924	90
8	490	19,498	1340544	193294	67005	50905	99630	150
9	98	4,25	267954	30649	13371	10157	19924	121
10	96	5,586	263783	37199	5322	4032	19163	70

Kadangi DEO modelyje egzistuoja galimybė pasirinkti visas priežastis: kodėl, kada, kur, ką ir kas (5W), tai, norint sumažinti atributų skaičių, ieškant naudotojų galima pasirinkti failo CAM parametrų paiešką, naudotojų namų katalogą, patį naudoją, failo plėtinį (csv) arba nuorodą į bet kokį failą, nustatymą. Lentelėje yra nurodyti sisteminiai naudotojai „user“ ir operacinės sistemos katalogai „Users“. Taigi, pačioje pabaigoje su „DEO Path CAM“ (5W) mes turime tik 153 atributus (5.2 lentelė), kuriuos turės ištirti bylos ekspertas, kad priimtų galutinį sprendimą. Tokiam sprendimui priimti prireiks 60,54 val. (naudojant COCOMO II laiko sąnaudų skaičiuoklę (Geeks for geeks, 2019)).

5.2 lentelė. Tyrimo laikas pritaikius DEO ir HiD modelius

DEO Atributai	Mėnesiai	Valandos	HiD Atributai	Mėnesiai	Valandos
153	0,38	60,54	10181	58,30	9327,62
166	0,42	66,77	13779	83,82	13411,70
127	0,30	48,42	9726	55,19	8829,65
332	0,96	153,39	10164	58,18	9308,94
39	0,07	11,74	30477	217,30	34768,76
498	1,56	249,52	30477	217,30	34768,76

90	0,20	32,03	9726	55,19	8829,65
150	0,37	59,12	50905	402,17	64347,99
121	0,29	45,68	10157	58,13	9301,24
70	0,15	23,69	15973	100,08	16013,50

Akivaizdu, kad kiekviename elektroninių nusikaltimų skaitmeniniame įkaltyje potencialiai yra arba gali būti nereikalingos informacijos. Taikant HiD ir DEO modelius, šios informacijos kiekį galima sumažinti iki 99,943 procentų. Antrojo (realaus) atvejo analizės rezultatai apibendrinti 5.3 lentelėje. Naudojant FTK įrankį informacijai surinkti, iš disko atvaizdo buvo atkurti 268 108 objektai. Naudojant AutoPSY, buvo atrinkti 194 103 objektai. Jei ekspertas nesinaudotų DEO modeliu, jis turėtų juos visus išanalizuoti rankiniu būdu. Tokiam uždaviniui atlikti jis užtruktų neprognozuojamą laiko kiekį, ir tyrimas galėtų užsitęsti metų metus. Pritaikius DEO modelį, labai sumažėjo analizuojamų duomenų kiekis. Modelis išskyrė 277 objektus skaitmeniniai įkalčių analizei atlikti.

5.3 lentelė. Eksperimentinio tyrimo rezultatai

Objekto tipas	**Surinkimas**	**Tyrimas**			**Analizė**
	FTK	**AutoPSY 4.9**	**DEO modelio n-vektorių aibę**		**Pritaikius DEO modelį**
			P_{App}	P_{Os}	
Archyvai	11692	1885	0	0	0
Duomenų bz.	11663	98	0	0	0
Dokumentai	54420	24621	1854	10643	110
E. paštas	3	0	0	0	0
Paleidžiamieji	82201	75901	687	142658	0
Grafikos	42009	33045	0	0	0
Interneto ir bendravimo	7373	0	0	0	0
Multimedijos	1860	1718	0	0	0
Šifruoti	3067	0	0	0	0
Kiti	14858	0	271	1784	47
Windows OS registras	26778	56835	8928	60618	24
Neidentifikuoti	12184	0	625	284	83
Iš viso:	268108	194103	12365	215987	277
			228352		

Įvertinome visų lyginamų metodų (įrankių) efektyvumą. Akivaizdu, kad vieno unikalaus sprendimo nėra, tačiau, taikant HiD ir DEO modelius, pavyko smarkiai sumažinti analizuojamų duomenų kiekį. Tai reiškia tik viena – eksperto laiko sąnaudos bus mažesnės.

Nagrinėdami aukščiau lentelėse pateiktus eksperimento rezultatus, akivaizdžiai matome HiD ir DEO modelių panaudojimo naudą (5.4 lent.). Svarbu tai, kad abu šie modeliai papildo vienas kitą ir sugeba pateikti rezultatus su nusikaltimų elektroninėje erdvėje įkalčius lydinčiais objektais, kuriuos galima peržiūrėti tyrimo pradžioje.

5.4 lentelė. Skaitmeninių įkalčių imties sumažinimas (kartais)

Įkeltas įtariamojo magnetinio disko atvaizdas	**HiD f(sr4) user**	**DEO Users (5W)**
1	26	20
2	18	23
3	26	20
4	53	30
5	26	20
6	26	20
7	26	20
8	26	20
9	26	20
10	17	50
Vidurkis	**27**	**24**

Jeigu tyrimo tikslas – maksimaliai greitai susidaryti galimo nusikaltėlio profilį, tai, naudodami HiD imties duomenų kiekį, galime sumažinti vidutiniškai iki 27 kartų. Naudojantis DEO modeliu ir nieko nežinant apie naudotoją, imties duomenų kiekį galima sumažinti vidutiniškai iki 24 kartų. Ekspertui nebereikia galvoti apie skaitmeninius įkalčius, kurie skirti informacinės sistemos veikimui užtikrinti. Tokio tipo objektai patenka į 5W modelio funkciją ir, neturėdami jokios vertės, yra pašalinami iš imties. DEO modelis turi dar vieną unikalią objektų imties supaprastinimo galimybę. Priklausomai nuo tyrime esančios informacijos, objektų kiekį galima sumažinti iki maksimaliai tikslingų (5.4 5.4 lentelė. Skaitmeninių įkalčių imties sumažinimas (kartais), stulpelis: DEO Path CAM (5W)). Tokį rezultatą DEO modelis pasiekia, kai žinome atlikto nusikaltimo preliminarią datą (*When*) ir ko (*What*) ieškome. Labai

naudinga žinoti kodėl (*Why*), jei, tarkime, tyrimas yra susiejamas su vaikų pornografija arba autorinių teisių pažeidimais. Žinojimas, kodėl (*Why*) taip įvyko, gali suformuoti DEO uždavinį, kad būtų galima sėkmingai rasti visus skaitmeninių įkalčių objektus, kurie patenka į mūsų tyrimo laiko intervalą „kada“ (*Where*). Modelis visais tyrimo atvejais nukreiptas į objektą „kas“ (*Who*), todėl ir turime rezultatą, kurį išanalizavę ekspertai gali išskirti tikrus įkalčius. Pagrindinis siūlomo metodo tikslas – sumažinti skaitmeninių įkalčių skaičių, tiriant nusikaltimus elektroninėje erdvėje, yra pasiektas. Eksperimentai su DEIC įrankiu pademonstravo realią galimybę sumažinti ekspertui analizuoti pateikiamą duomenų kiekį ir sutrumpinti nusikaltimų elektroninėje erdvėje skaitmeninių įkalčių radimo laiką.

5.2. Penktojo skyriaus išvados

1. Praktiniam siūlomų modelių įvertinimo rezultatui pasiekti buvo sukurtas skaitmeninio elektroninių nusikaltimų tyrimo (DEIC) įrankis. Naudojant DEIC įrankį, buvo atlikti nusikaltimų elektroninėje erdvėje tyrimai iš dešimties diskų vaizdų su skaitmeniniais įrodymais.
2. Naudojant siūlomą ontologija pagrįstą transformacijos sistemą, siūlomo metodo palyginamiesiems tyrimams atlikti buvo parinktas FTK įrankis. Iš eksperimento rezultatų galime aiškiai pamatyti HiD ir DEO modelių naudojimo pranašumus. Svarbu tai, kad abu šie modeliai papildo vienas kitą ir gali pateikti rezultatus su skaitmeninių įrodymų objektais, kurie buvo siūlomi peržiūrėti skaitmeninio nusikalstamumo tyrimo pradžioje.
3. Jei ekspertas turi informacijos apie įtartiną naudotoją, pavyzdžiui, naudotojo vardą, slapyvardį ar kt., jis (ji) galėtų naudoti „HiD“ tam, kad kuo greičiau sužinotų įtariamojo naudotojo profilį ir vidutiniškai 27 kartus sumažintų reprezentacinę objektų imtį pirmajai peržiūrai atlikti. Kai ekspertas nieko nežino apie įtartiną naudotoją, galima pritaikyti DEO modelį ir vidutiniškai 24 kartus sumažinti reprezentacinę objektų skaičių imtį atliekant pirmąją peržiūrą.

