KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Šarūnas Grigaliūnas

ELEKTRONINIŲ NUSIKALTIMŲ PĖDSAKŲ IR ĮTARIAMOJO ĮPROČIŲ KORELIACIJA

Baigiamasis magistro darbas

Vadovas
Doc. dr. Javgenijus Toldinas

KAUNAS, 2015

KAUNO TECHNOLOGIJOS UNIVERSITETAS
INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

TVIRTINU
Katedros vedėjas
(parašas) Prof. dr. Algimantas Venčkauskas
(data)

ELEKTRONINIŲ NUSIKALTIMŲ PĖDSAKŲ IR ĮTARIAMOJO ĮKALČIŲ KORELIACIJA

Baigiamasis magistro darbas
Informacijos ir informacinių technologijų sauga (kodas 621E10003)

Vadovas
(parašas) Doc. dr. Jevgenijus Toldinas
(data)

Recenzentas
(parašas) Doc. dr. Gediminas Činčikas
(data)

Projektą atliko
(parašas) Šarūnas Grigaliūnas
(data)

KAUNAS, 2015

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Informatikos fakultetas

(Fakultetas)

Šarūnas Grigaliūnas

(Studento vardas, pavardė)

Informacijos ir informacinių technologijų sauga (kodas 621E10003)

(Studijų programos pavadinimas, kodas)

Baigiamojo projekto „Elektroninių nusikaltimų pėdsakų ir įtariamojo įpročių koreliacija“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

20 15 m. gegužės 19 d.

Kaunas

Patvirtinu, kad mano **Šarūno Grigaliūno** baigiamasis projektas tema „Elektroninių nusikaltimų pėdsakų ir įtariamojo įpročių koreliacija“ yra parašytas visiškai savarankiškai, o visi pateikti duomenys ar tyrimų rezultatai yra teisingi ir gauti sąžiningai. Šiame darbe nei viena dalis nėra plagijuota nuo jokių spausdintinių ar internetinių šaltinių, visos kitų šaltinių tiesioginės ir netiesioginės citatos nurodytos literatūros nuorodose. Įstatymų nenumatytų piniginių sumų už šį darbą niekam nesu mokėjęs.

Aš suprantu, kad išaiškėjus nesąžiningumo faktui, man bus taikomos nuobaudos, remiantis Kauno technologijos universitete galiojančia tvarka.

(vardą ir pavardę įrašyti ranka) *(parašas)*

Grigaliūnas, Š. Elektroninių nusikaltimų pėdsakų ir įtariamojo įpročių koreliacija. *Kvalifikacinio laipsnio pavadinimas* baigiamasis projektas / vadovas doc. dr. Javgenijus Toldinas; Kauno technologijos universitetas, informatikos fakultetas, kompiuterių katedra.

Kaunas, 2015. 51 psl.

Grigaliunas, S. The correlation between the evidence of cibercrime and suspect habits. Master‘s thesis / supervisor Assoc. Prof. Dr. Jevgenijus Toldinas; Department of Computer Science, Faculty of Informatics, Kaunas University of Technology. – Kaunas, 2015. – 51 p.

SANTRAUKA

Elektroninis nusikaltimas atliktas nuotoliniu būdu yra ypač sunkiai įrodomas. Elektroninių bylų tyrėjams, poėmio menu, pateikta kompiuterinė įranga ir skaitmeninės laikmenos priklausymas konkrečiam įtariamajam, kuris atliko nusikaltimą fiziškai nekontaktuodamas, sąsajumą padaryti labai sunku. „Bendras įpročio profiliavimas“ – tai metodas veikiantis skaitmeninėje aplinkoje, kurį galima būtų prilyginti pirštų anspaudams. Naudojant matematines koreliacijos skaičiavimo modelį skaitmeninį pėdsaką galima palyginti su kitu rastu, dar neidentifikuotu elektroniniu pėdsaku. Turint bendrą profilių duomenų įrašymo ir kopijavimo valdymo sistemą galima panaudoti net tik elektroninių nusikaltimų prevencijai, bet ir intelektualios nuosavybės savininkui nustatyti.

SUMMARY

Cybercrime carried out remotely is extremely difficult to prove. Electronic files for researchers, seizure art, the computer equipment and digital media belonging to a particular suspect, who carried out the crime physically, make connection very difficult. Total habit profiling '- is a method of operating a digital environment, which can be equated with fingerprints. Using a mathematical model for calculating the correlation digital footprint can be compared with any other written yet unidentified electronic fingerprint. A common profiles data recording and reproduction management system can be used not only in cyber crime prevention, but also to identify the owner of the intellectual property.

TURINYS

Lentelių sąrašas 6
Paveikslų sąrašas 7
Terminų ir santrumpų žodynas 8
Įvadas 9
1. eletroninių nusikaltimų ir jų pėdsakų analizė 11
1.1. Elektroninių nusikaltimų pėdsakų klasifikacija 11
1.2. Elektroninių nusikaltimų procesas 12
1.3. Skaitmeninės ekspertizės procesas ir skaitmeninių įrodymų analizė 13
1.3.1. Skaitmeninės ekspertizės principai 14
1.3.2. Skaitmeninės ekspertizės metodika 14
1.3.3. Skaitmeninės ekspertizės procesas 14
1.3.4. Tyrimo proceso kūrimas 14
1.3.5. Skaitmeniniai įrodymai 15
1.4. Analizės tikslas 16
1.5. Išvados 16
2. eletroninių nusikaltimų pėdsakų fiksavimo metodikos projektavimas 17
2.1. Elektroninio pėdsako aptikimo sistemos struktūra 18
2.2. Vartotojo skaitmeninis profiliavimo procesas 18
2.2.1. Kompiuterinės sistemos elektroninių pėdsakų aptikimo sritys 19
2.2.2. Skaitmeninio profiliavimo metodas 20
2.2.3. Skaitmeninio profiliavimo proceso modelis 20
2.2.4. Elektroninio pėdsako indentifikavimo sistemos valdymo procesų modeliavimas 28
2.3. Išvados 36
3. Elektroninių nusikaltimų pėdsakų fiksavimo metodikos ir modelio eksperimentinis tyrimas 37
3.1. Eksperimentinio tyrimo scenarijus 37
3.2. Eksperimentinio tyrimo eiga 37
3.3. Eksperimentinio tyrimo rezultatų apibendrinimas 45
3.4. Išvados 48
4. IŠVADOS 50
5. Literatūra 51
6. Priedai 53
6.1. priedas. Tyrimo profilio gauti įkalčiai ir jų fiksavimas 53
6.2. priedas. Įkalčių fiksavimo realizavimas 53
6.3. priedas. S(i) – socialinio tinklo sąsajumas 54
6.4. priedas. Tyrimo metu įgytos kompetencijos siejamos su tyrimo atlikimu 58
6.5. priedas. Straipsniai 59

LENTELIŲ SĄRAŠAS

1.1 lentelė. Esamų diskų analizės sprendimų (nemokamų) palyginimas.....14
2.1 lentelė panaudos atvejo „įjungti pėdsakų atitikimo“ specifikacija 30
2.2 lentelė panaudos atvejo „Namų direktorijos“ įkalčių sąsajumo specifikacija 31
3.1 lentelė Informacijos filtravimas pagal indikatorius 38
3.2 lentelė Įkalčių analizės rezultatas.....43
3.3 lentelė Įkalčių, naudojant S(i), analizės rezultatas.....45
3.4 lentelė Šaltinio pasitikėjimo matavimo apibūdinimas 48

PAVEIKSLŲ SĄRAŠAS

1.1 pav. Elektroninio pėdsako sąsajos su įtariamuoju algoritmas....15
2.1 pav. Hierarchinės struktūros modelis....18
2.2 pav. Skaitmeninio pėdsako ir įpročio koreliacijos algoritmas....26
2.3 pav. Namų direktorijos sistemos procesų valdymo modelis....28
2.4 pav. Detalizuotas namų direktorijos būsenos keitimo procesas....29
2.5 pav. Sąsajumo valdymo sistemos procesų modelis....29
2.6 pav. Elektroninio pėdsako identifikavimo valdymo sistemos reikalavimų modelis....30
2.7 pav. Elektroninio pėdsako identifikavimo valdymo sistemos koncepcinis duomenų modelis....32
2.8 pav. Indikatoriaus koncepcinio duomenų modelio detalizavimas....33
2.9 pav. Elektroninio pėdsako sistemos duomenų esybės būsenų diagrama....34
2.10 pav. Vartotojo (tyrėjo) “ncurses” sąsaja....35
2.11 pav. Elektroninių pėdsakų valdymo sistemos diegimo diagrama....36
3.1 pav. Windows OS registrai....38
3.2 pav. Elektroninių nusikaltimų pėdsakų fiksavimas....44
3.3 pav. Elektroninių nusikaltimų pėdsakų fiksavimo koreliacija su S(i)....45
3.4 pav. Profilio informacinis rezultatas....47

TERMINŲ IR SANTRUMPŲ ŽODYNAS

Įprotis – tai žmogaus veiklos elektroninėje erdvėje susiformavęs polinkis atlikti tam tikrą veiksmą, kuris gali būti prilygintas elektroniniam pirštų anspaudui.

Profilis – tai skaitmeninių indikacijų visuma.

Idioma – reikšmė, kuri nesutampa su atskirai paimtų dėmenų reikšmėmis.

Modus operandi (MO) – operatyvinis metodas (naudojama operatyviosios informacijos surinkimui).

Indikatorius – rodikliai renkami ir analizuojami duomenų tyrimo kontekste.

Pasitikėjimas – įvertis informacijos siuntėjui ir gavėjui.

Snapshot – veikiančios operacinės sistemos momentinis atvaizdas.

ĮVADAS

Tiriant įvairių rūšių nusikaltimus labai dažnai tenka tirti ir kompiuteriuose, mobiliuosiuose telefonuose, kituose skaitmeniniuose įrenginiuose esančią informaciją, kuri būna saugoma arba slepiama įvairiomis formomis ir kuri dažniausiai turi tiesioginį ryšį su tyrimo aplinkybėmis, todėl sparčiai auga informacinių technologijų tyrimų poreikis. Be to, siekiant įvykio vietoje tinkamai paimti tyrimo objektus ir juos išsaugoti taip pat yra būtinos tam tikro lygio informacinių technologijų žinios. Netinkamai paėmus ir apžiūrėjus tyrimo objektus neretai labai pasunkinamas tyrimų atlikimas, o kartais atlikti tyrimą išvis būna nebeįmanoma. Lietuvos policijos kriminalistinių tyrimų centro ir Lietuvos teismo ekspertizių centro specialistai ir ekspertai nebespėja atlikti šios rūšies tyrimų sparčiai augant jų poreikiui. Ikiteisminio tyrimo įstaigose būtina turėti parengtą specialistą, sugebantį tinkamai paimti tyrimo objektus, prireikus atlikti jų apžiūrą, atlikti nesudėtingą skaitmeninėse laikmenose esančios informacijos analizę, konsultuoti tyrėjus informacinių technologijų tyrimo skyrimo klausimais.

Todėl šiandien svarbios problemos yra kompiuterinės informacijos saugojimas, paieška bei ilgalaikio informacijos naudojimo galimybių užtikrinimas, tai daro tiesioginę ištaką tiriant nusikaltimus, daromus šioje specifinėje aplinkoje. Tyrėjai, tirdami nusikalstamas veikas, ieško informacijos apie objektyvios tikrovės faktus, įvykius, reiškinius bei žmogaus mąstymo, įpročių rezultatus, dažniausiai fiksuotus dokumentuose. Kompiuterinės informacijos atsiradimas bei sparti sklaida lemia ir nusikaltimus tiriančių pareigūnų darbo pokyčius. Jie susiduria su nauju reiškiniu – kompiuteriniais nusikaltimais bei nusikaltimų pėdsakus fiksuojančiais elektroniniais išrašais – dokumentais, kurie keičia nusistovėjusią šių nusikaltimų tyrimo praktiką ir darbo metodus.

„Namų direktorijos“ (arba virtualios aplinkos) susikūrimas laikui bėgant tampa daliniu įpročiu. Kaip pavyzdys tai gali būti rašybos klaida dokumentuose, direktorių užvadinimas, rekvizitai dokumentuose, meta duomenys, failų užvadinimas, paieškos raktai (iš istorijos saugomų bylų), raktinių žodžių pasikartojimas ir t.t. Tai leidžia sutapatinti elektroninį pėdsaką su asmenybę (tapatybės identifikavimas), įrenginiu (USB, kietasis diskas, CD/DVD), mobiliu telefonu, socialiniu profiliu, komentarai internete ar kita elektroninės informacijos saugojimo priemone. Įvairūs davikliai („source crowler“, „grabber“, „snapshots“, „dump“ ir k.t.) renka ir klasifikuoja informaciją pvz., apie padaryta tokia pat klaidą, sudarytą toki pat medį, konkrečioje vietoje atliktą veiksmą (pvz.: foto), jei tas failas turi tokius meta duomenis. Aptikus pėdsaką informacija apdorojama, dedama prie „pėdsako“ sąsajų su bylomis. Jei tai aptinkama socialiniam tinkle (įtariamasis pasinaudojo išmaniuoju telefonu, padarė foto su gps koordinatėmis), vykdomi prevencijos ar sulaikymo veiksmai.

Darbo problematika ir aktualumas

Elektroninis nusikaltimas atliktas nuotoliniu būdu yra ypač sunkiai įrodomas. Elektroninių bylų tyrėjams, poėmio menu, pateikta kompiuterinė įranga ir skaitmeninės laikmenos priklausymas konkrečiam įtariamajam, kuris atliko nusikaltimą fiziškai nekontaktuodamas, sąsajumą padaryti labai sunku.

Nustačius „bendrą įpročio profilį“ skaitmeninėje aplinkoje, tai galima būtų prilyginti pirštų anspaudui. Naudojant matematinę koreliaciją galima įprotį palyginti su kitu rastu, dar neidentifikuotu elektroniniu pėdsaku. Turint bendrą duomenų įrašymo ir kopijavimo valdymo sistemą galima panaudoti net ir intelektualiniai nuosavybei nustatyti.

Darbo tikslas ir uždaviniai

Naudojantis įvairiais elektroninio pėdsako fiksavimo būdais, aprašyti elektroninio pėdsako palyginimo sistemos metodą, kuris koreliuotu su įtariamojo įpročiu (-iais).

Sukurti elektroninių nusikaltimų (po įvykdyto fakto) pėdsakų profilių koreliavimo būdą;

Realizuoti pėdsakų fiksavimo dalį;

Pritaikyti elektroninių pėdsakų fiksavimo ir profiliavimo koreliaciją įrodinėjant įtariamojo tapatybę.

Darbo rezultatai ir jų svarba

Tikslesnis metodas susieti gautą elektroninį pėdsaką su konkrečiu įtariamuoju. „Elektroninis profilis“ ateityje gali tapti pirštų anspaudų analogija tiriant nusikaltimus elektroninėje erdvėje.

Darbo struktūra

Elektroninių nusikaltimų ir jų pėdsakų analizė;
Elektroninių nusikaltimų pėdsakų fiksavimo metodikos projektavimas;
Elektroninių nusikaltimų pėdsakų fiksavimo metodikos ir modelio eksperimentinis tyrimas;
Gautų eksperimentinio tyrimo rezultatų palyginimas.

1. ELETRONINIŲ NUSIKALTIMŲ IR JŲ PĖDSAKŲ ANALIZĖ

1.1. Elektroninių nusikaltimų pėdsakų klasifikacija

“Pėdsako” samprata žymiai platesnė, nei tradiciškai kriminalistikoje skirstomi į materialiuosius ir idealiuosius. Jie apima visą tyrėjo tyrimo renkamą informacijos visumą, kuri reikšminga nustatant teisingą paieškos, tyrimo, versijų kėlimo, tyrimo veiksmų kryptį. Plačiąja reikšme – tai įvairios materialios pasekmės rengiantis, darant bei slepiant nusikaltimą. Pėdsakai medžiagos – tai kietos, skystos ar lakios substancijos, atspindinčios pėdsaką sudarančio objekto vidinę sandarą. Tačiau nepakanka vien tradicinės kriminalistinės pėdsakų sampratos tiriant kompiuterinius nusikaltimus.