6. BENDROSIOS IŠVADOS

1. Yra daugybė prieinamų nusikaltimų elektroninėje erdvėje priemonių – nuo atskirų paketų iki sudėtingų integruotų įrankių, sukurtų plačiam nusikaltimų tyrimui. Išanalizavus nusikaltimų elektroninėje erdvėje metodus, modelius ir sistemas, paaiškėjo, kad nėra vieno aukštesnio lygio metodo, modelio ar sistemos, galinčių padengti eksponentinio skaitmeninės informacijos augimo apimtį pagrindinėse su kibernetinių nusikaltimų kriminalistika susijusiose srityse. Taigi, norint sutelkti dėmesį į ekspertizės laiko ir išlaidų sumažinimą, reikia naujo, holistinio nusikaltimų elektroninėje erdvėje ekspertizės metodo.
2. Naujai pasiūlyta daugiasluoksnė architektūra ir ontologija pagrįsta transformavimo sistema (OBTS), kurioje realizuojamas siūlomas modelis ir XDT, gali pasitarnauti ekspertams, dirbantiems nusikaltimų elektroninėje erdvėje srityje, sutrumpinti laiką, reikalingą tinkamam skaitmeniniam įrankiui iš NIST priemonių katalogo pasirinkti, kad būtų atliktas įrodymų tyrimas.
3. Naujai pasiūlytas metodas pagrįstas:
    - Įpročių identifikavimo srities (HiD) modelis nuo esamų sprendimų išsiskiria tuo, kad integruoja specifinius metodus, priimtus iš intelektinio ir tradicinio profiliavimo, kad būtų galima gauti informacijos, kuri padėtų sukurti skaitmeninį profilį su įtariamo naudotojo įpročių atributais, o tada į jį atsižvelgti tiriant įrodymus;
    - Skaitmeninių įrodymų objekto (DEO) modelis išsiskiria iš esamų sprendimų tuo, kad gali padėti intelektualiai vertinti situaciją laiko kritinių sprendimų priėmimų atžvilgiu ir automatizuoti paiešką nusikaltimų elektroninėje erdvėje ekspertizės srityje.
4. Tais atvejais, kai ekspertas turi tam tikros informacijos apie įtartiną naudotoją, pavyzdžiui, naudotojo vardą, slapyvardį ar kt., jis galėtų naudoti „HiD“, kad kuo greičiau sužinotų įtariamojo naudotojo profilį ir vidutiniškai 27 kartus sumažintų reprezentacinę objektų imtį pirmajai peržiūrai.
5. Tais atvejais, kai ekspertas nieko nežino apie įtartiną naudotoją, galima pritaikyti DEO modelį ir vidutiniškai 24 kartus sumažinti reprezentacinę objektų skaičių imtį pirmajai peržiūrai.
6. Sukurtas DEIC (elektroninių nusikaltimų skaitmeninių įrodymų tyrimas) įrankis įrodo siūlomo metodo praktinį pritaikymą padėti nusikaltimų elektroninėje erdvėje ekspertizės specialistams ir įforminti

nusikaltimų elektroninėje erdvėje proceso ekspertizės etapą, sumažinant tiriamų duomenų kiekį iš įtartinos sistemos ar skaitmeninio įrenginio.

7. LITERATŪRA

1. ABDUL-GHANI, H. A., and D. KONSTANTAS.. A Comprehensive Study of Security and Privacy Guidelines, Threats, and Countermeasures: An IoT Perspective. *Journal of Sensor and Actuator Networks*. 2019, 8(2), 22.

2. ACCESSDATA. (). AccessData Group. *Forens ic Toolkit* (FTK). 2019. Prieiga internete: http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

3. AYERS, D. (). A second generation computer forensic analysis system. *Digital Investigation*. 2009, 6, S34–S42.

4. AJIJOLA, A., ZAVARSKY, P., & RUHL, R. (). *A review and comparative evaluation of forensics guidelines of NIST SP* 800-101 Rev.1:2014 and ISO/IEC 27037:2012. *World Congress on Internet Security* (WorldCIS-2014) (p. 66–73). Pristatytas 2014 World Congress on Internet Security (WorldCIS), London, United Kingdom: IEEE. 2014. [žiūrėta 2019-08-22]. Prieiga internete: http://ieeexplore.ieee.org/document/7028169/

5. AKBAL, E., DOGAN, S., & S. DOGAN. Forensics Image Acquisition Process of Digital Evidence. *International Journal of Computer Network and Information Security*. 2018, 10(5), 1–8.

6. ALABDULSALAM, S., SCHAEFER, K., KECHADI, T., & LE-KHAC, N.-A. Internet of Things Forensics – Challenges and a Case Study. G. Peterson & S. Shenoi (Sud.), *Advances in Digital Forensics XIV* (T. 532, 2018, p. 35–48). Cham: Springer International Publishing. [žiūrėta 2019-10-01]. Prieiga internete: http://link.springer.com/10.1007/978-3-319-99277-8_3

7. ALTHEIDE, C., CARVEY, H. A. *Digital forensics with open source tools*. Burlington, MA: Syngress, 2011.

8. ARSHAD, H., JANTAN, A. B., & O. I.ABIODUN. Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. *Journal of Information Processing Systems*. 2018, 14(2), 346–376.

9. ARXSYS. *Digital Forensics Framework* (DFF). 2019. Prieiga internete: https://github.com/arxsys/dff

10. ASHTON, K. That „Internet of Things“ Thing. *RFiD Journal*. 2009, 22(7), 97–114.

11. BAGGILI, I., BAABDALLAH, A., AL-SAFI, D., & MARRINGTON, A. Research Trends in Digital Forensic Science: An Empirical Analysis of Published Research. Marcus rogers & K. C. Seigfried-spellar (Sud.), *Digital Forensics and Cyber Crime* (2013, T. 114, p. 144–157). Berlin, Heidelberg: Springer Berlin Heidelberg. [žiūrėta 2019-09-30]. Prieiga internete: http://link.springer.com/10.1007/978-3-642-39891-9_9

12. BARSKE, D., STANDER, A., JORDAAN, J. A Digital Forensic Readiness

framework for South African SME's. 2010 *Information Security for South Africa* (2010, p. 1–6). Pristatytas 2010 Information Security for South Africa (ISSA), Johannesburg, South Africa: IEEE. [žiūrėta 2019-08-22]. Prieiga internete: http://ieeexplore.ieee.org/document/5588281/

13. BASHIR, M., & M. KHAN(. Triage in Live Digital Forensic Analysis. *The International Journal of Forensic Computer Science*. 2013, 8(1), 35–44.

14. Basis Technology*Autopsy*. 2019a. Prieiga internete: https://www.autopsy.com/

15. Basis Technology. *Sleuth Kit*. 2019b. Prieiga internete: http://www.sleuthkit.org/sleuthkit/

16. BEEBE, N. L., LIU, L. Ranking algorithms for digital forensic string search hits. *Digital Investigation*. 2014, 11, S124–S132.

17. BERLA. *Infotainment and Vehicle System Forensics (iVe*). 2019. Prieiga internete: https://berla.co/ecosystem/

18. BHANDARI, S., & V. JUSAS. An Abstraction Based Approach for Reconstruction of TimeLine in Digital Forensics. *Symmetry*. 2020, 12(1), 104.

19. BlackBag Technologies. (). *BlackLight*. 2019. Prieiga internete: https://www.blackbagtech.com/

20. BOEHM, B., VALERDI, R., LANE, J. A., & BROWN, A. W. (). COCOMO suite methodology and evolution. *CrossTalk*. 2005, (4), 20–25.

21. BOTTRILL, M. C., JOSEPH, L. N., CARWARDINE, J., BODE, M., COOK, C., GAME, E. T., GRANTHAM, H., et al. Is conservation triage just smart decision making? *Trends in Ecology & Evolution*. 2008, 23(12), 649–654.

22. BRAIN ADAMS, R. *The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practi*ce. Philosophy of Murdoch University, 2012.

[žiūrėtaPrieiga internete: http23. BRIAN D., C. *A hypothesis-based approach to digital forensic investigations*. 2006, may 1.

24. BRINSON, A., ROBINSON, A., & M. ROGERS. A cyber forensics ontology: Creating a new approach to studying cyber forensics. *Digital Investigation*. 2006, 3, 37–43.

25. BUCHANAN, B. (*Module Leader: Module number: Email: Telephone: Web page: Within ProfSIMS: MSN Messenger: Version*:, 139, 2011.

26. CANTER, D. Offender profiling and investigative psychology. *Journal of Investigative Psychology and Offender Profiling*. 2004, 1(1), 1–15.

27. CANTRELL, G., & D. DAMPIER. Implementing the Automated Phases of the Partially-Automated Digital Triage Process Model. *Journal of Digital Forensics, Security and Law*. 2012, 96–116.

28. CANTRELL, G., DAMPIER, D., DANDASS, Y. S., NIU, N., & C. BOGEN, (Research toward a Partially-Automated, and Crime Specific Digital Triage Process Model. *Computer and Information Science*. 2012, 5(2), p. 29.

29. CARRIER, B. (). *Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers*, 2003, 1(4), 12.

30. CARRIER, B. File system forensic analysis. Boston, Mass. ; London: Addison-Wesley, 2005.

31. CARRIER, B. D., & SPAFFORD, E. H. (s.a.). *An Event-Based Digital Forensic Investigation Framework*, 12.

32. CARRIER, B., & SPAFFORD, E. H. *Getting Physical with the Digital Investigation Process*, 2003, 2(2), 21.

33. CASEY, E. *Handbook of digital forensics and investigation*. Amsterdam ; Boston: Academic, 2010.

34. CASEY, E. Clearly conveying digital forensic results. *Digital Investigation*. 2018, 24, 1–3.

35. CASEY, E., BACK, G., & S. BARNUM. Leveraging CybOXTM to standardize representation and exchange of digital forensic information. *Digital Investigation*. 2015, 12, S102–S110.

36. CHABOT, Y., BERTAUX, A., NICOLLE, C., & M.-T. KECHADI. A complete formalized knowledge representation model for advanced digital forensics timeline analysis. *Digital Investigation*. 2014a, 11, S95–S105.

37. CHABOT, Y., BERTAUX, A., NICOLLE, C., & KECHADI, T. (). *Automatic Timeline Construction and Analysis for Computer Forensics Purposes*, 2014b. Unpublished. [žiūrėta 2020-05-17]. Prieiga internete: http://rgdoi.net/10.13140/2.1.3595.1040

38. CHEN, H., FININ, T., & A. JOSHI. An ontology for context-aware pervasive computing environments. *The Knowledge Engineering Review*. 2003, 18(3), 197–207.

39. COHEN, F. Toward a Science of Digital Forensic Evidence Examination. K.-P. Chow & S. Shenoi (Sud.), *Advances in Digital Forensics VI* (T. 337, p. 17–35). Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. [žiūrėta 2019-08-22]. Prieiga internete: http://link.springer.com/10.1007/978-3-642-15506-2_2

40. ĆOSIĆ, J., & BAČA, M. *A Framework to (Im)Prove „Chain of Custody" in Digital Investigation Process*, 2010, 5.

41. ĆOSIĆ, J., & ĆOSIĆ, Z. *The Necessity of Developing a Digital Evidence Ontology,* 2012. Unpublished. [žiūrėta 2020-05-17]. Prieiga internete: http://rgdoi.net/10.13140/RG.2.1.4184.5843

42. COSIC, J., COSIC, Z., & M. BACA. An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence. *Journal of Information and*

Organizational Sciences. 2011, 35. . Prieiga internete: https://pdfs.semanticscholar.org/f498/174e390ec63ac9d84948900b5a20028069e9.pdf

43. COSTANTINI, S., DE GASPERIS, G., & R. OLIVIERI. Digital forensics and investigations meet artificial intelligence. *Annals of Mathematics and Artificial Intelligence*. 2019, 86(1–3), 193–229.

44. CRUZ, F., MOSER, A., & M. COHEN. A scalable file based data store for forensic analysis. *Digital Investigation*. 2015, 12, S90–S101.

45. DALINS, J., WILSON, C., & M. CARMAN. Monte-Carlo Filesystem Search – A crawl strategy for digital forensics. *Digital Investigation*. 2015, 13, 58–71.

46. DAMAŠEVIČIUS, R., TOLDINAS, J., VENČKAUSKAS, A., GRIGALIŪNAS, Š., MORKEVIČIUS, N., & JUKAVIČIUS, V. Visual Analytics for Cyber Security Domain: State-of-the-Art and Challenges. R. Damaševičius & G. Vasiljevienė (Sud.), *Information and Software Technologies* (T. 1078, p. 256–270). Cham: Springer International Publishing, 2019. [žiūrėta 2020-03-27]. Prieiga internete: http://link.springer.com/10.1007/978-3-030-30275-7_20

47. DATTA, S., & C. PAN. An Intelligent Forensic Framework towards Cloud: Its Ontological Aspects. *International Journal of Computer Applications*. 2016, 138(9), 1–8.

48. DEFT Association. DEFT, 2019. Prieiga internete: http://www.deftlinux.net/

49. DELVENNE, J.-C. Category Theory for Autonomous and Networked Dynamical Systems. *Entropy*. 2019, 21(3), 302.

50. DOUGLAS, J. E., RESSLER, R. K., BURGESS, A. W., & C. R. HARTMAN. Criminal profiling from crime scene analysis. *Behavioral Sciences & the Law*, 1986, 4(4), 401–421.

51. DZEMYDIENE, D. *Intelligent decision support systems for assistance in forensic investigation procese.* Handbook of Electronic Security and Digital Forensics, 2010, 603–630.

52. ERVURAL, B. C., & ERVURAL, B. (). *Overview of Cyber Security in the Industry* 4.0 Era. Industry 4.0: Managing The Digital Transformation (p. 267–284). Cham: Springer International Publishing, 2018. [žiūrėta 2019-08-22]. Prieiga internete: http://link.springer.com/10.1007/978-3-319-57870-5_16

53. FELDMAN, R., & SANGER, J. *The text mining handbook: Advanced approaches in analyzing unstructured data*. Cambridge ; New York: Cambridge University Press, 2007.

54. FISKE, S. T., & TAYLOR, S. E. *Social cognition. MacGraw-Hill series in social psychology*. New York, NY: MacGraw-Hill, 1991.

55. COHEN, F. *Digital forensic evidence examination*. Place of publication not identified: Asp Press, 2009.

56. GARFINKEL, S. Digital forensics XML and the DFXML toolset. *Digital Investigation*. 2012, 8(3–4), 161–174.

57. GARFINKEL, S. L. Carving contiguous and fragmented files with fast object validation. *Digital Investigation*. 2007, 4, 2–12.

58. GARFINKEL, S. L. Digital forensics research: The next 10 years. *Digital Investigation*. 2010, 7, S64–S73.

59. GARFINKEL, S., MALAN, D., DUBEC, K.-A., STEVENS, C., & PHAM, C. (2006). Advanced Forensic Format: An Open Extensible Format for Disk Imaging. M. S. Olivier & S. Shenoi (Sud.), *Advances in Digital Forensics II* (T. 222, p. 13–27). Boston, MA: Springer New York. [žiūrėta 20190-10-02]. Prieiga internete: http://link.springer.com/10.1007/0-387-36891-4_2.

60. *Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018*. (2018, kovo 21). Prieiga internete: https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018

61. GEDDES, M., & ZADEH, P. B. *Forensic analysis of private browsing. 2016 International Conference On Cyber Security And Protection Of Digital Services (Cyber Security)* (p. 1–2). 2016. *Pristatytas 2016 International Conference On Cyber Security And Protection Of Digital Services* (Cyber Security), London, United Kingdom: IEEE. [žiūrėta 2019-08-22]. Prieiga internete: http://ieeexplore.ieee.org/document/7502341/

62. Geeks for geeks. *COCOMO Model,* 2019. Prieiga internete: https://www.geeksforgeeks.org/software-engineering-cocomo-model/

63. GIOVA, G. *Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems*, 2011, 11(1), 10.

64. GLADYSHEV, P. F*ormalizing Event Reconstruction in Digital Investigations*. University College Dublin. 2004. Prieiga internete: http://formalforensics.org/publications/thesis/

65. GORANIN, N., & MAŽEIKA, D. *Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos* (1-asis leid.), 2011. TEV. [žiūrėta 2020-03-29]. Prieiga internete:
http://www.ebooks.ktu.lt/eb/239/nusikaltimai_elektronineje_erdveje_ir_ju_tyrimo_metodikos/

66. GRABOSKY, D. P. *Computer Crime: A Criminological Overview*, 2010, 21.

67. GRIER, J., & G. G. RICHARD. Rapid forensic imaging of large disks with sifting collectors. *Digital Investigation*. 2015, 14, S34–S44.

68. GRIGALIUNAS, S., TOLDINAS, J., & A. VENCKAUSKAS.An Ontology-Based Transformation Model for the Digital Forensics Domain. *Elektronika ir Elektrotechnika*. 2017, 23(3), 78–82.

69. GRIGALIŪNAS, Š. *DEO Model Tool*, 2019. Prieiga internete: https://digitalevidenceobject.com/

70. GRIGALIŪNAS, Š., & TOLDINAS, J. *Data analysis methods for software systems. Digital evidence object model for cybercrime investigation*. Vilnius University, 2017. [žiūrėta 2020-03-28]. Prieiga internete: https://www.mii.lt/damss/index.php?page=doi_2017&lang=en

71. GRIGALIŪNAS, Š., & J. TOLDINAS. Habits Attribution and Digital Evidence Object Models Based Tool for Cybercrime Investigation. *Baltic J. Modern Computing*. 2020, 8, 275–292.

72. GROSOF, B. N., HORROCKS, I., VOLZ, R., & DECKER, S. (). *Description logic programs: Combining logic programs with description logic. Proceedings of the twelfth international conference on World Wide Web—WWW '03* (2003, p. 48). Pristatytas *The twelfth international conference*, Budapest, Hungary: ACM Press. [žiūrėta 2019-08-22]. Prieiga internete: http://portal.acm.org/citation.cfm?doid=775152.775160

73. HARICHANDRAN, V. S., WALNYCKY, D., BAGGILI, I., & F. BREITINGERCuFA: A more formal definition for digital forensic artifacts. *Digital Investigation*. 2016, 18, S125–S137.

74. HARRIS, R. Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem. *Digital Investigation*. 2006, 3, 44–49.

75. HENSELER, H., & HYDE, J. Technology assisted analysis of timeline and connections in digital forensic investigations. *The 2019 edition of the International Conference on Artificial Intelligence and Law* (ICAIL), 2019.

76. HIKMATYAR, M., PRAYUDI, Y., & I. RIADI. Network Forensics Framework Development using Interactive Planning Approach. *International Journal of Computer Applications*. 2017, 161(10), 41–48.