Prasidėjus elektroninių nusikaltimų erai mokslininkai ieško naujų sąvokų, kurios galėtų tiksliau išreikšti šių nusikaltimų formas, darymo būdus bei padėtų veiksmingiau fiksuoti šiuos specifinius pėdsakus. Vienas Rusijos mokslininkų V. A. Meščiarikovas pasiūlė kriminalistikoje vartoti terminą – „kibernetinė erdvė“ [1]. Tokia sąvoka išdomi, nes suvokiama kaip daugialypis daugiasluoksnis informacijos objektas, kurio sandara priklauso nuo „kompiuterinės informacijos ypatybių“ bei „automatizuotų informacinių sistemų principų”. Taip yra išskiriami aštuoni lygiai:

- pasaulinis informacinis tinklas (internetas ar kt.);
- vietinis informacinis tinklas (kompiuterių sistema);
- kompiuteris (gali būti ir specializuotos paskirties);
- elementari kompiuterinė sandaros grandis (laikmena);
- pirmo lygmens informacinė struktūra (loginis informacijos nešėjas);
- antro lygmens informacinė struktūra (failas);
- trečio lygmens informacinė struktūra (failo įrašas);
- elementari informacinė grupė (16, 32, 64) ar vienas šalia kito sudėlioti baitai, baitas ar net bitas.

Tokiu būdu, kompiuterinio nusikaltimo pėdsakai atsiranda „kibernetinėje erdvėje“. Beje, panašių terminų yra ir kai kurių lietuvių bei Vakarų Europos autorių straipsniuose, kurie teigia, kad „kibererdvė“ – tai „kompiuterinių tinklų kuriama nauja erdvė, kurioje vyksta individų komunikacija ir kiti socialiniai procesai“ [2].

Elementai gali būti suvokiami kaip informaciniai, bei techniniai objektai. Toks sudėtingumas išdėstyti bei suderinti pėdsakų objektų ypatybes teikia galimybes daryti išvadas, kad:

- neveiksminga tiriant kompiuterinius nusikaltimus naudoti dvi pėdsakų rūšis – materialiuosius ar idealiuosius, nes pėdsakų susidarymo reiškiniai čia suvokiami „mechaniškai“;
- idealiųjų ir materialiųjų pėdsakų santykis kompiuteriniuose nusikaltimuose sprendžiamas idealiųjų naudai;
- atsiranda nauja ypatinga „virtualiųjų“ pėdsakų grupė, sąlygota specifinių „kibernetinėje erdvėje“ vykstančių procesų, kurie žmogaus juslėmis nesuvokiami, todėl jie ir atsiduria tarp idealiųjų ir materialiųjų pėdsakų;
- „virtualieji“ pėdsakai labai nepastovūs (savaip „lakūs“), pirma – dėl „subjektyvumo“ veiksnio, t. y. tiesioginės priklausomybės nuo jo nuskaitymo, nustatymo budo, antra – tvirto ryšio tarp „virtualiojo“ pėdsako informacijos ir ją įrašiusio įrenginio ar įrangos, ir trečia – dėl „virtualiųjų“ pėdsakų laikinumo;
- „virtualieji“ pėdsakai nepatikimi, nes yra galimybė juos neteisingai nuskaityti.

Sąvoka “kibernetinė erdvė” pelnytai apima viską, kas susijęs su kompiuterinėmis technologijomis. „Elektroninio“ pėdsako sąvoka vartojama ir kitų mokslininkų darbuose, tačiau dažniausiai norint išskirti laiko atžvilgiu neaiškų pėdsaką formuojantį objektą, kai kažkuriuo abstrakčiu pėdsakų susidarymo momentu susidaro nevienareikšmiška subjekto nustatymo, inicijavusio lokalų kompiuterinės informacijos apdorojimą, situacija (kitaip tariant, kai esamu momentu neaišku, kas paliko pėdsaką). Techninės bei programinės kompiuterinės įrangos naudojimas yra būtinas norint pajusti, taip pat ir ieškant, fiksuojant bei paimant kompiuterinių nusikaltimų pėdsakus. Tačiau tai nėra

tokia svarbi aplinkybė, dėl kurios į kriminalistikoje vartojamų sąvokų sąrašą turėtume nedvejodami ištraukti ir „elektroninio“ pėdsako formuluotę. Kompiuterinio nusikaltimo pėdsako susidarymas veikiamas tam tikro mechanizmo (mechaninio, fizikinio ar net cheminio), šis pėdsakas lieka ant materialaus objekto, todėl logiška manyti, kad tai yra ne kitoks, o materialusis pėdsakas.

Kalbėdami apie teorinius dalykus visada turime prisiminti ir praktinio šių žinių naudojimo galimybę. Juk kompiuteriniams nusikaltimams dažnai būdingas ne tik vietinis, bet ir tarptautinis mastas. Tad kaip renkami išrodomąją reikšmę turintys objektai, esantys kitos valstybės teritorijoje? Tarkim, norime gauti informacijos apie padaryto kompiuterinio nusikaltimo ar pažeidimo pėdsakus, kurios laikmena – užsienio valstybės jurisdikcijoje esantis serveris. Šiuo atveju privalėsime kreiptis į šios valstybės teisėsaugos institucijas, ir tik jie turės teisę ištirti mus dominančią informaciją ir tik tiek, kiek tai leidžia tarptautiniai teisinės pagalbos susitarimai, nes priešingu atveju iš karto kyla ne tik savarankiškų veiksmų legitimumo (nes tai prieštarauja pagrindiniams tarptautinių norminių teisinių susitarimų dėl kovos su kompiuteriniais nusikaltimais principams), bet ir surink- tų duomenų naudojimo išrodinėjimo procese leistinumo klausimas. Todėl teiginys, kad nacionalinės teisėsaugos atstovai, tiriantys kompiuterinius nusikaltimus, negali gauti juos dominančios informacijos [3].

Kompiuterinių nusikaltimų pėdsakai susidaro ne kažkur „kibernetinėje erdvėje“, o tik esant konkrečioms nusikaltimo aplinkybėmis, kai neteisėtos veikos subjekto kompiuterine technika paveikiama kompiuterinė informacija.

1.2. **Elektroninių nusikaltimų procesas**

Pėdsako padarymo mechanizmas – tai specifinė konkreti proceso forma, kurios paskutinėje stadijoje susidaro pėdsakas atspindys. Kompiuterinės informacijos laikmenose informacija gali būti įrašoma laikinai ar saugoma nuolat, todėl šias laikmenas galima suskirstyti į laikinuosius bei pastoviuosius informaciją saugančius įrenginius – kaupiklius [4]. Išskirsime šias informacijos saugojimo formas: vaizdinę (žmogui priimtina forma suvokiama kompiuterinė informacija, pvz., simboliai, grafika, garsas); nevaizdinę loginę (kompiuterinė informacija, suvokiama loginėmis kompiuterių duomenų struktūromis); nevaizdinę fizikinę (kompiuterinė informacija čia suprantama kaip fizikinės struktūros – tai galėtų būti elektromagnetinis laukas, taip pat laidininkų, puslaidininkių, magnetiniai, magnetooptiniai ir optiniai įrengimai kaip šio lauko bei informacijos nešėjai). Žmogus (subjektas) daro poveikį suvoktai informacijai, po to ši informacija verčiama į skaitmeninę formą (tai būtina, jei norime šią informaciją apdoroti programine kompiuterinės technikos įranga). Vėliau kompiuterinė informacija virsta elektromagnetiniu signalu (tai būtina, jei norime šią informaciją apdoroti technine kompiuterine įranga, tarkim, įrašyti į laikmenas ar kt.) [5].

Kompiuterinių nusikaltimų pėdsakai juos tiriančiam subjektui suvokiami žmogui priimtina forma, t. y. dažniausiai naudojant kompiuterinę techniką. Tradicinės kompiuterinės technikos skirstymas į „programinę“ bei „techninę“ jau nuo pat pradžių buvo, galima sakyti, abejotinas, jei tik buvo kalbama apie kompiuterinės informacijos apdorojimą bei saugojimą [6]. Net Lietuvos Respublikos gyventojų pajamų mokesčio išstatyme yra „asmeninio kompiuterio vieneto su programine įranga“ sąvoka, kurią sudarančių elementų sąrašą papildo Informacinės visuomenės plėtros komiteto prie Lietuvos Respublikos Vyriausybės įsakymas „Dėl asmeninio kompiuterio vienetą sudarančių elementų sąrašo patvirtinimo“, bei Lietuvos Respublikos kibernetinio saugumo įstatymas [7], kurie apibrėžia, kad kompiuteris yra visuma techninių priemonių su programine įranga, be kurios jis tampa tik „gėlių vazonu“.

Kompiuterinė informacija yra pėdsaką priimantis objektas. Atitinkamai elektroninių nusikaltimų pėdsakai bendrąją reikšme ir yra ta pati kompiuterinė informacija. Elektroninių nusikaltimų pėdsakų susidarymui, suskirstyti taip [8]:

- kompiuterinės informacijos kokybinius ypatumus;
- informacijos objekto naudojamos kompiuterinės įrangos ypatybes bei charakteristikas;
- kompiuterinės informacijos materialiąsias išraiškos formas, žmogaus suvokiamas intuityviai ir lengvai apdorojamas programine technine kompiuterine įranga;
- neteisėtos veikos subjektų poveikio formas kompiuterinės informacijos apdorojimo,

perdavimo ar saugojimo procesams;
- kompiuterinės informacijos pateikimo tarpinių skaičiavimų bei informacijos laikmenose formas.

1.3. **Skaitmeninės ekspertizės procesas ir skaitmeninių įrodymų analizė**

Kompiuteriai ir tinklai tapo tokie susiję su mūsų kasdieniu gyvenimu, kad beveik į bet kokį tyrimą įeina kokie nors **skaitmeniniai įrodymai**. Tokie nusikaltimai kaip vaikų išnaudojimas ir vaikų pornografija, sukčiavimas, narkotikų gabenimas, terorizmas ir žmogžudystės dažnai yra susiję su kompiuteriais ir elektroniniais skaitmeniniais prietaisais.

Nusikaltimo atkūrimo mokslas (arba menas) gaunant ir analizuojant skaitmeninius įrodymus yra vadinamas **skaitmeninės ekspertizės** arba **kompiuterinės ekspertizės** arba **elektroniniai atradimai.**

Turėtume žinoti, kad visi elektroniniai prietaisai, tokie kaip CD, DVD, USB „flash“ laikmenos, kietieji diskai (HDD), atminties kortelės / lazdelės, SIM kortelės, išmanieji telefonai, mobilieji telefonai, planšetiniai ir pan., fiksuoja mūsų informaciją, įskaitant ir ištrintus duomenis. Ieškodami skaitmeninių įrodymų mes turime žiūrėti į telefonų knygas, sms / mms žinutes, paveikslėlius, dokumentus tokius kaip tekstiniai failai, skaičiuoklės, sistemos įrašai, maršrutizatoriaus įrašai, ugniasienės įrašai, IDS įrašai ir sukaupti interneto failai.

Skaitmeninės ekspertizės mums leidžia atkurti įvykius skaitmeniniame prietaise. Seniau tai buvo daroma tik su kompiuteriais, bet dabar skaitmeninė ekspertizė apima visus skaitmeninius prietaisus tokius kaip mobilieji telefonai, skaitmeninės kameros ir net GPS prietaisai. Jie buvo naudojami pagaunant žudikus, pagrobėjus, sukčius, mafijos bosus ir daugelį kitų nedraugiškų žmonių.

Ką žmonės darė vietiniu kompiuteriu. Į tai įeina [9].

- Ištrintų failų atkūrimas
- Elementarus iššifravimas
- Tam tikro tipo failų ieškojimas
- Tam tikrų frazių ieškojimas
- Įdomių kompiuterio vietų apžiūra

Ką nuotoliniai vartotojai darė tinkle. Į tai įeina.

- Įrašų failų skaitymas
- Veiksmų rekonstrukcija
- Šaltinių atsekimas

Pagal elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011 - 2019 metais programą, yra siekiama užtikrinti Lietuvos gyventojų, organizacijų bei visos valstybės saugumą kibernetinėje erdvėje. Tam būtina kelti elektroninės informacijos saugos kultūrą: rengti kibernetinio saugumo specialistus, ruošti jų kvalifikacijos tobulinimo programas. Taip pat didelę reikšmę turi parengtų informatikos teisės specialistų skaičius bei atliekami moksliniai tyrimai informatikos teisės srityje. Galiausiai, iki 2019 m. norima įsteigti bent 1 laboratoriją, skirtą neteisėtos veiklos kibernetinėje erdvėje skaitmeninių įrodymų analizei. Skaitmeninių kriminalistinių tyrimų sritis yra pakankamai sudėtinga, reikalaujanti aukštos kompetencijos. Lietuvoje jau pradėta panašaus tipo veikla - L3CE („Lietuvos kibernetinių nusikaltimų kompetencijų ir tyrimų centras“), kur bus nagrinėjami elektroniniai nusikaltimai ir apmokomi pareigūnai juos tirti.

AccessData ne vieninteliai gali pasiūlyti skaitmeninių tyrimų sprendimus statiškiems, kintantiems ir tinkle esantiems duomenims. FTK [10] visame pasaulyje laikomas skaitmeninių tyrimų kokybės standartu dėl savo intuityvių sąsajų, el. laiškų analizės, pagal poreikius keičiamų duomenų apžvalgos ir stabilumo. Šis sprendimas leidžia vartotojams apdoroti daug duomenų: nuo skaitmeninių vaizdų iki el. laiškų archyvų; analizuoti registrus, vykdyti tyrimus, iškoduoti failus, slaptažodžius. Taip

pat svarbus pastebi, kad yra nemokamas AutoPSY [11] sprendimas. Šis sprendimas yra skirtas bylų nagrinėjimui. Jis leidžia susikelti informaciją, ją indeksuoti ir vėliau atlikti kryptingas paieškas. Šią sistemą ir panaudosim, kai bus ieškomas I (indikacijos) ar sąsajos tarp įtariamojo ir gautų duomenų.

1.1 lentelė. Esamų diskų analizės sprendimų (nemokamų) palyginimas

Palyginimo kriterijus	**FKT Imager**	**LiveView [12]**	**AutoPSY**	**Disk2VHD [13]**
Sistemų formatai	Virtualių ir Raw	Vmware, VirtualBox	Virtualių ir Raw	Hyper-V
Vartotojų sąsaja	Windows aplikacija	Java aplikacija	Java, Python	Windows aplikacija
Snapshot	DD	DD	-	Raw
Kontrolinės suma	MD5	nenaudojama	Naudoja	nenaudoja
Pėdsako sąsaja	Yra galimybė įsidėti į atmintinė (Note)	Nėra	Yra galimybė įdėti į atmintinę	nėra
OS (darbo aplinkos)	Windows	Windows, Linux, OSX	Windows, Linux, OSX	Windows

Labai akivaizdus pavyzdys, kai yra naudojami instrumentai ištirti, o svarbiausiai susieti juos su įtariamuoju, neturi tokios funkcinė galimybės.

Tokį, subjektyvų funkcionalumą ir noriu pasiūlyti, kaip tyrimą, įrodyti galimybę susieti žmogiškąjį įprotį su failų sistemoje esančiais failai (ar kai kuriais atvejais įrenginiu).

1.3.1. Skaitmeninės ekspertizės principai

Kaip ir bet koks kitas mokslas, skaitmeninė ekspertizė naudoja apibrėžtus metodus, šiuo atveju norima išlaikyti nepažeistus įrodymus. Apgalvokite priežastis: jeigu praradote įrodymų kontrolę bent minutei, tai jau nebe įrodymai – jie gali būti pakeisti.

1.3.2. Skaitmeninės ekspertizės metodika

Formali skaitmeninė ekspertizė yra kriminologijos šaka, taigi tai yra viskas apie legalų teisinių įrodymų rinkimą. Toliau pateiktas pavyzdys rodo žingsnius, kuriuos reikia atlikti kriminaliniame tyrime [14].

1.3.3. Skaitmeninės ekspertizės procesas

Kai tiriate kompiuterinį nusikaltimą, turite savo darbą paremti procesu. Prieš pradedant skaitmeninį tyrimą jums reikės įrankių rinkinio, kurie būtų **ekspertizės įrankių rinkiniu**. Bet pirmiausiai jums reikia susikurti **tyrimo procesą,** kad įsitikinti jog įrodymai yra tikri, pavyzdžiui dokumentuojant **suėmimo grandinę.** Tada galite sukurti **tyrimo komandą** [15].

1.3.4. Tyrimo proceso kūrimas

Tyrimo procesas turi būti nurodytas iš anksto. Jeigu esate susijęs su bylinėjimuisi, labai tikėtina, kad pateiksite politikos ir procedūrų dokumentą kaip savo veiksmų priežastį. Jeigu esate gynybos komandoje, yra paranku turėti kontrolinį sąrašą tokiems atvejams kai skamba visi aliarmai ir yra sunku susikaupti.

Turbūt pats svarbiausias pavienis dokumentas yra suėmimo grandinės dokumentas, kuriame turi būti vieta kur aprašoma kas tiksliai buvo paimta kaip įrodymas, kas tai paėmė ir koks buvo

tolimesnis suėmimas. Praradote įrodymus bent kelioms minutėms? Greičiausiai jie dabar jau yra beverčiai.

1.3.5. Skaitmeniniai įrodymai

Skaitmeniniai įrodymai yra apibrėžiami kaip bet kokia informacija turinti įrodomąją vertę, kuri yra laikoma arba perduodama skaitmenine forma.

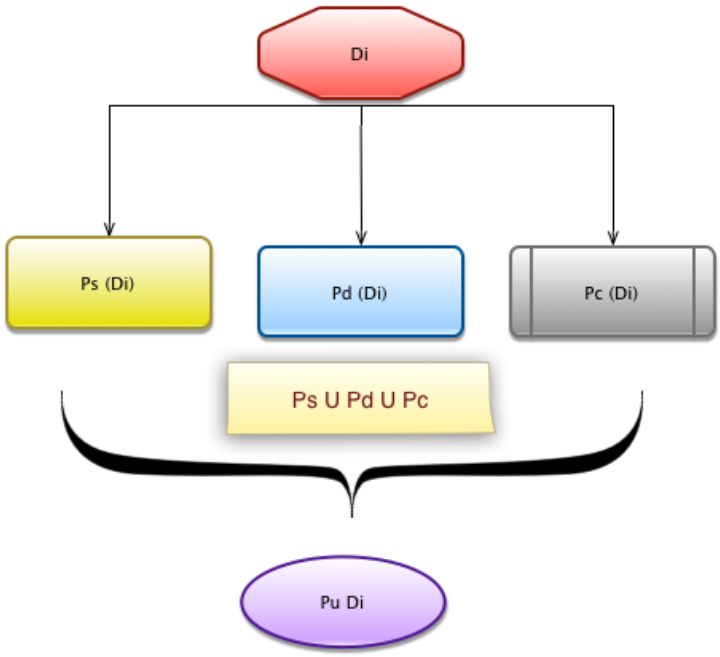
Skaitmeninę informaciją galima surinkti tiriant skaitmenines laikmenas, stebint tinklo eismą arba sudarant skaitmeninių duomenų, rastų skaitmeninės ekspertizės metu, kopijas. Skaitmeniniai įrodymai randami tokiuose failuose kaip[16]:

- Grafiniai failai
- Garso arba vaizdo įrašų failai
- Interneto naršyklės istorija
- Serverių įrašai
- Žodžių apdirbimo ir skaičiuoklių failai
- E-pašto antraštės
- Ugniasienių, maršrutizatorių ir IDS įrašai

Šiai dienai visa programinė įranga analizuoja tik faktą (pėdsakas yra ar nėra), bet niekaip jo nelygina su įrenginiu, kuriam jis buvo rastas, su vartotojo “namų direktorija” [17] tam, kad įrodyti tiesioginę sąsają. Tokio įrankio funkcionalumo pasirinkimą atliksiu analizės dalyje.

Esant pasikartojančiam elektroniniam pėdsakui galima nustatyti nusikaltimą atlikusio asmens tapatybę (PASTABA: jei tokia tapatybė jau yra fiksuota duomenų įrašais).

Naudosime teorinio sprendimo palyginimo (koreliacijos) modelį [18] (1.1 pav.)



1.1 pav. Elektroninio pėdsako sąsajos su įtariamuoju algoritmas

Di - identifikuoja įrenginį (failus, aplinką).
Pd Di - identifikuoja įrenginį profilį;
Pc Di - identifikuoja vartotojo aplanko (namų direktorija) profilį;
Ps Di - identifikuoja tam tikrą sistemos profilis;
Pu Di-Vartotojo profilis

1.4. **Analizės tikslas**

Naudojantis įvairiais būdais ir metodais suprojektuoti elektroninio pėdsako fiksavimo sistemą, kuri būtų valdoma skirtingais profiliais, numatyti profiliavimo ir koreliacijos galimybes. Ji būtų tyrėjui patogi [19].

Tikslui pasiekti keliami sekantys uždaviniai:

- Parengti struktūros modelį
- Parengti procesų modelius
- Aprašyti vartotojo (tyrėjo) reikalavimus
- Sukurti profilio (Pu) sudarymo koncepcinį modelį
- Aprašyti duomenų modelį, duomenų esybės būsenų diagramą
- Sukurti įkalčio (snapshot – momentinis sistemos atvaizdas) fiksavimo sąsają
- Aprašyti koreliaciją tarp skaitmeninio (elektroninio) pėdsako ir įtariamojo profilio

1.5. **Išvados**

Mokslas ir elektroninių nusikaltimų tyrėjai sutinka, kad žmogaus nusikalstama veikla persikėlusi į skaitmeninę erdvę privalo būti tinkamai renkami ir fiksuojami tam, kad įrodyti susikaltimo sudedamąsias dalis.

Apžvelgtas ir pasiūlytas kitoks būdas elektroninių pėdsakų įrodymo būdas – įtariamojo profiliavimas pagal gautus skaitmeninius pirštų anspaudus. Toks pirštų anspaudų sudarymo būdas yra koreliacija tarp: „įpročio“, „namų direktorijos“, „socialinio / paieškos tinklo informacijos dedamosios“ ir poėmio metu sulaikytos kompiuterinės / programinė įrangos.

2. ELETRONINIŲ NUSIKALTIMŲ PĖDSAKŲ FIKSAVIMO METODIKOS PROJEKTAVIMAS

Tyrimų metodų, įskaitant profiliavimo metodus kibernetinėje erdvėje apjungti nėra lengva, ypač kalbant apie tinkamą (fizinį) tyrimo metodą [20]. Pagrindinės priežastys, gali būti apibendrinti taip:

- netinkami ir neišsamūs dokumentai šiuo klausimu;
- sunkumai, kaip sujungti žmogaus prigimtį su kompiuterių mokslo;
- pasireiškia nepasitikėjimas kai kalbama apie tradicinį baudžiamosios atsakomybės profiliavimą ir apskritai psichologinius vartotojo tyrimus.

Siekiant geriau paaiškinti skirtumą tarp skaitmeninio ir tradicinio Profiliavimas, buvo pateikta analitinėje dalyje santykiai tarp tradicinių ir elektroninių pėdsakų. Apie pagrindinius paraleles kalbama ir su profiliavimu modeliais susija Douglas, Ressler, Burgess, Hartman. Skaitmeninis Profiliavimas gali būti vertinga technika ekspertiziniai analizei. Tokių modelių tyrėjai pateikia tik galimo naudojimo pavyzdį. Elgsenos pažeidėjas, taip pat gali būti panašus į kasdieninę elgsena, tačiau ji taip pat gali būti unikali aptariamam asmeniui, ir atsiranda tik spontaniškai. Jei yra pasikartojanti nusikaltimų vieta (kaip serijinio ar pakartoti nusikaltėlio – tai gali būti įprotis), ji yra daug labiau tikėtina. Bet koks unikalus elgesys yra tinkamas patikrinti ir tam reikia modelio.

Trys elementai susieti nusikaltimus ir pasikartojančius nusikaltimus [21]:

- veikimo būdas (modus operandi);
- ritualas (požymiai fantazija ar psichologinį poreikį);
- parašas (unikalūs deriniai elgesį).

Kalbant apie modus operandi (MO), Douglas & Olshaker apibrėžti kaip "ką pažeidėjas turi daryti atlikti nusikaltimą". MO sudaro bent šias sudedamąsias dalis:

- užtikrinti nusikaltimo sėkmę;
- tapatybės apsauga;
- pabėgimo efektas.

Pagal Keppel, prieš 1800-ius, sąvoka "modus operandi" buvo laikomas gyvūnų elgesio aprašymas. Tik po šio laikotarpio, kai terminas pradėjo nesimatytų anglų utilitarizmo literatūros "modus operandi" nurodė žmogaus elgesio aprašymas [22].

Kriminologijos šis apibrėžimas buvo pateiktas: "Modus operandi principas, už kurį baudžiama gali naudoti tą patį metodą kelis kartus, ir bet kokią analizę, ar įrašyti tos metodikos visais sunkiais nusikaltimais suteiks identifikavimo priemones konkrečiam nusikaltimui". Šis apibrėžimas gali būti taikomas su elektroniniais nusikaltimais, taip pat galima nustatyti ritualą ir parašas elementus kaip tradicinių nusikaltimų. Ritualas yra elgesys, kuris viršija būtinas priemones nusikalsti. Pagal apibrėžimą, jis yra potipis kartais vadinamas "ritualo parašas". Pagal šį apibrėžimą ir nusikaltimų klasifikacija vadove, ritualas gali būti taikomos elektroninių nusikaltimų, nors daugiau įsilaužėlių (hakerių) elgesį galima apibūdinti ritualas. Kita vertus, “parašas” - sąvoka geriau atitinka įsilaužėlių pasaulyje. Apskritai, parašas ir elgesio derinys, tai kaip turėtumėm identifikuoti įsilaužėlį. Douglas & Olshaker apibrėžti kaip "kažką nusikaltėlis turi atlikti siekdamos įvykdyti save emociškai ... tai nėra reikalinga sėkmingai įgyvendinti nusikaltimą, tačiau tai gali būti priežastis, jis iškelia konkretų nusikaltimą į pirmąją vietą". Parašas, kaip hakerio elgesys, yra iš "prekės ženklų" serijos. Juo galima rūšiuoti ir atspindėti nusikaltėlių peržengimą padarius nusikaltimą - "išreikšti save". Tai atspindintis tam tikru būdu jų asmenybės. “defacing” išpuoliuose, šis aspektas yra ryškesni nei kitur, nes iš Hack vaidyba tada yra matoma visiems. Šiaip motyvacijos, veiksmai, ir modus operandi tradicinių nusikaltimų atžvilgiu elektroninių nusikaltimų yra skirtingi. Pavyzdžiui, atrodo, kad nuo 2009 metų mes įžengėm į naują erą, kurioje organizuojami nusikaltėliai gali veikti tapatybės vagystės perpardavimo operacijas. Taip pat užsiimama kibernetiniu karu, kuris įsilaužimą kaip daugiapakopio proceso individualizuoja tris pagrindinius etapus – čia pagal bestseleriu Hacking Exposed 3 leidinys (žr. priedai). Šie etapai yra: konkretus atvejas, skenavimas ir išskaičiavimas. Tai nėra šio darbo tikslas aprašyti kiekvieną iš šių etapų, bet tie patys argumentai gali kilti. Pavyzdžiui, veiksmo laikas gali kisti nuo 48/72 valandų nuolat dirba per tinklo įsibrovimo į ilgesnį laikotarpį, pavyzdžiui, įvyko dėl pedofilų

veiksmų. Pasak Richard Stiennon IT Harvest Inc hakeriai rado būdų, kaip supaprastinti tam tikrų klasikinių metodikos taikymų efektyvumą. Visų pirma, pati naujausia tendencija buvo nuo virusų ir Trojos arklys naudojimas kaip modus operandi.

Pagrindinė sritis Taikymas ir galimas indėlis [23]:

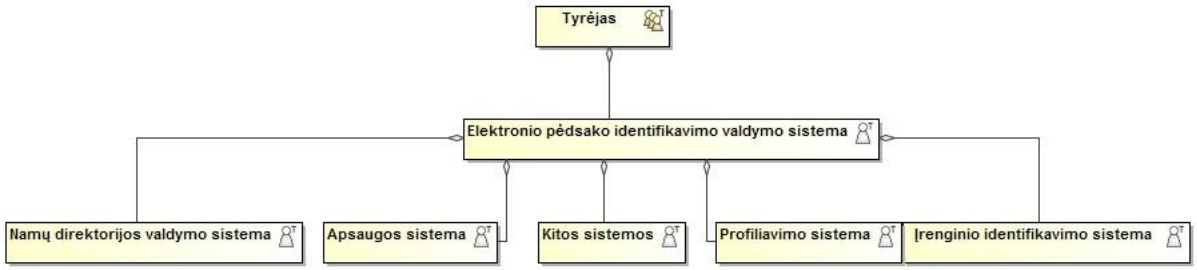
- Incidentų reagavimas ir suprasti atakos tipą
- Ribų tyrimo sritis / įsilaužimo naudojimo / grėsmės / duomenų išvadai / suprasti socialinės inžinerijos technika
- Kompiuterių elektroniniai tyrimai ir baigti tyrimą ištirti duomenų slėpimo supratimas, kaip naudoti / anti ekspertizės / slaptažodžio spėjimai

Skirtumas tas, kad "naujas" metodas naudoja virusus ar Trojos arklius, kuris yra pagal užsakymą pagaminti ir turi tokį patį poveikį kaip ir jei kas nors buvo įdėjęs į tikslinę sistemą keylogger kompiuteryje. Naujasis metodas yra laikomas lengvesniu, nei senas.

2.1. **Elektroninio pėdsako aptikimo sistemos struktūra**

Šioje dalyje, kuriamas elektroninio pėdsako aptikimo sistema. Modeliuojami fiksuojamos informacijos (tyrėjo) valdymo sistemos veiklų procesai. Sudaroma UML panaudos atvejų diagrama, tyrėjų reikalavimų modelis, sudaromas koncepcinis duomenų modelis. Pateikiamas grafinės sąsajos prototipas ir sistemos diegimo diagrama.

Elektroninio pėdsako identifikavimo valdymo hierarchinės struktūros modelis yra pateiktas 2.1 pav.



2.1 pav. Hierarchinės struktūros modelis

Modelyje pavaizduota hierarchinė struktūra, kurioje matome, kad elektroninio pėdsako identifikavimo valdymo sistema, valdo žemesnio lygmens sistemas. Elektroninio pėdsako identifikavimo valdymo sistemoje tyrėjas nustato nurimus parametrus, pagal kuriuos dirba sistema (profiliavimas, namų direktorijos, apsaugos funkcija, kurios atitinka galimam įvykiui ir kt.). Visos kitos sistemos perduoda iš įrašytų / kopijuotų duomenų informaciją į bendrą valdymo sistemą, ir vykdo jos nurodymus.

2.2. **Vartotojo skaitmeninis profiliavimo procesas**

Skaitmeninės profiliavimo procesas, kuris buvo sukurtas šiam tyrimui apima šešių etapų ciklą:

nustatyti tikslą: ko ieškoti, susijusių su rūšies problema;

renka ir vertina tikslinius duomenis iš atminties (failų sistemoje palikti įrašai), kuriuose yra naudingos informacijos;

atrenka susijusią informaciją bei ištraukia rodiklius (indikatorius) kiekvieno analizuojamo srityje;

informacijos atitikimo duomenys (rodikliai), siekiant nustatyti trūkumus, neatitikimus ar panašumus;

indikatorių kolekcija palyginimui ar sukūrimui "skaitmeninio profilio";

profilio analizė, palyginta su pradiniu tikslo.