77. HOLDER, H. E., ROBINSON, O. L., & ROSE, K. *Electronic Crime Scene Investigation: An On-the-Scene Reference for First Responders* (No. NCJ 227050). United States. Office of Justice Programs, 2009. Prieiga internete: https://www.hsdl.org/?view&did=30477

78. HONG, I., YU, H., LEE, S., & K. LEE. A new triage model conforming to the needs of selective search and seizure of electronic evidence. *Digital Investigation*. 2013, 10(2), 175–192.

79. HORSMAN, G., LAING, C., & P. VICKERS. A case-based reasoning method for locating evidence during digital forensic device triage. *Decision Support Systems*. 2014, 61, 69–78.

80. HUI, Y. What is a Digital Object?: What is a Digital Object? *Metaphilosophy*. 2012, 43(4), 380–395.

81. HUTCHINS, E. M., CLOPPERT, M. J., & Amin, R. M. *Intelligence-Driven*

Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, 2014, 14.

82. YAQOOB, I., HASHEM, I. A. T., AHMED, A., KAZMI, S. M. A., & C. S. HONGInternet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generation Computer Systems*. 2019, 92, 265–275.

83. IEONG, R. S. C. FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*. 2006, 3, 29–36.

84. III, G. A. F., & K. CLINTON. Computer forensics laboratory and tools. *Journal of Computing Sciences in Colleges*, 2005, vol. 20 Issue 6, June 2005, 143–150.

85. INGRAM, S. If the *Profile Fits: Admitting Criminal Psychological Profiles into Evidence in Criminal Trials*, 1998, 54, 29.

86. Internet of Things Architecture. *IoT-A Internet of Things – Architecture.* 2013, rugsėjis. Prieiga internete: https://web.archive.org/web/20130918185701/http://www.iot-a.eu/public/terminology.

87. IRONS, A., & H. LALLIE. Digital Forensics to Intelligent Forensics. *Future Internet*. 2014, 6(3), 584–596.

88. YUNIANTO, E., PRAYUDI, Y., & B. SUGIANTORO. B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management. *International Journal of Computer Applications*. 2019, 181(45), 22–29.

89. YUSOFF, Y., ISMAIL, R., & Z. HASSAN. Common Phases of Computer Forensics Investigation Models. *International Journal of Computer Science and Information Technology*. 2011, 3(3), 17–31.

90. JAHANKHANI, H., WATSON, D. L., ME, G., & LEONHARDT, F. Handbook of Electronic Security and Digital Forensics. *WORLD SCIENTIFIC*, 2010 [žiūrėta 2020-03-27]. Prieiga internete: http://www.worldscientific.com/worldscibooks/10.1142/7110

91. JANSEN, A. Object-oriented diplomatics: Using archival diplomatics in software application development to support authenticity of digital records. (D. Luciana Duranti, Sud.) *Records Management Journal*. 2015, 25(1), 45–55.

92. JUSAS, V., BIRVINSKAS, D., & E. GAHRAMANOV. Methods and Tools of Digital Triage in Forensic Context: Survey and Future Directions. *Symmetry*. 2017, 9(4), 49.

93. JUSTICKIS, V. (). Criminal Data Mining. *WORLD SCIENTIFIC*, 2010. [žiūrėta kovo 29, 2020-03-20]. Prieiga internete: http://www.worldscientific.com/worldscibooks/10.1142/7110

94. KARABIYIK, U., & AKKAYA, K. *Digital Forensics for IoT and WSNs. H.*

M. Ammari (Sud.), Mission-Oriented Sensor Networks and Systems: Art and Science (T. 164, p. 171–207). Cham: Springer International Publishing, 2019. [žiūrėta 2019-10-02]. Prieiga internete: http://link.springer.com/10.1007/978-3-319-92384-0_6

95. KÄVRESTAD, J. *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications*. Cham: Springer International Publishing, 2018. [žiūrėta 2019-08-22]. Prieiga internete: http://link.springer.com/10.1007/978-3-319-96319-8

96. KOHN, M. D., ELOFF, M. M., & ELOFF, J. H. P. (). Integrated digital forensic process model. *Computers & Security*. 2013, 38, 103–115.

97. KOOPMANS, M. B., & J. I. JAMES. Automated network triage. *Digital Investigation*. 2013, 10(2), 129–137.

98. KURT, M. N., YILMAZ, Y., & X. WANG. Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid. *IEEE Transactions on Information Forensics and Security*. 2019, 14(2), 498–513.

99. LASSILA, O., & MCGUINNESS, D. *The Role of Frame-Based Representation on the Semantic Web,* 11, 2014.

100. LYLE, J. R. If error rate is such a simple concept, why don't I have one for my forensic tool yet? *Digital Investigation*. 2010, 7, S135–S139.

101. LIM, K.-S., & C. LEE. A framework for unified digital evidence management in security convergence. *Electronic Commerce Research*, 2013, 13(3), 379–398.

102. LIM, K.-S., & LEE, S*A Methodology for Forensic Analysis of Embedded Systems*. 2008 Second International Conference on Future Generation Communication and Networking (2008, p. 283–286). Pristatytas *2008 Second International Conference on Future Generation Communication and Networking* (FGCN), Hainan, China: IEEE. [žiūrėta 2019-10-01]. Prieiga internete: http://ieeexplore.ieee.org/document/4734223/

103. Linuxlinks. *Automated Image and Restore*, 2019. Prieiga internete: http://www.linuxlinks.com/AutomatedImageandRestore/

104. LOHIYA, R., & SHAH, P. *Video Based Face Detection and Tracking for Forensic Applications*, 2015, 7(1), 9.

105. LTEC. *Ekspertinių tyrimų eilės Lietuvos policijos kriminalistinių tyrimų centre (LPKTC) ir Lietuvos teismo ekspertizės centre*, 2016, birželio 29. Prieiga internete: http://www.ltec.lt/index.php?id=883

106. LUTHFi, A. *The Use Of Ontology Framework For Automation Digital Forensics Investigation*, 2014. [žiūrėta 2019-08-22]. Prieiga internete: https://zenodo.org/record/1091430

107. MAGALINGAM, P., MANAF, A., AHMAD, R., & Z. YAHYA.A New Digital Evidence Retrieval Model for Gambling Machine Forensic Investigation.

The International Journal of Forensic Computer Science. 2009, 49–56.

108. Magnet Forensics. *Magnet Forensics. Internet evidence finder* (IEF), 2019. Prieiga internete: http://www.magnetforensics.com

109. MARTINEZ-ROMO, J., & ARAUJO, L. Analyzing Information Retrieval Methods to Recover Broken Web Links. C. Gurrin, Y. He, G. Kazai, U. Kruschwitz, S. Little, T. Roelleke, S. Rüger, ir kt. (Sud.), *Advances in Information Retrieval* (T. 5993, p. 26–37). Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. [žiūrėta rugpjūčio 22, 2019-08-22]. Prieiga internete: http://link.springer.com/10.1007/978-3-642-12275-0_6

110. MARTURANA, F., ME, G., BERTE, R., & TACCONI, S. *A Quantitative Approach to Triaging in Mobile Forensics. 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications* (2011, p. 582–588). Pristatytas 2011 *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communication*s (TrustCom), Changsha, China: IEEE. [žiūrėta 2019-10-01]. Prieiga internete: http://ieeexplore.ieee.org/document/6120868/

111. MARTURANA, F., & S. TACCONI. A Machine Learning-based Triage methodology for automated categorization of digital media. *Digital Investigation.* 2013, 10(2), 193–204.

112. MARTURANA, F., TACCONI, S., BERTE, R., & ME, G. (). *Triage-based automated analysis of evidence in court cases of copyright infringement*,2012. 2012 IEEE International Conference on Communications (ICC) (p. 6668–6672). Pristatytas ICC 2012 – *2012 IEEE International Conference on Communications, Ottawa*, ON, Canada: IEEE. [žiūrėta spalio 1, 2019-10-01]. Prieiga internete: http://ieeexplore.ieee.org/document/6364819/

113. MICHAEL B., M., JEFFREY L, S., & DAVID W, H. (s.a.). *Crime Scene Investigation. Electronic Crime Scene Investigation: A Guide for First Responders*, Second Edition. Prieiga internetu: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

114. Microsoft. *Web.config Transformation Syntax for Web Project Deployment Using Visual Studio*, 2019. Prieiga internete: https://docs.microsoft.com/en-us/aspnet/web-forms/overview/deployment/visual-studio-web-deployment/web-config-transformations

115. MIRANDA LOPEZ, E., MOON, S., & PARK, J. Scenario-Based Digital Forensics Challenges in Cloud Computing. *Symmetry*. 2016, 8(10), 107.

116. MITRE. *Cyber Observable eXpression* (CybOXTM), 2019. Prieiga internete: http://cyboxproject.github.io/about/

117. MONGAY BATALLA, J., & P. KRAWIEC. Conception of ID layer performance at the network level for Internet of Things. *Personal and Ubiquitous Computing*. 2014, 18(2), 465–480.

118. MONTASARI, R. *A Formal Two Stage Triage Process Model (FTSTPM) for Digital Forensic Practice*, 2016, 19.

119. MONTASARI, R., CARPENTER, V., & R. HILL. A road map for digital forensics research: A novel approach for establishing the design science research process in digital forensics. *International Journal of Electronic Security and Digital Forensics*. 2019, 11(2), 194.