2.2.1. Kompiuterinės sistemos elektroninių pėdsakų aptikimo sritys

Ši dalis numato pagrindinės sritys, iš kurių būtų galima išgauti naudingos rodiklius ir skaitmeninio profilio projektui parengti. Kad būtų paprasčiau, čia jis bus valdomas tyrimas, kuriam kompiuteris yra naudojamas su "Apple OS X" operacine sistema (OS).

Vartotojų analizė

OS diegimas įrašytas į registro failą, kuriame yra data įrenginio, vartotojo vardai / organizacija ir serijos numerius. Iš šio failo galima gauti informaciją apie vartotojus, kurie turi prieigą prie kompiuterio, pavyzdžiui, datą montavimas, atitikčių skaičių, paskutinį prieigos, paskutinis slaptažodžių keitimas ir t.t. [24] ..

Tekstinių bylų analizė

Kiekvienas turi savo kūrybos stilių, naudojant specifines idiomas (tarmes), tos pačios klaidos sintaksės ar gramatikos, rašybos, kad yra vadinamieji "parašų", kad atskirti jį.

Asmens aplankų analizė

Vartotojas naudoja tų pačių kolekcijų muzikos ar nuotraukų aplankalus, dažnai pervardina juos į aplanką su tuo pačiu pavadinimu, dažnai dedamas į tą pačią poziciją.

Aplankų organizavimo analizė

Vartotojo naudoja pakartotinai tą patį modelį failų ir aplankų organizavimui, kad būtų greičiau susigrąžinti ar surasti, ypač kai jis nori perkelti failus iš vieno kompiuterio į kitą.

Slapyvardžio analizė

Slapyvardis naudojamas prieigai prie momentinių pranešimų (IM), dienoraščių, forumų, socialinių tinklų, be to, galima naudoti e-pašto adresus. Jei kartojamas įvairių prietaisų gali būti lengvai atpažįstamas.

Log failų analizę ir susijungimų istoriją

Įprasta naršyti konkrečias svetaines, pavyzdžiui, forumai, interneto paštas, FTP jungtis, reikalauja vartotojo paskyros, dažnai “gaminamos” iš to pačio prisijungimo vartotojo vardo ir slaptažodžio. Visi šie duomenys yra aptinkami ir atpažįstami, kai kartojami įvairiuose vietose [25].

Aparatūros įrenginių analizė

Naudotojas, kuris naudoja daugiau nei kompiuterio, dažnai naudojamas norint prisijungti prie jų tuos pačius įrenginius: USB raktai, mobilieji telefonai, fotoaparatai, MP3 grotuvai ir pan. Tai galima rasti įrodymų nagrinėjant primontavimo failą visų šių įrenginių ir palyginkite pavadinimus, serijinius numerius ir t.t. ..

Programinės įrangos įdiegimo analizė

Kalbant apie techninę įrangą, vartotojas, kuris naudoja daugiau nei vieną kompiuterį, dažnai gauna tą pačią programinę įrangą, kuri palieka daugiau įrodymų (pavadinimas, versija, serijos numeris) failuose.

Programinio kodo sąrašų analizė

Kiekvienas programuotojas turi savo asmeninį stilių: iš funkcijų, kad jis geriausiai žino, pasirinkimas, ir kokiu būdu jis juos naudoti, nepamirštant savo pastabas į kodo antraštes. Rūšiuoti, kad atskirti kiekvieną programuotoją iš kitų.

Iš gautos analizės taip pat galima gauti informaciją apie žinių ir įgūdžių vartotojo kompiuterį (pvz., programavimo įrankiai, daugeliu operacinių sistemų, virtualių mašinų ir t.t. ..) būvimą.

Dėl tvarkaraščio analizė

Tvarkaraštis suteikti naudingos informacijos apie datą ir laiką (net laiko trukmę). Šie registrai yra svarbus nustatinėjant informacijos apie kompiuterio laiką: įjungimas ir išjungimas. Jie, taip pat, naudinga žinoti apie failus / aplankus operacijų, interneto prieigos ir el. paštą, ir t.t. ..

- virtualioje mašinoje analizė
- “modus operandi" (kažko darymo) analizė

Norėdami grįžti ar kartoti, pavyzdžiui, kai kurių elektroninių nusikaltimų (pvz., sukčiavimo apsimetant atakos - serveriuose - ir t.t. ..) nusikaltėlių tapatybę, tai yra naudinga, kad rekonstrukcijos ir atlikti analizę modus operandi. Norėdami tai padaryti, ši informacija gali būti gaunama iš duomenų analizės [26]:

- atakos tikslas (sukčiavimo, nustoja teikti paslaugą, politinė ataka ir pan.);
- priemonės ir metodai, naudojami įsilaužimo (rootkit, shells, kirminų, socialinės inžinerijos ir kt.);
- techniniai įgūdžiai, naudojami;
- galima koreliacija su priemonėmis socialinės inžinerijos;
- pasirinktas atakos laikas (diena / naktis, vidaus / pabaigos savaitės ir kt.);
- atakos trukmė, galimas dažnis (vieną arba suskaidyta į iš anksto nustatytus laiko intervalus ir pan.);
- koreliacija pasirinktu už išpuolį su išorinių įvykių metu;
- pasirinkimai aukų (Lietuvos ar užsienio vyriausybė įstaiga, bankas, komercinė organizacija ir t.t.);
- tipologija naudojama anti-ekspertizės metodai;
- laimėjimo tikslai.

2.2.2. Skaitmeninio profiliavimo metodas

Skaitmeninio Profiliavimo metodas, kuris apima tyrinėjimą, palyginant ir pripažįstant skaitmeninių profilių vartotojo priklausančius skaitmeninius prietaisus. Identifikavimas atliekamas naudojant skaitmeninio profilio paimtos informacijos iš kompiuterio tikrumo pridedant prie žinomo objekto ir profilių, paimtų iš kitų skaitmeninių prietaisų, kuriais tie nusikaltimai buvo padaryti, palyginant, bet negali būti neabejotinai siejamas su subjektu. Reikėtų pažymėti, kad principas, kuriuo grindžiama metodas, yra dvipusis, tai yra, ji taip pat gali pradėti nuo vartotojo skaitmeninės profilio "anoniminis" esančio prietaise, palyginti su profiliais kitų prietaisų (taip pat dalyvavo / nedalyvavo nusikaltimas) neabejotinai susiejamas su konkrečiais subjektais. Jis taip pat gali išgauti skaitmeninę profilį "modus operandi" (pvz., kibernetinio išpuolio) palyginti su kitais siekiant atpažinti ir identifikuoti autorius. Metodas apima šiuos žingsnius, kurie aprašyti ciklu, kuris gali būti kartojamas, kai tik gaunama nauja informacija [27]:

ekstrapoliacija skaitmeninio vartotojo (arba vartotojų) profilio, prietaisą priskiriant kaip "standartinis profilyje";

ekstrapoliacija iš vartotojų skaitmeninių prietaisų kitam analizės profiliavimui;

palyginimas profilių, gautų siekiant pabrėžti panašumus - skirtumus;

kiekybinė ir kokybinė analizė konvergenciją - skirtumų tarp profilių suteikimo ir tada identifikacijos klausimu;

2.2.3. Skaitmeninio profiliavimo proceso modelis

Modelio sukūrimas prasideda nuo informacijos, apibūdinančių rastų failus kompiuteryje. Reikėtų pažymėti, kad formuojame profilį kiekvieno vartotojo susijusio su operacine sistema, įdiegta į prietaisą, įskaitant virtualias mašinas.

Modelis aprašas[28]:

- elementai;
- profiliai;
- funkcijos ir funkcijų elementų;
- operacijų seka sukuriant skaitmeninį profilį;
- palyginimas;
- rezultatų vertinimas.

Charakteristikos ir elementų funkcijos

D - skaitmeninį įrenginys

Skaitmeninio prietaiso "D_i" yra skirtas:

- bet kokio skaitmeninio prietaiso numatytą su nuolatinės atminties gali saugoti failus. Pavyzdys: PC, Mobilus telefonas, navigacijos sistema, telefono stotys ir kt. . ;
- laikymo įtaisas, galintis saugoti duomenis. Pavyzdys: Kietasis diskas, flash kortelė, atminties kortelės, smart card, USB pen, USB HDD, CD, DVD, DAT ir t.t. ..);
- plotas atmintis, kurioje jie yra saugomi nutolusiame duomenų failams vartotojams.
- virtuali mašina, kuriame yra operacinė sistema;
- failų rinkinys apie užklausas. Pavyzdys: log failą.

f - ypatybė

Funkcija "f_i" priskirta bendrajai pagrindiniai aparatūros ar programinės įrangos funkcijai, toliau suskaidomos į daugiau elementarių analizuojami tyrimo kontekste, nes tai yra informacija, kuri apibūdina "skaitmeninę elgesį" vartotojo prietaiso. Funkcija yra kilus iš failų įrenginio viduje ir atrinktų remiantis objektyviais tyrimais. Ji gali būti sudarytas iš:

- failo ypatybes (metaduomenis, tipo);
- turinys failą (tipo informaciją).

Failas gali turėti vieną ar daugiau funkcijų: jie laikomi pagrindinėmis funkcijomis, priklausomai nuo tyrimo tikslo:

- Failo pavadinimas. (Tekstų, nuotraukų, muzikos, filmų, video, ir t.t.): pavyzdys. Tuo pačiu pavadinimu sukurti asmeniniai failai įvairiuose įrenginiuose, galima daryti išvadą, kad jie buvo laikomi to paties vartotojo;
- Kelias. Pavyzdys: kai kurie failai atrodo identiški, kad ši funkcija reiškia, kad šis failas turi tą pačią vietą aplanko medį, atsižvelgiant į kitą (tą patį aplanko pavadinimą arba nustatyti katalogų);
- MD5 (ar kitas hash algoritmas) Funkcija suteikia matematinį tikrumą dėl tos pačios bylos, rastos įvairių prietaisų turinio, sutapimas;
- sukūrimo data, pakeitimas, panaikinimas. Šie trys požymiai numatyti redaguoti, trinti tuos pačius failus, kai rasti kitų prietaisų istorijose;
- Bet kokia informacija susijusi su tikslu, gali būti imtasi peržiūrėti jos turinio.

Bylos sritis

Siekiant geriau nustatyti, kaip apibrėžti prietaiso Di failai, kurie gali turėti išsaugojimo ypatybių, jie buvo suskirstyti pagal rūšis konkrečiose srityse, apibrėžiama kaip Ai (Di)

$$U_i \, A_i(D_i) \subset D_i \qquad (1)$$

Tai tada apibrėžia Ai(Di), kaip vienalyti pogrupyje Di, kuriame, suskirstyti pagal tipą, visi failai, kuriuose gali būti ypatybės, palyginant su prietaisu Di.

Klasifikavimas sričių failo A

Kiekvienas įrenginys turi savo konkrečią klasifikaciją, kur yra funkcijų, atsižvelgiančių jo specifinį pobūdį ir įdiegtas programas. Čia randame bendrą klasifikaciją pagrindinių sričių, susijusių su asmeniniu kompiuteriu. Tyrimų ypatybių skaičius sritis yra lanksti, nes ji priklauso nuo tyrimų ir programinės įrangos prietaise [29].

A_1 - Registry File: sistemos vartotojai.

A2 - Registry File: aparatūros įrenginių.

A3 - Registry File: programinės įrangos įrenginių.

A(4) asmens bylų sritys: čia yra laikomi "asmens byla" visi tie failai saugomi vartotojo prietaise išorės įdiegtų programų, ir kuri gali būti pateikiama informacija, apibūdinanti kaip "skaitmeninį elgesį". Funkcija gali būti gaunama iš aprašančių metaduomenų rinkmenų. Asmens bylų srityje buvo suskirstyta pagal tipą failo sekančiose kategorijose: A4 - tekstinių failų asmens Tekstiniai failai, parašytų vartotojas rankos (DOC, DOCX, TXT, RTF, ODT, PDF, XLS, ir t.t. ..). Atskleisti rašymo stilių. Jų analizė gali išryškinti keletą funkcijų. Be informacijos, kuri gali suteikti per metaduomenų analizę, kitų funkcijų, gali būti nustatyta:

- parašas;
- slapyvardis;
- tinkamas pavadinimas;
- slaptažodžio prieiti;
- idioma;
- rašybos;
- spausdinimo klaidų;
- nuoroda į konkretų įvykį;
- nuoroda į konkretaus asmens;
- nuoroda į tam tikrą objektą;
- nuoroda į vietą;
- ypatingą frazę;
- elektroninio pašto adresas;
- ir t.t.

A5 - asmeninis elektroninio pašto laiškai (išskyrus biuletenius, reklamos ir pan.)

A6 - Pokalbiai.

A7 - Vaizdai ((BMP, JPG, TIF, ir kt.)

Jie ypač mokėtiną atsižvelgiant į padarytų nuotraukų iš kameros, mobilieji telefonai ir tt.

A8 - Grafikos vaizdai (JPG, TIF, DWG ir pan.)

Pavyzdžiui, kolekcijos grafinių vaizdų, pavyzdžiui, DVD viršelių, CD, teminių kolekcijų nuotraukas, meno, komiksų, ir t.t. ..

A9 - (.. MPG, AVI ir t.t.) Filmai video

Filmai, pagaminti iš vaizdo kamerų, mobiliųjų telefonų ir tt .. yra daugiausia svarbus.

A10 - Garso failai (WAV, MP3 ir pan.)

Garso failų, saugomų vartotojas kolekcijos ypač mokėtiną.

A_{11} - URL

F ypatybių suformavimo galimybė

Nuo įvairių sričių analizę, jis surinko pagrindinių ypatybių rinkinį. Kaip nustatyti požymis F, tačiau tai ketina visų analizuotų skaitmeninių prietaisų, atskirų savybių rinkinį.

$$F = \{f_1(A_i)(D_i), f_2(A_i)(D_i),... f_n(A_i)\ (D_i)\}$$

M-minimalus ypatybių galimybė

Kai iš svarbiausių ypatybių nuimamas nuo prietaiso komplektą fiksuota, ji turi būti sumažinta iki ypatybės faktiškai esančius nagrinėjamo įrenginio, atsižvelgiant į konkrečius reikalavimus, atliekant tyrimą. Veiksmas atliekamas remiantis pirminės atrankos ypatybių, konkrečiam prietaisui, apriboti skaičių siekiant suformuoti minimalų ypatybių rinkinį.

"Mi" atitinka ypatybių, kurios priklauso visų pagrindinių ypatybių, parinktų atsižvelgiant į konkretų tyrimą.

$$m_i(A_i)(D_i) \in F(D_i) \qquad (2)$$

Todėl tapatybių minimalus yra išreiškiamas:
$m_i(A_i)(D_i)$, kai:

m_i - įvardytos minimalios ypatybės;

A_i – identifikuoja falą priklausanti imties šaltiniui;

D_i - identifikuoja skaitmeninį prietaisą, iš kurio ji buvo išgauti.

M - minimalus ypatybių rinkinys

Jis apibrėžiamas kaip minimalus rinkinys iš S(Di) poaibio dydis, bet jau atsižvelgiant į konkretaus atvejo, tyrimas.

$$M(D_i) \in F(D_i) \quad (3)$$

$$M(D_i) = \{m_1(A_i)(D_i), m_2(A_i)(D_i), \ldots m_n(A_i)(D_i)\}$$

Ypatybių rinkinys yra minimalus - filtrais būti taikomoms byloms, kurios charakteristikos informacija (rodikliai), bus taikomi sudaryti skaitmeninį profilį.

Indikatorius

Rodikliai (indikatoriai) yra renkami ir analizuojami tyrimo kontekste - profiliavimo tikslais, bendra ypatinga informacija. Jie gaunami iš failų atrinktų būtiniausių taikymo filtrų, skaitmeninį profilį sukurti, operacijos metu. Tai apibrėžiama kaip $i_i(l_i)(A_i)(D_i)$. Kuris apibrėžia naudojant informaciją, kaip filtrų (failų kolekcija). Ypatybė minimum m_i yra konkrečioje srityje (Ai) specifinio prietaiso (Di) . (Ii) nustato failą, iš kurio rodiklis ištrauktas.

Rodiklis - iš tikrųjų, skaitmeninių įrodymų. Toks gali būti:

- aptikti;
- palyginti;
- pripažinti.

I - nustatyti Indikatorių

Tai apibrėžiama, kaip indikatorių I (Di) rinkinys:

$$I(D_i) = \{i_1(l_i)(A_i)(D_i), i_2(l_i)(A_i)(D_i) \ldots i_n(l_i)(A_i)(D_i)\}$$

Indikatorių, kurie apibūdina visą informaciją, rinkinys yra renkami iš bylų.
Jame aprašoma "skaitmeninis elgesys" vartotojo kuriam priklauso įrenginys.

k - failas, kuriame Indikatoriai

$k_i(A_i)(D_i)$ unikaliai identifikuoja kiekvieną failą, kuriame yra vienas ar daugiau indikatorių, kai:

- (Ai) identifikuoja imtį, kurioje galite rasti failą;
- (Di) identifikuoja įrenginį.

Failas, kuriame yra vienas ar daugiau rodiklių yra "šaltiniu skaitmeniniams įrodymams", patvirtinantis šaltinį, todėl yra naudinga išgauti iš jo informaciją

K - failų rinkinys, kuriuose yra Indikatoriai

K (Di) apibrėžia failų, kuriuose yra informacijos, susijusios su konkrečiu įrenginiu (Di) rinkinys.

$$K(D_i) = \{k_1(A_i)(D_i), k_2(A_i)(D_i) \dots k_n(A_i)(D_i)\}$$

Naudinga veiksmų seka skaitmeninio profilio sukūrimo

Operacijų seka yra tokia ekstrapoliacija penkių profilių iš kompiuterio:

- profilis gaunamas iš failus;
- profilis gauta iš naudotojo aplanko failus;
- profilį gaunamas iš likusių sričių atminties failus.

Iš šių veiksmų yra:

- vartotojo aprašymas, kurį sudaro jų vientisumą;
- aprašymo pavyzdys, kuris sutampa su vartotojo profiliu, bet nurodo prietaiso pasirinkto, kaip "pavyzdžio" palyginus su kitais.

Iš pavyzdinio profilio veiksmų yra sudarytas:

- indikatoriai arba informacija, apibūdinanti būti naudojama norint palyginti su kitų profilių vartotojo identifikacijai;
- failai, kuriuose yra tokių bandymų.

Turint omenyje, kad kompiuteris gali aptikti daugelio vartotojų buvimą, pateikiamas paaiškinimas metodo, pristato skaitmeninės profilio asmeninio kompiuterio pridedamas prie vieno vartotojo, atsižvelgiant į "Windows 7" operacinės sistemos pavyzdį (default install) ar „debesyje instaliuotą sistemą [30].

Ps - profilio sistemos

Atskaitos taškas yra žurnalo failų (A_1 sritis), pateikia visą informaciją (indikatoriai) apie vartotoją, mašinos konfigūracija. Jie sudarys sistemos aprašymą Psi (Di), kurioje (Di) identifikuoja tam tikrą įrenginį.

$$Ps_i(D_i) = I(Ps_i)(D_i)\ (S_i) \cup K(Ps_i)(D_i) \qquad (4)$$

Kur surinktų nuo failus indikatorių rinkinys yra vadinamas $I(Ps_i)(D_i)(S_i)$, kai:

I - identifikuoja visus indikatorius išmatuoti;

Psi - identifikuoja tam tikrą sistemos profilį;

Di - identifikuoja tam tikrą įrenginį;

Si – identifikuoja tam tikrą socialinių tinklų profilį.

failų rinkinys, kuris yra jų vadinamas $K(Ps_i)(D_i)(S_i)$, kai:

K - identifikuoja failus, rinkinys;

Psi - identifikuoja tam tikrą sistemos profilis;

Di - identifikuoja tam tikrą įrenginį.

Si – identifikuoja tam tikrą socialinių tinklų profilį, kai:

1. kiekvienas indikatorius sudaro vienetinį informacijos gabalą, kuris labiau nesiskaido;
2. kiekvienas indikatorius reiškia vieną ar daugiau failų;

3. kiekvienas profilis gali sudaryti vienas ar keli socialinių tinklų profiliai;
4. kiekvienas failas gali būti vienas arba daugiau indikatorių.

PC - Vartotojo Namų aplanko profilis

Antrasis žingsnis yra saugomų failų aplankus sukurtų bet kuriam vartotojui operacinės sistemos analizė. Iš tiesų, jie yra labiausiai "asmeninai" failai padaryti vartotojui. Šis veiksmas sukuria profilį vadinami Pc(Di) (vartotojo aplanko aprašymą), remiantis bylų analizės aplanką, sukurtą prietaise (Di) vartotoju operacinės sistemos. Yra kiekvienam rasti kompiuterio atminties vartotojui aplankas. (pvz., kompiuterio : /Users/SG/ ...) Jei yra kelios operacinės sistemos (įskaitant OS esančios virtualios mašinos), kiekvienas iš jų turėtų būti laikomas atskiru įrenginiu. Įkalčiams naudosim atviro kodo programinę įrangą [31].

Vartotojo aplankas profilis Pci (Di) yra apibrėžiama taip:

$$Pc_i(D_i) = I(Pc_i)(D_i) \cup K(Pc_i)(D_i) \quad (5)$$

, kur:

• I (Pci) (Di) yra pagal failų surinktų indikatoriai, savo vartotojo katalogą, jeigu:
- Ii - identifikuoja surinktų indikatorių rinkinį;
- Pci - identifikuoja vartotojo aplanko profilį;
- Di - identifikuoja įrenginį.

• K (Pci) (Di) yra failų rinkinys, kuriame yra indikatorius, kuriame:
- K - identifikuoja failus, rinkinys;
- Pci - identifikuoja vartotojo aplanko profilį;
- Di - identifikuoja įrenginį.

, kai:

• kiekvienas indikatorius susideda iš vieno gabalo informacija toliau suskaidomos;
• kiekvienas indikatorius reiškia vieną ar daugiau failų;
• kiekvienas failas gali būti vienas arba daugiau indikatorių.

Pd - Įrenginio profilis

Iš vartotojo aplanko profilio sukūrimo nepakanka apibrėžti visą profilį vartotojo kompiuterio, nes kitos savybės gali būti nustatytos iš failų, saugomų teritorijų, kurios nėra įtrauktos į bendruosius naudotojus aplankus. Įrenginio profilis apima tuos failus, kurie yra pavyzdžiui padėti į katalogus kitų skirsnių (diskų), papildomi kietieji diskai, taip pat įskaitant “deallocated” failai ir tt .. antrasis ratas bus baigtas, kai minimalaus skirtųjų funkcijų naudojimu siekiama pabrėžti visus funkcijai priklausančius failus, saugomus už vartotojų katalogo ribų. Įrenginio Profilis Pdi (Di) yra apibrėžiama taip:

$$Pd_i(D_i) = I(Pd_i)(D_i) \cup K(Pd_i)(D_i) \quad (6)$$

Kur indikatorių rinkinys sudarytas iš failų, esančių vartotojo aplanką, vadinamas Ii(Pdi) (Di), kai Pdi - nustatyti prietaiso profilį:

- I - identifikuoja visus nustatytus indikatorius;
- Pdi- nustatyti prietaiso profilį;
- Di - identifikuoja įrenginį.
- visas failas, kuriame jie vadinami Ki (Pdi) (Di), kai:
- K - identifikuoja failus, rinkinys;
- Pdi - identifikuoja įrenginį profilį;
- Di - identifikuoja įrenginį.

, kai:

kiekvienas indikatorius susideda iš vieno gabalo informacija toliau suskaidomos;

kiekvienas indikatorius reiškia vieną ar daugiau failų;
kiekvienas failas gali būti vienas arba daugiau indikatorių.

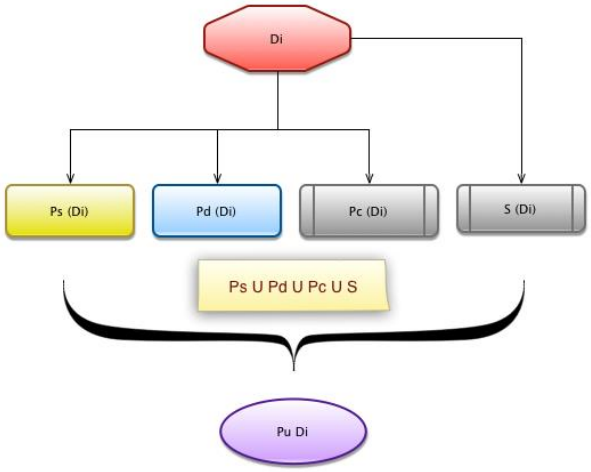
Pu-Vartotojo profilis

Iki šiol nagrinėti profiliai (žr. 2.2 pav.) sudaryti iš visų elementų, reikalingų sukurti vartotojo aprašymą vadinama Pu(Di). Tai skaitmeninis elgesio modelis, kuris apibūdina vartotojo sąveiką su skaitmeniniu prietaisu pagal technine analize. Todėl jis yra sudarytas iš:

1. visi apibūdinantys informacija (indikatoriai), kurie pripažįstami visos mašinos analizės metu.
2. visi failai, kuriuose yra jiems;
3. visi socialinių tinklų profiliai.

Vartotojo aprašymą Pu(Di) tada apibrėžiam:

$$Pu(D_i) = I(Pu)(D_i))(S_i) \cup K(Pu)(D_i) \quad (7)$$



2.2 pav. Skaitmeninio pėdsako ir įpročio koreliacijos algoritmas

kur I (Pu) (Di) – išvesta iš keturių rodiklių indikatorių pranešimų:

$$I(Ps)(D_i) \cup I(Pc)(D_i) \cup I(Pd)(D_i) \cup (S_i) \quad (8)$$

K (Pu) (Di) - išvesta iš keturių rinkmenų:

$$K(Ps)(D_i) \cup K(Pc)(D_i) \cup K(Pd)(D_i) \cup K(S_i) \quad (9)$$

, kurioje
Socialinis vartotojo profilis

$$S = I(Pd_i)(D_i) \cup K(Pd_i)(S_i) \quad (10)$$

- I - identifikuoja visus nustatytus indikatorius;
- Pdi- nustatyti prietaiso, kuriuo buvo naudotasi socialiniai tinklais, profilį;
- Di - identifikuoja įrenginį.
- visas failas, kuriame jie vadinami Ki (Pdi) (Di), kai:
- K - identifikuoja failus, rinkinys;
- Pdi - identifikuoja įrenginį profilį;
- Si - identifikuoja socialinių tinklų (-o) profilį.

Puc - Pavyzdinis Vartotojo profilis

Pavyzdinis vartotojo aprašymą Puc(Di) sutampa su vartotojo profilio Pu(Di), kuris skiriasi tik pagal apibrėžimą, nes jis yra nustatytas kaip palyginti su kitais prietaisais etalonas.

Tiesą sakant, surinkti indikatoriai bus naudojami kaip filtrai ieškoti informacijos per sutampančių prisiminimų kitų prietaisų.

Palyginimas

Kai pavyzdys profilis Puc(D1) gaunamas iš vieno įrenginio, surinkti rodikliai naudojami kaip filtrai už patį aptikti kitus prietaisus, nustatyti ryšius ir / ar skirtumus.

Kryžminis palyginimas

Žingsnį sudaro: visa surinkta informacija apie kiekvieną prietaiso analizę. Jos įgyvendinimas apima šiuos veiksmus:

(1) ekstrapoliacija mėginio vartotojų profilius Puc visų prietaisų analizės, kurių kiekvienas susideda iš trijų indikatorių rinkinių:

$I(Ps)(D_i) \cup I(Pc)(D_i) \cup I(Pd)(D_i)$;

ir trijose failai: $K(Ps)(D_i) \cup K(Pc)(D_i) \cup K(Pd)(D_i)$

(2) ekstrakcija ir taikymas:

- nustatyti indikatorių I (Pu) (Di) ir jo failai K (Pu) (Di) iš kiekvieno profilio;
- kiekvienas filtrų sudarytas iš indikatorių I (Pu) (Di) į kiekvieną prietaisų rinkinys.

(3) atnaujinti atskirus profilius į naujus nustatytus indikatorius.

Procedūra gali būti naudinga tais atvejais, kai gaunamas iš vieno įrenginio analizės informacija nėra labai svarbi, nes ji leidžia:

(1) išnagrinėja visus prietaisus duomenis;

(2) padidinti indikatorių gautų skaičių;

(3) atlikti vartotojo profiliai nuosekliau.

Ji taip pat leidžia nustatyti bet kokią papildomą vartotoją.

"Multi-User įrenginiai

Sudėtingesnis atvejis gali atsirasti, jei tame pačiame įrenginyje Di naudojasi daugiau nei vienas žmogus (pvz., asmeninis kompiuteris).

Kiekvienam vartotojui profilis turi būti ekstrapoliuoti, pagal šias taisykles:

(1) sukurti vartotojo aprašymą kompiuterio kiekvienam vartotojui (t.y. PC1, PC2, ir t.t.) Vienas vartotojo aplankas kompiuteryje;

(2) sukurti sistemą aprašymą Ps kiekvienam vartotojui (pvz., PS1, PS2, ir kt.);

(3) kurti unikalų prietaiso aprašymą Pd;

(4) skerspjūvio palyginti kiekviename kompiuteryje ir PD profilius, kad gamina vieną Pu profilio kiekvieną aptiktą vartotojui;

(5) kiekvieno vartotojo aprašymą Pui (Di) apibrėžiama kaip:

$$Pu_i(D_i) = Pc_i(D_i) \cup Pd(Pc_1)(D_i) \cup Ps(Pc_1)(D_i) \quad (11)$$

Palyginti tarp kito vartotojo aplanką profilius kompiuterio ir prietaiso aprašymą Pd, skirtos:

(1) nustatyti savo indikatorius komplektacijoje prietaiso profilio srityse;

(2) išskleisti failus, kuriuose jų yra, ir įtraukti juos į santykinio PdU, kur PdU reiškia vartotojo įrenginio profilį, Pd poaibį, kurią sudaro:

(i) indikatorius, bendra su kompiuteriu;

(ii) visi failai, kuriuose yra jiems.

(3) sukurti daug profilių Pui (Di), kiek yra vartotojų aplankai (tuščias), susidedanti iš:

$Pc_i(D_i) \cup Pdu_i(Pc_i)(D_i) \cup Ps_i(D_i)$

(4) sumažinti PD profilį, kuris galiausiai bus sudarytas iš šių indikatorių (ir susijusių failų) nėra įtrauktos į įvairių vartotojų profilių dydį.

(1) n vartotojų profiliai - tipiška informacijos, kuria aprašomas skaitmeninių vartotojams rasti mašiną elgesį, iš nustatytų ribų;

(2) nr. 1 anoniminis planšetinio įrenginio profilis (jei toks yra) - tai yra informacija, apibūdinančių nėra susijusi su tų vartotojų, kurie taip pat apima, kad informacija apie konfigūruotą sistemą, rinkinys.

Šis paskutinis profilis nebus ištrintas, bet yra galimybė tirti kaip anoniminį profilį, nes jame pateikiama informacija, gali būti naudinga kitų subjektų identifikavimo, palyginti su kitais prietaisais vėlesnei analizei.