120. MSAB. *XRY*, 2019. Prieiga internete: https://www.msab.com/xry/what-is-xry

121. MUKASEY, M. B., SEDGWICK, J. L., HAGY D. W. (s.a.). *Crime Scene Investigation. Electronic Crime Scene Investigation: A Guide for First Responders*, Second Edition. Prieiga internete: https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

122. MUNISWAMY-REDDY, K.-K., HOLLAND, D. A., BRAUN, U., & SELTZER, M. I. *Provenance-Aware Storage Systems*. USENIX Annual Technical Conference, General Track, 2006, 43–56.

123. NAGAR, U., NANDA, P., HE, X., & TAN, Z. *A framework for data security in cloud using collaborative intrusion detection scheme.* Proceedings of the 10th International Conference on Security of Information and Networks—SIN '17 (2017, p. 188–193). Pristatytas *the 10th International Conference, Jaipur*, India: ACM Press. [žiūrėta 2019-08-22]. Prieiga internete: http://dl.acm.org/citation.cfm?doid=3136825.3136905

124. NANCE, K., & RYAN, D. J. *Legal Aspects of Digital Forensics: A Research Agenda*, 2011. 2011 44th Hawaii International Conference on System Sciences (p. 1–6). Pristatytas *2011 44th Hawaii International Conference on System Sciences* (HICSS 2011), Kauai, HI: IEEE. [žiūrėta 2019-08-22]. Prieiga internete: http://ieeexplore.ieee.org/document/5719007/

125. NEWSHAM, T., PALMER, C., STAMOS, A., & BURNS, J. (s.a.). *Breaking Forensics Software: Weaknesses in Critical Evidence Collection*, 30.

126. NYKODYM, N., TAYLOR, R., & J. VILELA.Criminal profiling and insider cyber crime. *Computer Law & Security Review*. 2005, 21(5), 408–414.

127. NIST. *Computer Forensics Tool Catalog. Forensic Tool Taxonomy*, 2019. Prieiga internete: http://toolcatalog.nist.gov/taxonomy/index.php?ff_id=5

128. NOY, N. F., & MCGUINNESS, D. L. *Ontology Development 101: A Guide to Creating Your First Ontology*, 2001, 25.

129. OASIS. *MQTT and the NIST Cybersecurity Framework Version 1.0,* 2014. [žiūrėta Prieiga internete: http://docs.oasis-open.org/mqtt/mqtt-nist-cybersecurity/v1.0/mqtt-nist-cybersecurity-v1.0.html

130. OASIS. *Open Source Digital Forensic*, 2019. Prieiga internete: https://web.archive.org/web/20150228083211/http://www2.opensourceforensics.

org/tools

131. ODUSAMI, M., ABAYOMI-ALLI, O., MISRA, S., SHOBAYO, O., DAMASEVICIUS, R., & MASKELIUNAS, R. Android Malware Detection: A Survey. H. Florez, C. Diaz, & J. Chavarriaga (Sud.), *Applied Informatics* (T. 942, p. 255–266). Cham: Springer International Publishing, 2018. [žiūrėta rugpjūčio 22, 2019-08-22]. Prieiga internete: http://link.springer.com/10.1007/978-3-030-01535-0_19

132. OLIVIER, M. On a Scientific Theory of Digital Forensics. G. Peterson & S. Shenoi (Sud.), *Advances in Digital Forensics XII* (T. 484, p. 3–24). Cham: Springer International Publishing, 2016. [žiūrėta 2019-08-22]. Prieiga internete: http://link.springer.com/10.1007/978-3-319-46279-0_1

133. OpenText Corp. *EnCase*, 2019 . Prieiga internete: https://www.guidancesoftware.com/encase-forensic

134. Oracle. *VirtualBox,* 2019. Prieiga internete: https://www.virtualbox.org/

135. ORIWOH, E., JAZANI, D., EPIPHANIOU, G., & SANT, P. *Internet of Things Forensics: Challenges and Approaches.* Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing. Pristatytas *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, Austin, United States: ICST, 2013. [žiūrėta kovo 28, 2020-03-28]. Prieiga internete: http://eudl.eu/doi/10.4108/icst.collaboratecom.2013.254159

136. OVERILL, R. E., SILOMON, J. A. M., & K. A. ROSCOETriage template pipelines in digital forensic investigations. *Digital Investigation*. 2013, 10(2), 168–174.

137. OVERILL, R., KWAN, M., CHOW, K.-P., LAI, P., & LAW, F. A Cost-Effective Model for Digital Forensic Investigations. G. Peterson & S. Shenoi (Sud.), *Advances in Digital Forensics V* (T. 306, p. 231–240). Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. [žiūrėta spalio 1, 2019-10-01]., Prieiga internete: http://link.springer.com/10.1007/978-3-642-04155-6_17

138. PALMER, G. *A Road Map for Digital Forensic Research. Report From the First Digital Forensic Research Workshop* (DFRWS), 2001, november 6.

139. PAN, L., & L. M. BATTEN. Robust performance testing for digital forensic tools. *Digital Investigation*. 2009, 6(1–2), 71–81.

140. PassMarkTM Software. *OSForensics*, 2019. Prieiga internete: http://www.osforensics.com/

141. PATEL, C. P., & B. K. SHARMA. (). IJSRD - *International Journal for Scientific Research & Development,*| 2015, vol. 2, Issue 04, 2014 | ISSN (online): 2321-0613, 3(08), 3.

142. PATIL, S., DHARASKAR, R., & THAKARE, V. *Cloud Forensics: A*

Framework for Digital Forensic in Cloud Based Environment by Identifying SLA Breaches by Cloud Actors, 6, 2017.

143. PEERSMAN, C., SCHULZE, C., RASHID, A., BRENNAN, M., & C. FISCHER, iCOP: Live forensics to reveal previously unknown criminal media on P2P networks. *Digital Investigation*. 201618, 50–64.

144. PERON, C. S. J., LEGARY, M., & LABS, S. (s.a.). *Digital Anti-Forensics: Emerging trends in data transformation techniques*, 11.

145. PETHERICK, W. *The science of criminal profiling: All killers have their own modus operandi.* New York, NY: Barnes & Noble Books, 2005.

146. PLADNA B. *Computer Forensics Procedures, Tools, and Digital Evidence Bags: What They Are and Who Should Use Them*. 2008. Prieiga internete: http://www.infosecwriters.com/Papers/BPladna_Computer_Forensic_Procedures.pdf

147. POLLITT, M. A History of Digital Forensics. K.-P. Chow & S. Shenoi (Sud.), *Advances in Digital Forensics VI* (T. 337, p. 3–15). Berlin, Heidelberg: Springer Berlin Heidelberg, 2010. [žiūrėta 2019-10-01]. Prieiga internete: http://link.springer.com/10.1007/978-3-642-15506-2_1

148. PORTNOFF, R. S., AFROZ, S., DURRETT, G., KUMMERFELD, J. K., BERG-KIRKPATRICK, T., MCCOY, D., LEVCHENKO, K., et al. (). *Tools for Automated Analysis of Cybercriminal Markets*. Proceedings of the 26th International Conference on World Wide Web—WWW '17 (p. 657–666). Pristatytas the *26th International Conference*, Perth, Australia: ACM Press, 2017. [žiūrėta 2019-08-22]. Prieiga internete: http://dl.acm.org/citation.cfm?doid=3038912.3052600

149. PRAYUDI, Y., ASHARI, A., K PRIYAMBODO, T., & T. K PRIYAMBODO. A Proposed Digital Forensics Business Model to Support Cybercrime Investigation in Indonesia. *International Journal of Computer Network and Information Security*. 2015, 7(11), 1–8.

150. QUICK, D., & K.-K. R. CHOO. Big forensic data reduction: Digital forensic images and electronic evidence. *Cluster Computing*. 2016, 19(2), 723–740.

151. QUICK, D., & CHOO, K.-K. R. *Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT + OSINT): A timely and cohesive mix. Future Generation Computer Systems*, 2018, 78, 558–567.

152. QUICK, D., & CHOO, K.-K. R. (s.a.). *Data reduction and data mining framework for digital forensic evidence: Storage, intelligence, review and archive*, 11.

153. RAJABOINA, R., REDDY, P. C., & KUMAR, R. A. *Performance comparison of TCP, UDP and TFRC in static wireless environment*. 2015 2nd International Conference on Electronics and Communication Systems (ICECS) (p. 206–212). Pristatytas *2015 2nd International Conference on Electronics and*

Communication Systems (ICECS), Coimbatore, India: IEEE, 2015. [žiūrėta 2019-10-01]. Prieiga internete: http://ieeexplore.ieee.org/document/7124893/

154. RAZZAQ, A., ANWAR, Z., AHMAD, H. F., LATIF, K., & MUNIR. Ontology for attack detection: An intelligent approach to web application security. *Computers & Security*. 2014, 45, 124–146.

155. REITH, M., CARR, C., & G. GUNSCH. () The digital age can be characterized as the application of computer technology as a tool that enhances traditional methodologi. *International Journal of Digital Evidence*. 2002, 1(3), 12.

156. REKHIS, S., & BOUDRIGA, N. *A Formal Rule-Based Scheme for Digital Investigation in Wireless Ad-hoc Networks*. 2009 Fourth International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering (p. 62–72). Pristatytas *2009 Fourth International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering* (SADFE), Berkeley, California, USA: IEEE, 2009. [žiūrėta 2019-10-02]. Prieiga internete: http://ieeexplore.ieee.org/document/5341557/

157. RIADI, I., ISTIYANTO, J. E., & ASHARI, A. *Log Analysis Techniques using Clustering in Network Forensics*, 2012, 10, 9.