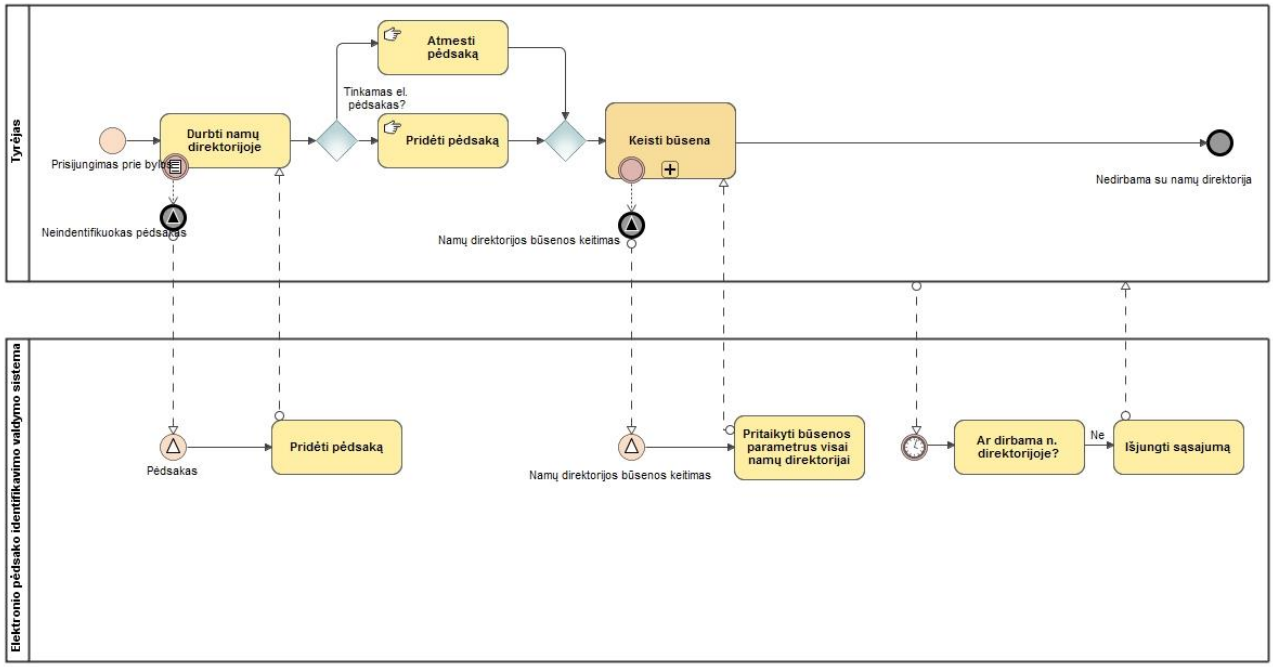
2.2.4. Elektroninio pėdsako indentifikavimo sistemos valdymo procesų modeliavimas

Pateikiami būsimi elektroninio pėdsako indentifikavimo sistemos valdymo procesų modeliai. Panašius modelius jau naudoja Valstybinės institucijos [32].

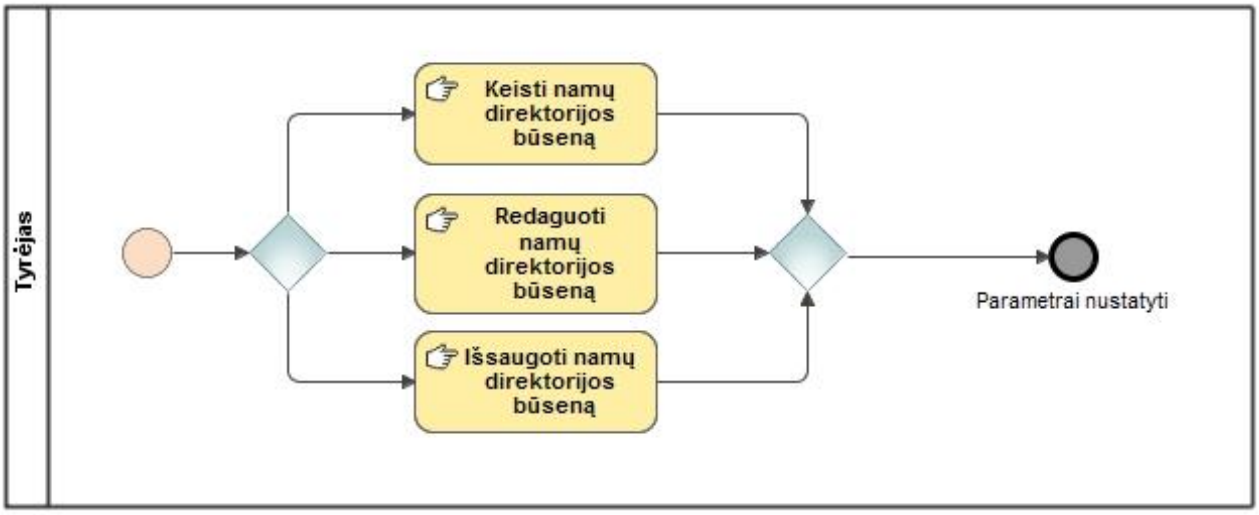
Namų direktorijos procesų modelis

Tyrėjui pradėjus elektroninio pėdsako (ar įrodymą, ar įprotį įtariamojo namų direktorijoje žr. 2.3 pav.) identifikavimo tyrimą, kuris patalpinamas į informacijos kopijavimo ar peržiūrėjimo sistemą, galima pačiam pridėti jį (objektyvios tyrimo priežastys) arba sistema pati nustato reikalingas jis ar ne (subjektyvios priežastys). Jei pėdsakas reikalingas, jis pridedamas prie tyrimo. Tyrėjui norit namų direktorijos turini analizuoti, reikalingi skirtingi informacijos gavimo pjūviai. Juos gali būtų iš anksto užprogramavęs sistemoje. Vėliau tereikia nurodyti norimą režimą ir namų direktorijos valdymo sistema jį pritaikys (žr. 2.4 pav.).

Būvio daviklis nuolat tikrina ar tyrėjas dirba (yra) su bylos įtariamojo namų direktorija. Tyrėjui išėjus iš namų direktorijos informacijos sistema išjungia sąsajumą.



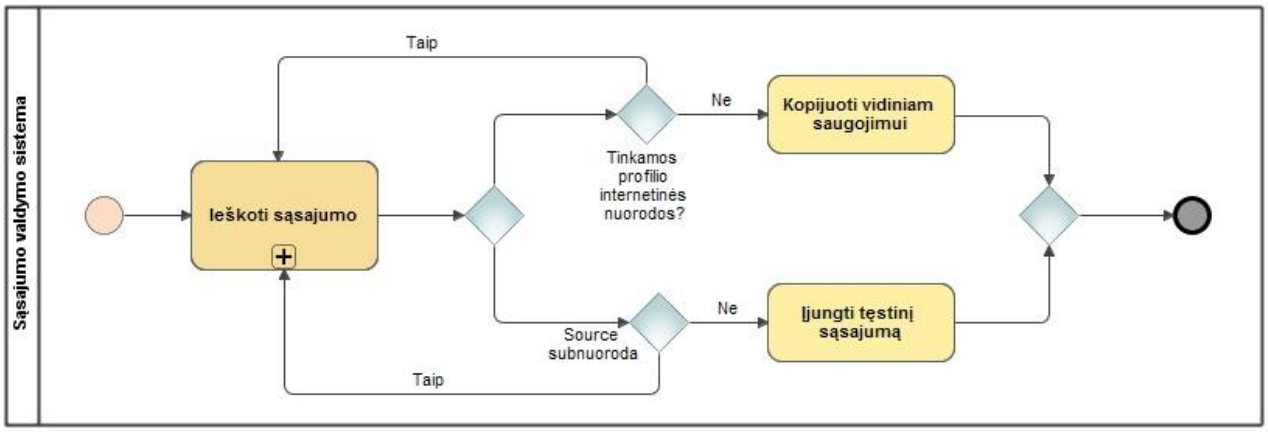
2.3 pav. Namų direktorijos sistemos procesų valdymo modelis



2.4 pav. Detalizuotas namų direktorijos būsenos keitimo procesas

Informacijos sąsajumo valdymo procesų modelis

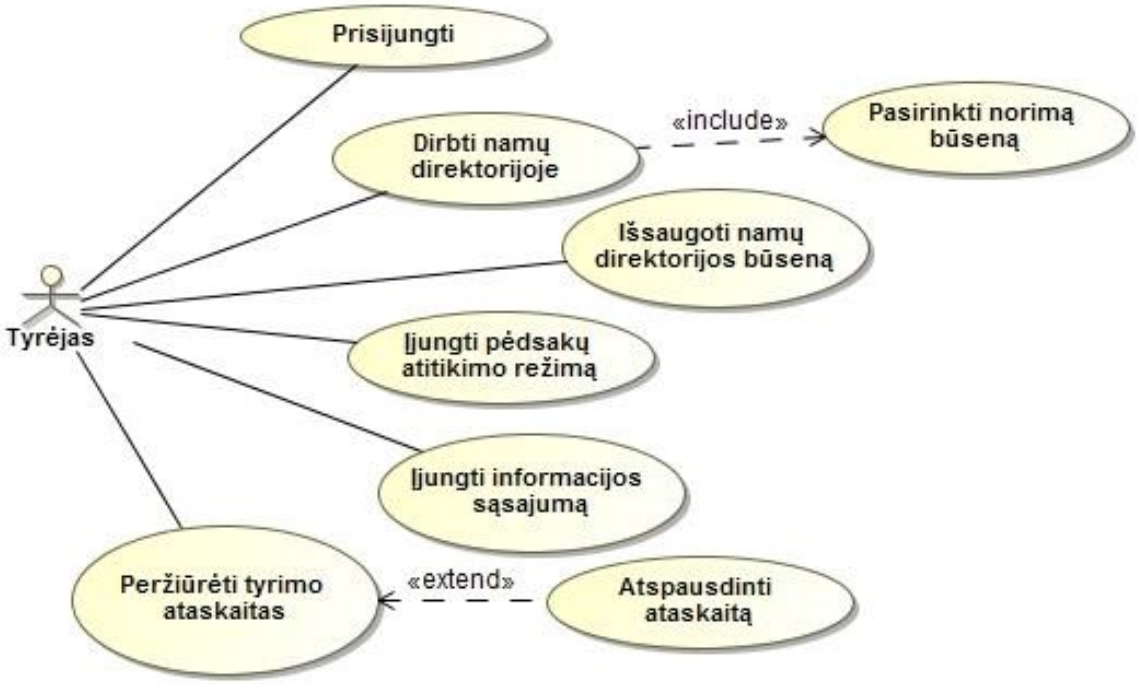
Įjungus automatinį sąsajumo valdymą (žr. 2.5), sistema nuolat tinkama profilį (įtariamojo pėdsaką) interneto nuorodose, jei profilis sutampa, kopijuojama vidiniam saugojimui, priešingu atveju įjungimas markeris (indeksuojamas, kaip patikrintas nesusijos šaltinis). Taip pat tikrinamos internetinės išeities tekstas (source), jei source yra subnuoroda, įjungiamas tęstinis sąsajumas.



2.5 pav. Sąsajumo valdymo sistemos procesų modelis

Vartotojo reikalavimo modelis

Pateikiamas elektroninio pėdsako indentifikavimo valdymo sistemos vartotojo reikalavimų modelis 2.6 pav. bei pateiktos specifikacijos lentelės.



2.6 pav. Elektroninio pėdsako identifikavimo valdymo sistemos reikalavimų modelis

2.1 lentelė panaudos atvejo „įjungti pėdsakų atitikimo“ specifikacija

PA „Įjungti pėdsakų atitikimo režimą“.		
Tikslas: Sistema be vartotojo (tyrėjo) įsikišimo daro paiešką (elektroniniai šaltiniai).		
Aprašymas: Vartotojas (tyrėjas) prisijungęs prie sistemos gali peržiūrėti paieškoje vykstančius procesus ir esamą situaciją. Matoma indeksavimo statistika, data/laikas kada pridėta nuoroda vidiniam saugojimui, subdirektorijų paieško rezultatas. Gali pakoreguoti nustatymus. Matomas socialinių tinklų ir įtariamojo sąsaja - medis.		
Prieš sąlyga:		Vartotojas privalo prisijungti prie sistemos.
Sužadinimo sąlyga:		Vartotojas pasirenka sąsajumo valdymą.
Aktorius:		Tyrėjas.
Susiję PA	**Išplečiantys PA**	Koreguoti nustatymus.
	Apimami PA	-
	Specializuoti PA	Gauti siūlomus nustatymus (automatizuota koreliacija).
Pagrindinis įvykių srautas		**Sistemos reakcija**
1. Vartotojas pasirenka sąsajumo valdymą		1.1 Tikrinama profilio nuorodos internete, išeities tekstus ir kt.
2. Vartotojas įjungia sąsajumo priežiūrą.		2.1 Sistema autonomiškai tikrina sąsajumą.
Po sąlygos:		Sistema autonomiškai tikrina sąsajumą.
Alternatyvūs scenarijai		

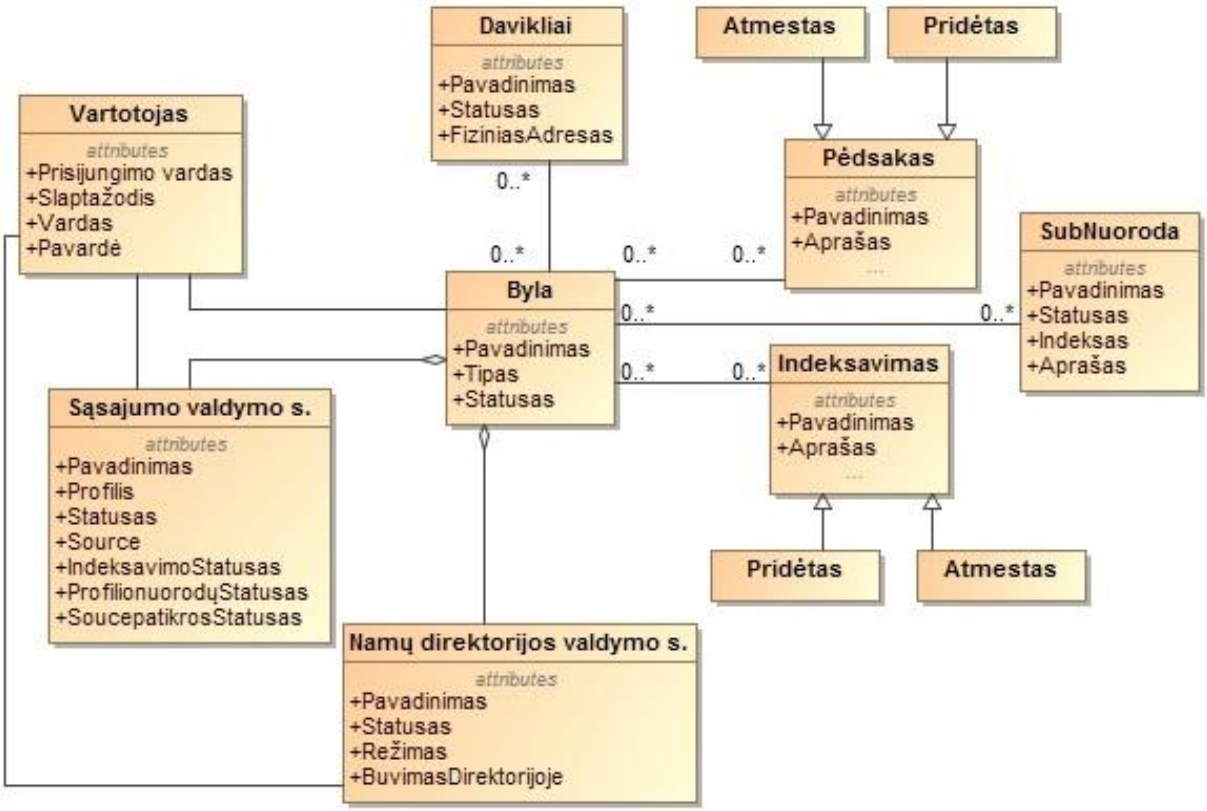
Siūlomos rekomendacijos pagal indeksavimo nustatymus (automatizuota koreliacija).	Vartotojui parodomas langas su siūlomais nustatymais

2.2 lentelė panaudos atvejo „Namų direktorijos“ įkalčių sąsajumo specifikacija

PA „Namų direktorijos“.		
Tikslas: Tyrėjui radėjus dirbti įtariamojo namų direktorijoje, pridėti rastą pėdsaką, pritaikyti norimą režimą		
Aprašymas: Vartotojui prisijungus prie bylos ir aptikus pėdsaką, jis yra pridedamas į bylą. Vartotojui pakeitus sąsajumo būseną, sistema perjungia sąsajumo paiešką.		
Prieš sąlyga:		-
Sužadinimo sąlyga:		Vartotojas įeina į bylą (namų direktoriją)
Aktorius:		Tyrėjas.
Susiję PA	**Išplečiantys PA**	Iš anksto išsaugoti režimai.
	Apimami PA	-
	Specializuoti PA	-
Pagrindinis įvykių srautas		**Sistemos reakcija**
1. Būvio tikrinimas		1.1 Tikrinama ar tyrėjas dirba su byloje esančia įtariamojo namų direktorija.
2. Tyrėjas byloje		2.1 Įjungiamas sąsajumas.
3. Keičiama sąsajumo būsena		3.1 Perjungiamas sąsajumas
4. Tyrėjas baigė darbą		4.1 Išjungiamas sąsajumas.
Po sąlygos:		Sąsajumas išjungtas
Alternatyvūs scenarijai		
2.2 Bylos darbo metu (atidaryta byla) sąsajumas neįjungiamas.		2.2.1 Read-only režimas.

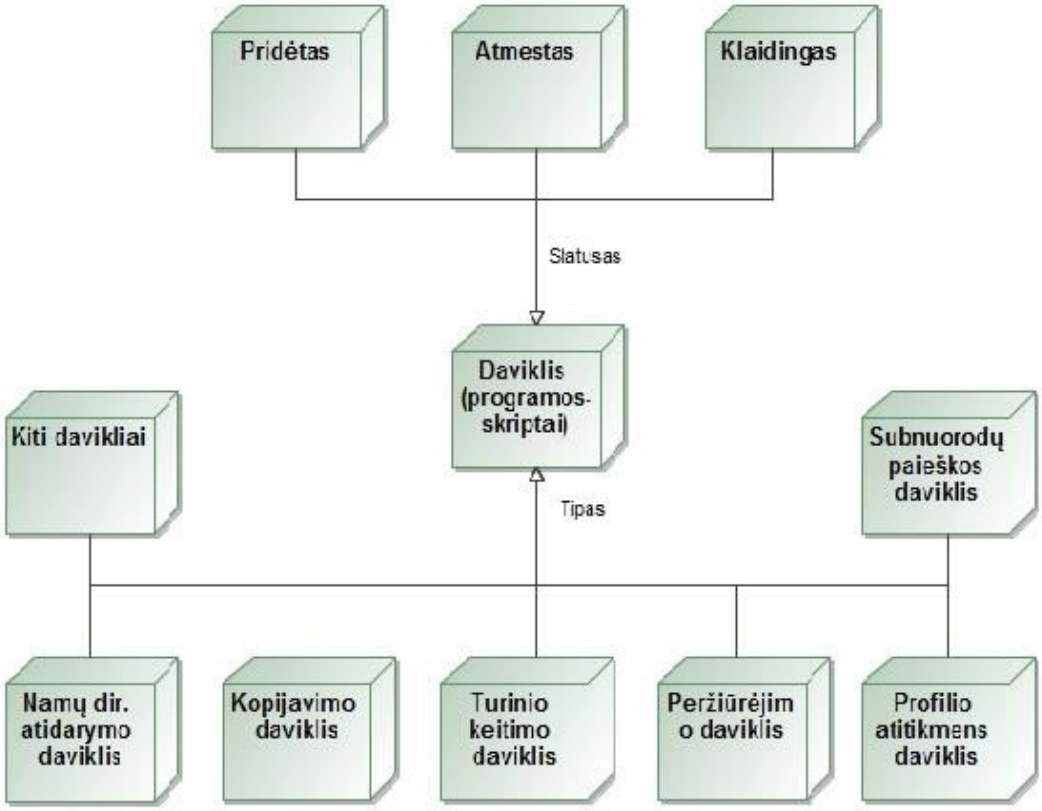
Koncepcinis duomenų modelis

Koncepcinis duomenų modelis pateiktas paveikslėlyje 2.7 pav. Duomenų modelyje pavaizduotas vartotojas, „namų direktorija“, valdymo sistemos, davikliai (programos-sriptai), valdomi įrenginiai.



2.7 pav. Elektroninio pėdsako identifikavimo valdymo sistemos koncepcinis duomenų modelis

Modelyje matome, kad vartotojas mato jam priskirtas bylas. Byla gali turėtų daug vartotojų. Byloje gali būti daug daviklių – indikatorių (žr. 2.8 pav.) (automatinės programos-scriptai), kurie renką informaciją ir ją perduoda į valdymo sistemą. Pagal surinktus duomenis vykdomos numatytos funkcijos, pvz., jei tyrėjas įėjo į namų direktoriją ir keičia turinį tada sistema įjungia sąsajumą, jei indeksuojamas profilis atitikimo internetinį šaltinį tada įjungiamas indeksavimas ir subnuorodų paieška.

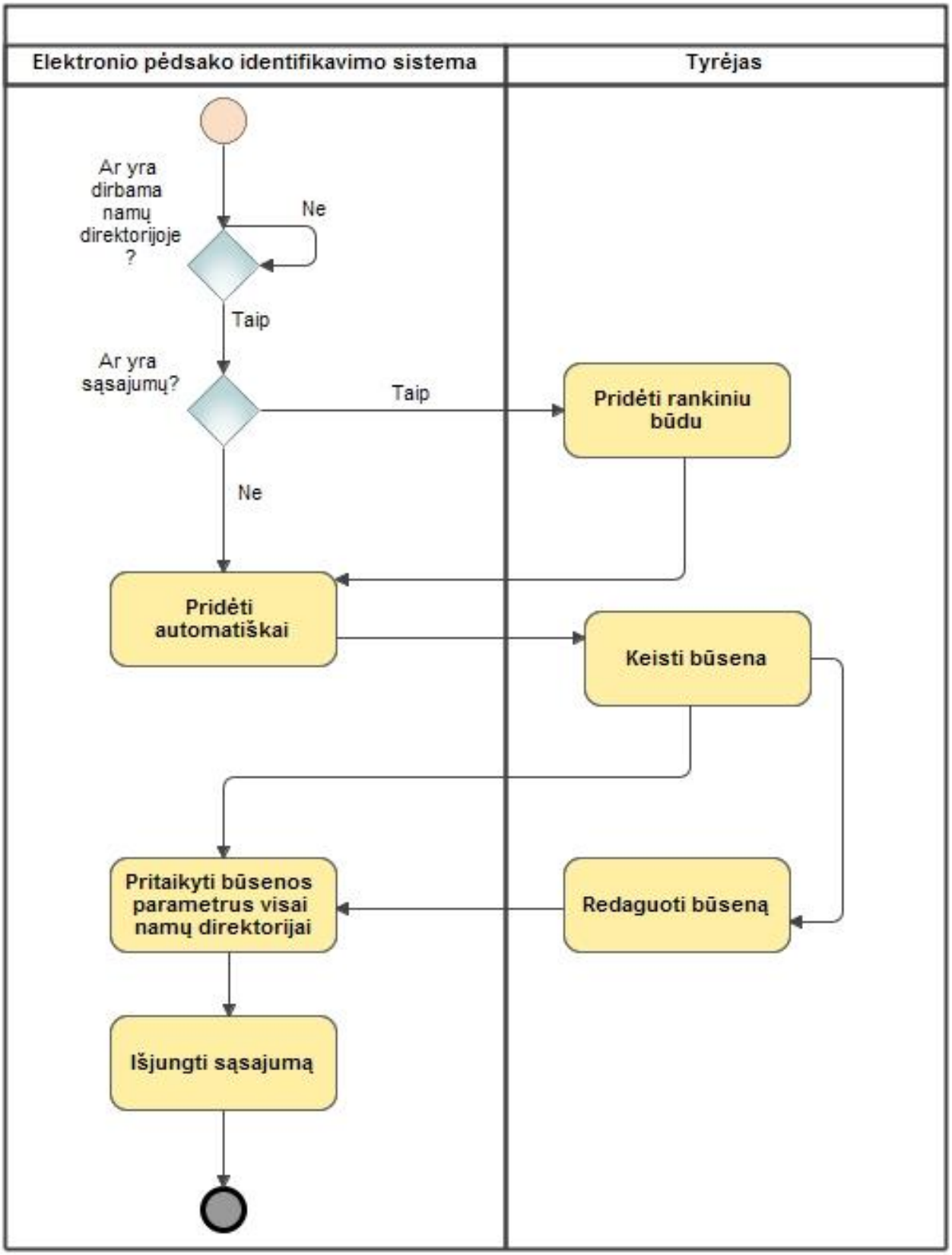


2.8 pav. Indikatoriaus koncepcinio duomenų modelio detalizavimas

Duomenų esybės „elektroninio pėdsako“ būsenų valdymas

Elektroninio pėdsako valdymo duomenų esybės būsenų diagrama pateikta 2.9 pav., ji turi 4 būsenas.

Pirmojoje būsenoje duomenų esybė užfiksuoja tyrėją, kuris įėjo į bylos namų direktoriją. Tada sistema patikrina sąsajumą. Jei byloje yra pėdsakų įjungiamas sąsajumas, kitu atveju neįjungiamas, tačiau paliekama galimybė tyrėjui rankiniu būdu įsijungti sąsajumą.

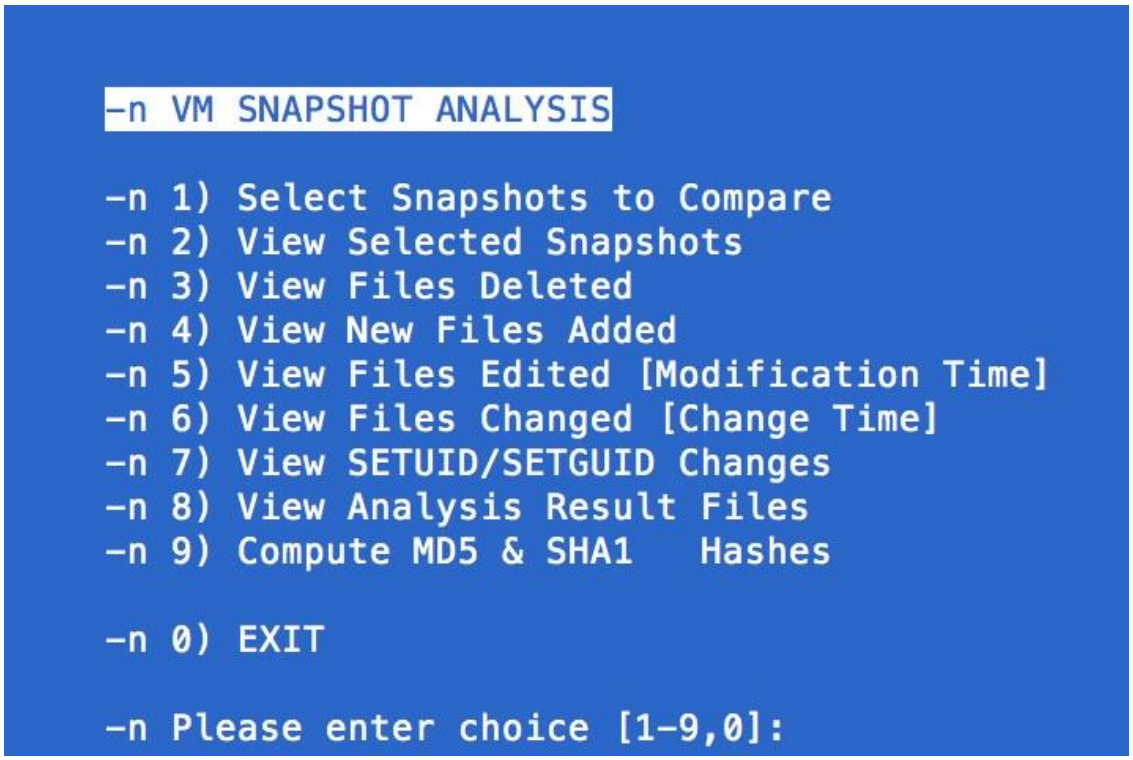


2.9 pav. Elektroninio pėdsako sistemos duomenų esybės būsenų diagrama

Jei tyrėją netenkina sąsajumo režimas, jis gali jį pasirinkti iš galimų, arba rankiniu būdu nusistatyti ir jį išsisaugoti. Pasirinkus kitą režimą, sistemą jį pritaiko parametrus visiems failams namų direktorijoje. Turinio keitimo daviklis tikrina ar namų direktorijoje yra / dirba tyrėjas, jei jis išeina iš bylos, sistema išjungia sąsajumos išvedimą į ekraną, taip galima visus resursus išnaudoti dirbant „tylos režimu“.

Tyrimo objekto naudotojų analizė

Žemiau pateiktas „elektroninio pėdsako pridėjimo“ tyrėjo grafinės (ncurses; žr. priedai) sąsajos vaizdas 2.10 pav. Vartotojas gali pasirinkti norimą “shapshots” namų direktorijoje, kurios parametrus gali peržiūrėti arba keisti. Matomos galimos tyrėjo galimybės (kontrolinės sumos, UID, GID), pėdsakus pridėti ar atmesti, taip pat jį gali keisti.



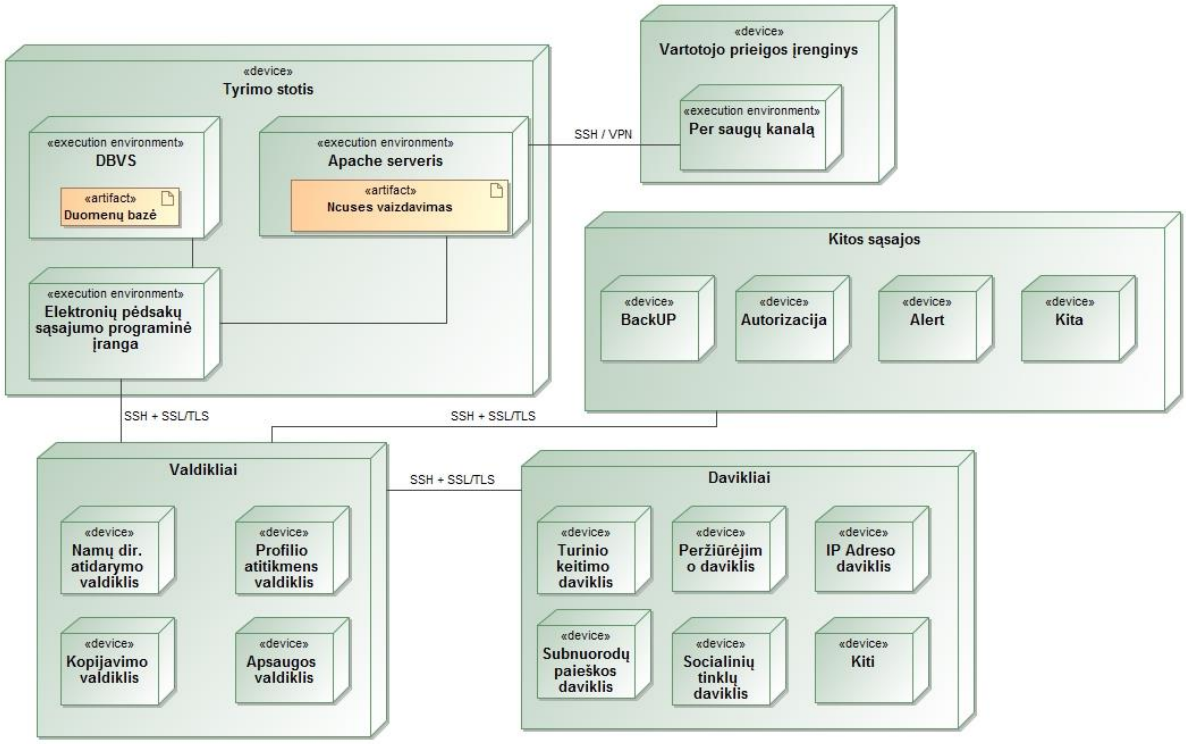
2.10 pav. Vartotojo (tyrėjo) “ncurses” sąsaja

Sistemos diegimo diagrama

Pagrindiniai sistemos elementai:

- sistemos tyrimo stotis;
- vartotojo prieigos prietaisai;
- valdikliai bei davikliai.