158. RYAN, J. D., & SHPANTZER, G. *Legal Aspects of Digital Forensics*, 2002. Prieiga internete: http://euro.ecom.cmu.edu/program/law/08-732/Evidence/RyanShpantzer.pdf

159. ROGERS, M. D. (1999). *Psychology of hackers: Steps toward a new taxonomy*. Prieiga internete: http://www.dvara.net/HK/hacker_doc.pdf

160. ROGERS, M. (). The role of criminal profiling in the computer forensics process. *Computers & Security*. 2003, 22(4), 292–298.

161. ROGERS, M., GOLDMAN, J., MISLAN, R., WEDGE, T., & S. DEBROTA. Computer Forensics Field Triage Process Model. The *Journal of Digital Forensics, Security and Law*, 2006, 27–40.

162. ROY, A., DIXIT, R., NASKAR, R., & CHAKRABORTY, R. S. *Digital Image Forensics: Theory and Implementation*. *Studies in Computational Intelligence* (T. 755). Singapore: Springer Singapore, 2020. [žiūrėta 2020-03-29]. Prieiga internete: http://link.springer.com/10.1007/978-981-10-7644-2

163. ROMAN, R., LOPEZ, J., & M. MAMBO. Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*. 2018, 78, 680–698.

164. ROUSSEV, V., & C. QUATES. (Content triage with similarity digests: The M57 case study. *Digital Investigation*. 2012, 9, S60–S68.

165. ROUSSEV, V., QUATES, C., & R. MARTELL. (Real-time digital forensics and triage. *Digital Investigation*. 2013, 10(2), 158–167.

166. ROWLINGSON, R. *A Ten Step Process for Forensic Readiness*, 2004, 2(3),

28.

167. SALAHDINE, F., & N. KAABOUCH. . Social Engineering Attacks: A Survey. *Future Internet*. 2019, 11(4), 89.

168. SALEEM, S., POPOV, O., & I. BAGILLI. (Extended Abstract Digital Forensics Model with Preservation and Protection as Umbrella Principles. *Procedia Computer Science*. 2014, 35, 812–821.

169. SARC. (). *Steganography Analysis and Research Center* (SARC), 2019. Prieiga internete: http://sarc-wv.blogspot.com/

170. SCG Canada Inc. *Covert Forensic Imaging Device* (CFID), 2019. Prieiga internete: http://www.scgcanada.com/

171. SCHOBBENS, P.-Y., HEYMANS, P., & TRIGAUX, J.-C. *Feature Diagrams: A Survey and a Formal Semantics*. 14th IEEE International Requirements Engineering Conference (RE'06) (p. 139–148). Pristatytas *14th IEEE International Requirements Engineering Conference*, Minneapolis/St. Paul, MN: IEEE, 2006. [žiūrėta 2019-10-01]. Prieiga internete: http://ieeexplore.ieee.org/document/1704057/

172. SCHULTZ, E. E., & SHUMWAY, R. *Incident response: A strategic guide to handling system and network security breaches* (1st ed.). Indianapolis, Ind: New Riders Pub., 2002.

173. Scripting News. *Outline Processor Markup Language*, 2019. [žiūrėta Prieiga internete: http://dev.opml.org

174. Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan, Rahman, S., & N. A. M. Khan. Digital Forensics through Application Behavior Analysis. *International Journal of Modern Education and Computer Science*. 2016, 8(6), 50–56.

175. SHARMA, H., KANWAL, N., & BATTH, R. S. *An Ontology of Digital Video Forensics: Classification, Research Gaps & Datasets*. 2019 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE) (p. 485–491). Pristatytas *2019 International Conference on Computational Intelligence and Knowledge Economy* (ICCIKE), Dubai, United Arab Emirates: IEEE, 2019. [žiūrėta 2020-05-17]. Prieiga internete: https://ieeexplore.ieee.org/document/9004331/

176.
SHARMA, T. N. *Analysis_of_Software_Cost_Estimation_using_COCOMO_II*, 2011, 2(6), 5.

177. SIAHAAN, A. P. U., & RAHIM, R. *Post-Genesis Digital Forensics Investigation* (preprint). INA-Rxiv, 2017. [žiūrėta spalio 2, 2019-10-02]. Prieiga internete: https://osf.io/h5bds

178. SINGER, D. A., & R. KOUDA. (A Comparison of the Weights-of-Evidence

Method and Probabilistic Neural Networks. *Natural Resources Research*. 1999, 8(4), 287–298.

179. SOMMER, F., DÜRRWANG, J., & KRIESTEN, R. *Survey and Classification of Automotive Security Attacks. Information*, 2019, 10(4), 148.

180. SONI, M., & M. K. BHARTI, (FraaS: A Framework for Digital Forensic Services in a Cloud-based Environment. *The International Journal of Forensic Computer Science*. 2015, 10(1), 15–22.

181. SREMACK, J. C. *The Gap between Theory and Practice in Digital Forensics*, 2007, 85.

182. STAMM, M. C., LIN, W. S., & LIU, K. J. R. *Temporal Forensics and Anti-Forensics for Motion Compensated Video. IEEE Transactions on Information Forensics and Security*, 2012, 7(4), 1315–1329.

183. STEEL, C. Idiographic Digital Profiling: Behavioral Analysis Based On Digital Forensics. *Journal of Digital Forensics, Security and Law*. 2014. [žiūrėta 2019-10-01]. Prieiga internete: http://commons.erau.edu/jdfsl/vol9/iss1/1/

184. SUÁREZ-ALBELA, M., FERNÁNDEZ-CARAMÉS, T., FRAGA-LAMAS, P., and L. CASTEDO. A Practical Evaluation of a High-Security Energy-Efficient Gateway for IoT Fog Computing Applications. *Sensors*. 2017, 17(9), 1978.

185. ŠTUIKYS, V., BURBAITĖ, R., & BESPALOVA, K. The LO Sequencing Problem and Its Solution Using Meta-Programming-Based Approach. G. Dregvaite & R. Damasevicius (Sud.), *Information and Software Technologies* (T. 538, p. 151–164). Cham: Springer International Publishing, 2015. [žiūrėta 2019-10-02]. Prieiga internete: http://link.springer.com/10.1007/978-3-319-24770-0_14

186. ŠTUIKYS, V., & DAMAŠEVIČIUS, R. *Meta-Programming and Model-Driven Meta-Program Development. Advanced Information and Knowledge Processing* (T. 5). London: Springer London, 2013. [žiūrėta spalio 2, 2019-10-02]. Prieiga internete: http://link.springer.com/10.1007/978-1-4471-4126-6

187. TAKWA, O., BELGACEM, C. R., & ADEL, D. *A New Digital Investigation Frameworks Comparison Method*, 2016, 3(4), 5.

188. Technical Analysis Group. (). ISTS. *Law enforcement tools and technologies for investigating cyber attacks: A national re-search and development agenda* (p. 35). Institute for security technology studines, 2004. Prieiga internete: http://index-of.es/Misc/pdf/ISTSLawEnforcementResearchandDevelopmentAgendaJune2004.pdf

189. THARWAT, A. Classification assessment methods. *Applied Computing and Informatics*, S2210832718301546, 2018.

190. TRIFONOV, R., MANOLOV, S., YOSHINOV, R., TSOCHEV, G., &

PAVLOVA, G. *Artificial Intelligence Methods for Cyber Threats Intelligence*, 2017, 2, 7.

191. TULOWIECKI, S. J. Information retrieval in physical geography: A method to recover geographical information from digitized historical documents. *Progress in Physical Geography: Earth and Environment*. 2018, 42(3), 369–390.

185. TURNBULL, B., & S. RANDHAWA. (Automated event and social network extraction from digital evidence sources with ontological mapping. *Digital Investigation*. 2015, 13, 94–106.

192. TURNER, P. Digital provenance – interpretation, verification and corroboration. *Digital Investigation*. 2005a, 2(1), 45–49.

193. TURNER, P.Unification of digital evidence from disparate sources (Digital Evidence Bags*). Digital Investigation. 2005b, 2 (3), 223–228.*

184. TURVEY, B. E. Criminal profiling: An introduction to behavioral evidence analysis. Oxford; Burlington, MA: Academic Press, 2012. [žiūrėta 2019-09-30]. Prieiga internete: http://site.ebrary.com/id/10480741

195. UMAIR, A., NANDA, P., & HE, X. (). *Online Social Network Information Forensics: A Survey on Use of Various Tools and Determining How Cautious Facebook Users are?* 2017 IEEE Trustcom/BigDataSE/ICESS (p. 1139–1144). Pristatytas *2017 IEEE Trustcom/BigDataSE/ICESS*, Sydney, Australia: IEEE. 2017. [žiūrėta2019-08-22]. Prieiga internete: http://ieeexplore.ieee.org/document/8029567/

196. VAN BUSKIRK, E., & V. T. LIU. Digital Evidence: Challenging the Presumption of Reliability. *Journal of Digital Forensic Practice*. 2006, 1(1), 19–26.

197. VENČKAUSKAS, A., JUSAS, V., PAULIKAS, K., & J. TOLDINAS. A Methodology and Tool for Investigation of Artifacts Left by the BitTorrent Client. *Symmetry*. 2016, 8(6), 40.

198. VENČKAUSKAS, A., MORKEVICIUS, N., BAGDONAS, K., DAMAŠEVIČIUS, R., & R. Maskeliūnas. A Lightweight Protocol for Secure Video Streaming. *Sensors*. 2018, 18(5), 1554.

199. VENČKAUSKAS, A., MORKEVICIUS, N., JUKAVIČIUS, V., DAMAŠEVIČIUS, R., TOLDINAS, J., & Š. GRIGALIŪNAS. An Edge-Fog Secure Self-Authenticable Data Transfer Protocol. *Sensors*. 2019, 19(16), 3612.

200. VENČKAUSKAS, A., TOLDINAS, J., GRIGALIŪNAS, Š., DAMAŠEVIČIUS, R., & JUSAS, V. *Suitability of the digital forensic tools for investigation of cyber crime in the Internet of Things and Services* (p. 86–97). Pristatytas *The 3rd International Virtual Research Conference In Technical Disciplines.* 2015. [žiūrėta 2019-10-01]. Prieiga internete: https://www.rcitd.com/archive/?vid=1&aid=2&kid=140301-67

201. VUKAŠINOVIĆ, M. *A Software System for automatic reaction to network anomalies and in Real Time Data Capturing necessary for investigation of digital Forensics*, 2017, 11, 8.

202. W3C. *Web Ontology Language*. 2019. Prieiga internete: http://www.w3.org/TR/2012/REC-owl2-overview-20121211/

203. WAHYUDI, E., RIADI, I., & PRAYUDI, Y. (). *Virtual Machine Forensic Analysis And Recovery Method For Recovery And Analysis Digital Evidence*, 2018, 16(2), 8.

204. WANG, N. A Knowledge Model of Digital Evidence Review Elements Based on Ontology. *International Journal of Digital Crime and Forensics*. 2017, 9(3), 49–57.

205. WEI, W., & WO, M. (s.a.). *Algorithm Research of Known-plaintext Attack on Double Random Phase Mask Based on WSNs,* 10.

206. WILSDON, T., & SLAY, J. *Validation of Forensic Computing Software Utilizing Black Box Testing Techniques*, 2006, 10.

207. WOOD, W., & RÜNGER, D. Psychology of Habit. *Annual Review of Psychology*. 2016, 67(1), 289–314.

208. ZAWOAD, S., & HASAN, R. (2015). *FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things*. 2015 IEEE International Conference on Services Computing (p. 279–284). Pristatytas *2015 IEEE International Conference on Services Computing (SCC),* New York City, NY, USA: IEEE. [žiūrėta 2019-10-02]. Prieiga internete: http://ieeexplore.ieee.org/document/7207364/

8. PUBLIKACIJŲ SĄRAŠAS

STRAIPSNIAI RECENZUOJAMUOSE MOKSLO LEIDINIUOSE

Grigaliūnas, Šarūnas; Toldinas, Jevgenijus; Venčkauskas, Algimantas. An ontology-based transformation model for the digital forensics domain // Elektronika ir elektrotechnika. Kaunas : KTU. ISSN 1392-1215. eISSN 2029-5731. 2017, vol. 23, iss. 3, p. 78-82. DOI: 10.5755/j01.eie.23.3.18337. [Science Citation Index Expanded (Web of Science); Scopus; Computers & Applied Sciences Complete] [IF: 1,088; AIF: 2,723; IF/AIF: 0,399; Q3 (2017, InCites JCR SCIE)] [CiteScore: 1,03; SNIP: 0,624; SJR: 0,258; Q3 (2017, Scopus Sources).

Šarūnas Grigaliūnas, Jevgenijus Toldinas. „Habits Attribution and Digital Evidence Object Models Based Tool for Cybercrime Investigation“. Baltic J. Modern Computing, Vol. 8 (2020), No. 2, 275-292. DOI: 10.22364/bjmc.2020.8.2.05.

Konferencijų pranešimų medžiagoje

Damaševičius, Robertas; Toldinas, Jevgenijus; Venčkauskas, Algimantas; Grigaliūnas, Šarūnas; Morkevičius, Nerijus; Jukavičius, Vaidas. Visual analytics for cyber security domain: state-of-the-art and challenges // Information and software technologies: 25th international conference, ICIST 2019, Vilnius, Lithuania, October 10–12, 2019: proceedings / Robertas Damaševičius, Giedrė Vasiljevienė (Eds.). Cham :Springer, 2019. ISBN 9783030302740. eISBN 9783030302757. p. 256-270. (Communications in computer and information science, ISSN 1865-0929, eISSN 1865-0937 ; vol. 1078). DOI: 10.1007/978-3-030-30275-7_20. [Scopus] [M.kr.: T 007] [Indėlis: 0,166]

Grigaliūnas, Šarūnas; Toldinas, Jevgenijus. Digital evidence investigation using habits attribution // RCITD - Proceedings in research conference in technical disciplines. Zilina : EDIS - Publishing Institution of the University of Zilina. ISSN 2453-6571. 2016, vol. 4, iss. 1, p. 30-35. DOI: 10.18638/rcitd.2016.4.1.86. [M.kr.: T 007] [Indėlis: 0,500]

Toldinas, Jevgenijus; Venčkauskas, Algimantas; Grigaliūnas, Šarūnas; Damaševičius, Robertas; Jusas, Vacius. Suitability of the digital forensic tools for investigation of cyber crime in the internet of things and services // RCITD 2015 [elektroninis išteklius] : 3rd international virtual

research conference in technical disciplines, October, 19-23, 2015. Zilina : EDIS - Publishing Institution of the University of Zilina, 2015. ISBN 9788055411255. ISSN 2453-6571. eISSN 1339-5076. 2015, vol. 3, iss. 1, p. 86-97. DOI: 10.18638/rcitd.2015.3.1. [M.kr.: T 007] [Indėlis: 0,200]

MOKSLINIŲ TYRIMŲ REZULTATŲ SKELBIMAS KONFERENCIJOSE

Grigaliūnas, Šarūnas; Toldinas, Jevgenijus; Lozinskis, Borisas. Habits attribution and digital evidence object tool with fuzzy logic for cybercrime investigation // 11th international workshop on data analysis methods for software systems, Druskininkai, Lithuania, November 28-30, 2019 / Lithuanian Computer Society, Vilnius University Institute of Data Science and Digital Technologies, Lithuanian Academy of Sciences. Vilnius : Vilnius University, 2019. ISBN 9786090703243. eISBN 9786090703250. p. 29. [M.kr.: T 007]

Grigaliūnas, Šarūnas; Toldinas, Jevgenijus. Digital evidence object model for cybercrime investigation // 9th International workshop on data analysis methods for software systems, DAMSS : Druskininkai, Lithuania, November 30 - December 2, 2017 / Lithuanian Computer Society, Vilnius University, Institute of Data Science and Digital Technologies, Lithuanian Academy of Sciences. Vilnius : Vilnius University, 2017. ISBN 9789986680642. p. 18-19. DOI: 10.15388/DAMSS.2017. [M.kr.: T 007]

Trumpos žinios apie autorių

Šarūnas Grigaliūnas gimė 1977 m. Yra įgyjąs elektronikos inžinerijos studijų krypties bakalauro laipsnį ir informatikos inžinerijos studijų krypties magistro laipsnį. 2015 m. pradėjo informatikos inžinerijos doktorantūros studijas Kauno technologijos universitete, tyrimų sritis – nusikaltimų elektroninėje erdvėje skaitmeninių įkalčių paieška. Vydydamas akademines veiklas, be tiriamosios veiklos, Š. Grigaliūnas dar vedė paskaitas, laboratorinius užsiėmimus nusikaltimų elektroninėje erdvėje ir jų tyrimų metodikos, saugumo patikros ir etiško įsilaužimo metodų, virtualios infrastruktūros saugos, temomis. Už akademinės veiklos ribų daugiau nei 5 metus Š. Grigaliūnas Prisidėjo prie LITNET CERT reagavimo į kibernetinės saugos incidentus komandos formavimo. Užimdamas IT saugumo skyriaus vadovo poziciją tapo atsakingas už IT valdymą, IT auditus, IT konsultacijas ir saugos transformacijų projektus. Projektuojant vienas didžiausių kibernetinių pratybų „Kibernetinis skydas“ atakas ir jų tyrimus, prisidėjo prie Lietuvos kritinių kontrolės priemonių efektyviai kibernetinei gynybai ir elektroninių įkalčių aptykimo.

Atstovavimas universitetui mokslo ir inovacijų politiką kuriančiose bei įgyvendinančiose tarptautinėse ir šalies institucijose: Š. Grigaliūnas - Lietuvos standartizacijos departamentas, techninis komitetas 79 (Informacijos saugumas); GEANT SIG – Informacijos saugumo valdymas (Information Security Management); ES MSP/DEI darbo grupė "Standardisation in support of digitising European industry"; Europos standartizacijos CEN/CLC/JTC 13 – “Cybersecurity and Data Protection” darbo grupė.

DEVELOPMENT OF CYBERCRIME FORENSIC INVESTIGATION METHOD

Resume

Computer crime is carried out with the help of computers, computer networks, and modern information technologies. Searching for digital evidence of these crimes requires specific expert knowledge and technical means, as the tool or computer technology for gathering information, planning and executing criminal activity, and illicit data exchange becomes a tool of illegal activity. The amount of data stored on computers has been growing rapidly every year, which makes investigation of digital evidence in cybercrime both time-consuming and difficult because of the need to investigate a large amount of data and provide well-grounded detailed proof.

This dissertation examines the problem of the emergence of a specialized, appropriate method and tool that helps an expert reduce the sample of the investigated data and deliver digital crime investigation choices. So far, specialized tools and techniques to automate expert research are insufficient.

This dissertation consists of an introduction, five main sections, and general conclusions.

The first section reviews the problem of searching for digital evidence of crime, and looks at the already existing search tools, models, and methods.

The second section proposes a multilayered ontology-based system for selecting the right tool for searching digital evidence. A wireframe, a taxonomy of digital evidence, is proposed to allow the categorization of evidence and the selection of the right tool for digital forensic.

The third section proposes a model to reduce the sampling of the digital evidence found by applying user digital profiling to their digital ‘habits’.

The fourth chapter proposes the Digital Evidence Object model, a method of expert investigation of cybercrime aimed to search for digital evidence of these crimes.

The fifth section describes the proposed DEO model application experiment which compares the results with similar tools available on the market. There was a positive evaluation of the numerical error finding obtained; the developed model was compared to the COCOMO II model,

which allows determining the applicability of the model.

The work is summarized by general conclusions confirming the need for the newly proposed object model of digital evidence and its suitability for use in experimental investigation of the digital evidence of cybercrime.

Problem formulation

The Term Bank of the Republic of Lithuania provides an approved definition of the term 'Forensic investigation': "In accordance with the procedure established by the laws of the Republic of Lithuania, an investigation by a forensic expert or a professional requiring special knowledge (forensics, object investigation and legal advice)." The Forensic Law of the Republic of Lithuania No. IX-1161 determines 'expert expertise' as "the detailed knowledge necessary to conduct an expertise, acquired in education, special training or professional activity in the field of science, technology, art or any other human activity." Computer crime is carried out by using computers, computer networks, and modern information technologies. Search for digital evidence of these crimes requires specific expert knowledge and technical measures, as the computer (with the data contained therein) becomes the tool of illegal activity, or computer technology is used for gathering information, planning and executing criminal activity and illicit data exchange.

The amount of data stored on computers has been growing rapidly every year, which makes the investigation of digital evidence in cybercrime time-consuming because of the need to investigate a large amount of data and to extract criminal evidence from it. Expert investigation begins with the collection, copying and authentication of each content on the digital medium. The following steps deal with the findings and extract evidence of crime by using a variety of methods and tools. The research deals with the frameworks, methods and models of the search for digital evidence of cybercrime. However, there is as of yet no specialized method and no tool available to assist an expert in reducing the size of the investigated data and to solve the problem of searching for and identifying digital evidence of cybercrime due to the lack of specialized tools and techniques to automate expert investigation. General conclusions:

1. There is a huge number of available computer forensic tools from standalone packages to complex integrated tools developed for a wide range crime investigations. The analysis of methods, models

and frameworks for cybercrime forensic investigation proved that there is no single superior method, model or framework, which would be able to cover the exponential growth of the amount of digital information with the main cybercrime forensics related areas. Therefore, a new, more holistic cybercrime forensic investigation method is needed to concentrate on reducing the expertise time and cost.

2. The newly proposed multi-layered architecture and ontology-based transformation system (OBTS), in which, the proposed model and XDT are realized, can serve experts who operate in terms of the forensics domain in reducing the time needed for the appropriate tool for digital evidence investigation selection from the NIST tool catalog.
3. The newly proposed method is based on:
    - Habits identification domain (HiD) model distinguished from the already existing solutions by its integration of the specific methods adopted from intelligence and traditional profiling in order to obtain information that helps to create a digital profile with the suspect user's habits attributes and then consider it during evidence investigation.
    - Digital evidence object (DEO) model is distinguished from the currently existing solutions because it supports situation-aware intelligent time-critical decision making and automated knowledge discovery in the digital forensics domain.
4. In situations when an expert has some information of the suspicious user, such as the user name, the nickname or other data, the habits identification domain (HiD) model may be used for getting the user profile of the potential offender as quickly as possible, and I achieve an average of 27 times reduced number of the representative evidence objects for the first review.
5. In situations when the expert does not know anything about the suspicious user, the digital evidence object (DEO) model may be used and achieve an average of 24 times reduced number of representative evidence objects for the first review.
6. The developed DEIC (Digital Evidence Investigation of Cybercrime) tool proves the practical applicability of the proposed method for assisting a computer forensics expert and formalizing

the examination phase of the digital forensic investigation process, reducing the amount of data to investigate from a suspicious system or a digital device thus accelerating acquisition of digital evidence.

Relevance of the thesis

Investigation of cybercrime poses many challenges for law enforcement and those responsible for ensuring information security. The main ones are: understanding of the specifics of the objects under consideration and the ability to analyze the data properly; knowledge of the laws governing general criminal investigation processes, new legal documents regulating the cyber space; ability to assess various risks. The challenges outlined above have influenced the evolution of tools, models and methods for the investigation of digital evidence in cybercrime, which has led to increasing demands imposed on experts. Yet, criminals have also become more cautious and realized that their actions can be tracked and that any digital footprints that they leave may later become evidence in court. Recent trends indicate that criminals are taking steps to complicate the work of experts by using data encryption methods, using automated tools to hide digital evidence, and avoiding the use of their own computers directly to commit crimes.

Specialized methods and tools can reduce the amount of data analyzed as digital evidence, help an expert to extract digital evidence, and shorten the time needed to perform expert analysis

The object of research

The object of this dissertation is the methods of cybercrime investigation designed to improve the process of expert investigation by reducing the searching time for digital evidence.

The aim of the thesis

The main aim of the dissertation is to enrich the area of cybercrime forensic investigation process by proposing an expert investigation method that would help the expert find digital evidence, reduce the sample of data for expert investigation, and shorten the search time for digital evidence.

The objectives of the thesis

In order to achieve the objective of the dissertation and solve the

scientific problem, the following tasks have been set:

1. To analyze the already existing methods, models and tools for expert investigation of cybercrime.
2. To develop a new approach which incorporates user-habits profiling and digital evidence object models.
3. To experimentally test and evaluate the tool developed by searching for digital evidence of cybercrime.

Research methodology

The following research methods were used to achieve the objective of the work:

1. Comparative analysis of scientific literature on the already existing techniques, models, and tools for cybercrime.
2. An experimental study of the proposed method and ontology-based transformations in the field of digital crime investigation, user-habits profiling, digital evidence, object models performed by using the developed tool in order to substantiate and evaluate the author's proposals.
3. A method of structured evaluation and generalization of the research and analysis results.

Scientific novelty of the thesis

The scientific novelty has been proven by the following results:

1. A method for profiling the attributes of user-habits for searching of cybercrime digital evidence has been proposed.
2. A two-stage ontology-based transformation model and an ontology-based transformation system have been proposed to enable the selection of an appropriate tool for searching for cybercrime digital evidence.
3. A method based on the digital evidence object model for cybercrime has been proposed.

Practical value of research findings

A tool has been developed and experimentally investigated for the search of cybercrime digital evidence which:

1. Allows reducing the sample size of the expert study data.
2. Enables the expert to more quickly evaluate the results provided by the tool and to extract digital evidence from the data by using patterns of user-habit attribute profiling and digital evidence

object models.
3. Can be used when urgent evaluation of cybercrime digital evidence is needed.

Defended statements

1. User-habit attribute profiling allows reducing the amount of data for forensic investigations performed during search for cybercrime digital evidence.
2. The digital evidence object model allows the selection of a reduced representative sample of data focusing on the potential offender and thus helping the expert to make a decision and to reduce the time of expert investigation.
3. The method based on the profiling of habit attributes and digital evidence object models can be applied both for the case study of an expertise, as well as for using the implemented automatization tool.

Approval of research findings

The materials of the dissertation have been approved at three international scientific conferences. Two articles with the citation index in peer-reviewed journals of the *Clarivate Analytics Web of Science* database have been published:

1. Grigaliūnas, Šarūnas; Toldinas, Jevgenijus; Venčkauskas, Algimantas. An ontology-based transformation model for the digital forensics domain // Elektronika ir elektrotechnika. Kaunas: KTU. ISSN 1392-1215. eISSN 2029-5731. 2017, vol. 23, iss. 3, p. 78-82. DOI: 10.5755/j01.eie.23.3.18337.
2. Šarūnas Grigaliūnas, Jevgenijus Toldinas. "Habits Attribution and Digital Evidence Object Models Based Tool for Cybercrime Investigation". Baltic J. Modern Computing, Vol. 8 (2020), No. 2, 275-292. DOI: 10.22364/bjmc.2020.8.2.05.

Dissertation structure

The scientific work consists of an introduction of the dissertation, five chapters, general conclusions, references, a list of the author's publications, and 2 appendices. The total scope of the dissertation is 98 pages without annexes. There are 31 pictures and 23 tables in the text. 208 references were used in the dissertation text.

UDK 004.056 (043.3)

SL344. 2020-07-23, 3,75 leidyb. apsk. l. Tiražas 50 egz.
Išleido Kauno technologijos universitetas, K. Donelaičio g. 73, 44249 Kaunas
Spausdino leidyklos „Technologija“ spaustuvė, Studentų g. 54, 51424 Kaunas