Tyrimo stotis susideda ir trijų pagrindinių komponentų: Sh (shell), duomenų bazių valdymo sistemos (gali būti rašymas į failą ar į sqlite duomenų bazę) su duomenų baze ir elektroninių pėdsakų valdymo sistema (ncuses). Į duomenų bazę kaupiami duomenys atkeliaujantys iš įvairių sistemų valdiklių (programos-scriptai), kurie duomenis gauna iš daviklių (scriptai, „robotai“). Surinkta informacija yra analizuojama ir pateikiamas rezultatas tyrėjui. Elektroninių pėdsakų valdymo sistemoje nustatomi norimi parametrai, tokie namų direktorija, kopijavimo režimas.



2.11 pav. Elektroninių pėdsakų valdymo sistemos diegimo diagrama

Vartotojas tereikia prisijungti per ssh (būtinai iš intraneto) arba naudojant VPN (per internetą), gali realiu laiku stebėti parametrus.

2.3. **Išvados**

Skaitmeninio pėdsako ir įpročio koreliacijos algoritmas leidžia palyginti bet kokią gautą informaciją tarp sudaryto įtariamojo profilio ir gauto įrenginio Tai gali būti atsarginė kopija „debesyje“, išoriniame diske, kitoje laikmenoje. Taip pat gauta galimybė pertikrinti duomenys naudojant dar vieną, papildomą kintamąjį – socialinių tinklų (ar gautų paieškų rezultatų) profilį. Toks modelis leidžia *dar padidinti* informacijos patikimumą iki 10 procentų.

Toks modelis leidžia ne vien tik nustatyti skaitmeninio nusikaltimo „pirštų anspaudų“ savininką, bet ir panaudoti prevencijos tikslais – nustatyti grupę asmenų veikiančiu kartu ar planuojant skaitmeninį nusikaltimą.

Taip pat šį modelį galima naudoti, kai atsiranda būtinybė nustatyti autorystės teises. Pagal profilio sudarymo metodą galima labai aiškiai išskirti kas konkrečiai dirbo prie išeities tekstų, redagavo konkrečius failus (video, audio, foto, dokumentai).

3. ELEKTRONINIŲ NUSIKALTIMŲ PĖDSAKŲ FIKSAVIMO METODIKOS IR MODELIO EKSPERIMENTINIS TYRIMAS

Tyrimo tikslas – apskaičiuoti (procentine išraiškai) elektroninio įpročio (pėdsako) priklausomybę įrenginiui (iš kurio jis buvo paimtas), sistemai (iš kurios jis buvo paimtas), namų direktoriai (su kuria jis koreliuoja) taip, įrodant pėdsako ir įtariamojo sąsajumą. Tokios informacijos patikimumas gali leisti nustatyti intelektualios nuosavybės [33] savininką ateityje.

Tam tikslui pasiekti keliami tyrimą sudarys trys uždaviniai.

- Virtualių aplinkų kūrimas su vienodu "įpročiu".
- Virtualių aplinkų tinkamas saugojimas (snapshot's) (žr. priedas 6.2)
- Koreliacija tarp: "įpročio – namų direktorijos – įrenginio – sisteminio" profilio.

Siekiamo sprendimo apibrėžimas

Elektroninio pėdsako sąsajumas tarp įtariamojo įpročių ir įrenginio, failų sistemos, failais.

3.1. **Eksperimentinio tyrimo scenarijus**

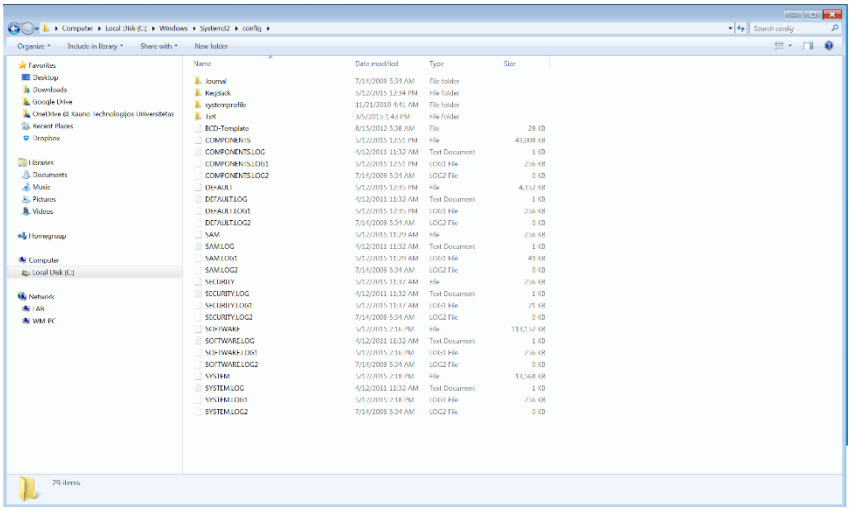
Scenarijus ir eiga
Padaryti poėmį. Mūsų atveju naudoti parašytą sprendimą sistemos "snapshot" atlikimui
Padaryti failų sulaikymą (kontrolinės sumos)

Tam, kad atlikti matematinį palyginimą reikia surinkti sekančia informaciją:
Įtariamojo "snapshot" – veikiančios (ar poėmio metu išsaugotos) sistemos – atiks įrenginio profilį
Įtariamojo namų direktorijos kopijos – atitiks namų direktorijos kriterijus
Socialinio tinklo profilio informacija – atitiks socialinio tinklo profilį

Užduotis
Poėmio metu (mūsų atveju snapshot) sulaikytos sistemos, vartotojo "SG" darbalaukio direktorijoje aptiktas katalogas "old". Ar jame esantys failai (žr. Priedas Nr. 6.1) priklauso:
A – poėmio metu sulaikytam įrenginiui (mūsų atveju snapshot kopija)
B – sudaryti socialinį profilį, pagal įpročius
C – sudaryti įrenginio profilį
D – aprašyti indikacijas, kurias panaudosim koreliacijai atlikti, pagal įpročius

3.2. **Eksperimentinio tyrimo eiga**

Darbas su Operacine sistema ir registrais



3.1 pav. Windows OS registrai

Patikriname registrus ir juose esančia informaciją (ar nėra pasikeitusi)

HKEY_LOCAL_MACHINE \SYSTEM : \system32\config\system
HKEY_LOCAL_MACHINE \SAM : \system32\config\sam
HKEY_LOCAL_MACHINE \SECURITY : \system32\config\security
HKEY_LOCAL_MACHINE \SOFTWARE : \system32\config\software
HKEY_USERS \UserProfile : \winnt\profiles\username
HKEY_USERS.DEFAULT : \system32\config\default

HKEY_LOCAL_MACHINE \HARDWARE : hive failas
HKEY_LOCAL_MACHINE \SYSTEM \Clone : hive failas

Randame sąsajas tarp instaliuotos įrangos (USB įšorinis diskas)

Randame sąsają tarp progrmainės įrangos (I)

Mūsų atveju yra programinė įranga: MS Office 2013, kuri registruota Šarūno Grigaliūno vardu, sarunas.grigaliunas@ktu.edu Serijos numeris: 149dbce7-a48e-44db-8364-a53386cd4580

```
cscript "C:\Program Files (x86)\Microsoft Office\Office15\OSPP.VBS" /dstatus
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

---Processing--------------------------------------------------------------
SKU ID: 149dbce7-a48e-44db-8364-a53386cd4580
LICENSE NAME: Office 15, OfficeO365ProPlusR_Subscription1 edition
LICENSE DESCRIPTION: Office 15, TIMEBASED_SUB channel
LICENSE STATUS:  ---LICENSED---
```

3.1 lentelė Informacijos filtravimas pagal indikatorius

Iš kur gauta informacija (iš)	**Filtras (kur)**	**Indikatorius (kas)**
k1(A1)(D1) - SAM	m8(A1) – komputerio vardas	i1(k1) (A1)(D1) - WM-PC

	m9(A1) – sistemos vartotojas	i2(k2) (A1)(D1) - SG
k2 (A1)(D1) - SYSTEM.DAT	m10(A1) - instaliuotos įrangos pavadinimas	i3(k3) (A1)(D1) -JM20336 SATA, USB Combo
	m14(A1) - serijos numeris	i4(k4) (A1)(D1) -
k3 (A1)(D1) - SOFTWARE.DAT	m13(A1) - programinė įranga	i5(k5) (A1)(D1) - MS Office 2013
	m14(A1) - serijos numeris	i6(k6) (A1)(D1) - 149dbce7-a48e-44db-8364-a53386cd4580
k4 (A2)(D1) - ID001.ffdata	m1(A2) - Failas	i7 (k4)(A2)(D1) - ID001-201311.ffdata
	m6(A2) - Kelias iki failo	i8 (k4)(A2)(D1) - c:\Users\SG\Documents\old\vmi\
	m16(A2) - slavyvardis (trumpinys)	i9 (k4)(A2)(D1) - sarugrig
	m7(A2) - MD5	I10 (k5)(A2)(D1) - Priedas su MD5 sumom
k5 (A2)(D1) - laiskas.docx	m1(A2) - Failas	i11 (k5)(A2)(D1) - laiskas.docx
	m16(A2) - slapyvardis	i12 (k5)(A2)(D1) - grigaliunas
	m6(A2) - Kelias	i13 (k5)(A2)(D1) - c:\Users\SG\Documents\old\

	m7(A2) - MD5	i14 (k5)(A2)(D1) - Priedas su MD5 sumom
k6 (A3)(D1) - MSOIdentityCRL	m28(A3) – autentifikavimos paketas	i15 (k6)(A3)(D1) - sarugrig@ktu.edu
	m28(A3) - vartotojo vardas	i16 (k6)(A3)(D1) - sarugrig
k7 (A3)(D1) - kibernetinesauga_sgrigaliunas.pdf	m28(A3) - URL	i17 (k7)(A3)(D1) - SKAITMENINISLEGIONAS.LT
	m28(A3) - URL	i18 (k7)(A3)(D1) - 5a.lt
k8 (A3)(D1) - disabledenabled_pritaikyta_lt_darbas - Copy.dovx	m28(A3) - URL	i19 (k8)(A3)(D1) - disabledenabled.eu
	m28(A3) - el paštas	I20 (k8)(A3)(D1) - info@disabledenabled.eu
k9 (A4)(D1) - Paslaugu sutartis_ios - Copy.docx	m19(A4) - Failas	i21 (k9)(A4)(D1) - Dokumentas
	m16(A4) - Asmens kodas	i22 (k9)(A4)(D1) - 37701260053
	m16(A4) -Adresas	i23 (k9)(A4)(D1) - Salėgrąžų 1-80, Kaunas

	m27(A4) - ID kortelės numeris	i24 (k9)(A4)(D1) - 12271358
	m24(A4) – dokumento išsaugojimo data	i25 (k9)(A4)(D1) - 2014-03-13 08:50:00
k10 (A5)(D1) - Pazyma_apie_laikina_pavanimo_itraukima (1).pdf	m1(A5) - Failas	i30 (k10)(A5)(D1) - Pazyma_apie_laikina_pavanimo_itraukima (1).pdf
	m6(A5) - path	I31 (k10)(A5)(D1) - c:\Users\SG\Desktop\
	m32(A5) – Tvarkytojas	i32 (k10)(A5)(D1) - Valstybinė įmonė registrų centras
	m24(A5) - asmensk kodas	i33 (k10)(A5)(D1) - 37701260053
	m24(A5) - Dokumento prašymo pateikimo data	i34 (k10)(A5)(D1) -2014-12-06 17:53
	m7(A5) - MD5	i35 (k10)(A5)(D1) - Priedas su MD5 sumom
k11 (A6)(D1) - darbas_teise.jpg	m1(A6) - Failas	i36 (k11)(A6)(D1) - darbas_teise.jpg
	m6(A6) - Kelias	i37 (k11)(A6)(D1) - c:\Users\SG\Desktop\KTYUML/KTU-UML-DARBAS/
	m7(A6) - MD5	i38 (k11)(A6)(D1) - Priedas su MD5 sumom
k12 (A6)(D1) - aplinka-2014-05-12-Draft.docx	m1(A6) - Failas	i39 (k12)(A6)(D1) - aplinka-2014-05-12-Draft.docx
	m6(A6) - Kelias	I40 (k12)(A6)(D1) - c:\Users\SG\Documents\old\
	m7(A6) - MD5	I41 (k12)(A6)(D1) - Priedas su MD5 sumom
k13 (A6)(D1) - BZN.docx	m1(A6) - Failas	i42 (k13)(A6)(D1) - BZN.docx

	m6(A6) - Kelias	i43 (k13)(A6)(D1) - c:\Users\SG\Documents\old
	m7(A6) - MD5	i44 (k13)(A6)(D1) - Priedas su MD5 sumom
k14 (A8)(D1) - JAR-PBA.doc	m1(A8) - Failas	i45 (k14)(A8)(D1) - JAR-PBA.doc
	m6(A8) - Kelias	i46 (k14)(A8)(D1) - c:\Users\SG\Desktop\old
	m7(A8) - MD5	i47 (k14)(A8)(D1) - Priedas su MD5 sumom
k15 (A8)(D1) - f_000014	m1(A8) - Failas	i48 (k14)(A8)(D1) -f_000014
	m6(A8) - path	c:\Users\SG\AppData\Local\Google\Chrome\User Data\Default\Cache
	m7(A8) - MD5	i49 (k14)(A8)(D1) - Priedas su MD5 sumom
k16 (A9)(Si)(D1) - History.dat	m40(A9) - URL	I50 (k16)(A9)(D1) - https://www.facebook.com/sarunas.grigaliunas
K17 (A2)(D1)	m16(A2) - formhistory.sqlite	i53 (k17)(A2)(D1) - sqlite
	m28(A2) - vartotojo vardas	i55 (k17)(A2)(D1) - sarunas.grigaliunas@gmail.com
K18 (A5)(D1) log.Sun.txt	m32(A5) – vartotojo vardas	i58 (k17)(A5)(D1) - log.Sun.txt
	m26(A2) - vartotojas	i59 (k17)(A5)(D1) - ginvest912
	m26(A2) - Kelias	I60 (k17)(A5)(D1) - c:\Users\SG\Desktop\backup\IBJts
	m7(A2) - MD5	I61 (k17)(A5)(D1) - Priedas su MD5 sumom
K18 (A9)(D1)	m30(A2) – Failas	I62 (k17)(A9)(D1) - ktuedu.sharepoit[1].xml
	m23(A2) - vartotojo inicialai	i63 (k17)(A2)(D1) - Šarūnas Grigaliūnas
	m7(A2) - MD5	i64 (k17)(A2)(D1) - Priedas su MD5 sumom
Tyrimas atliekamas c:\Users\SG namų direktorijoje		

Iš gautos informacijos ir įkalčių (žr. Priedas Nr. 6.1) ieškom papildomu sąsajų (žr. Priedas Nr. 6.3). Facebook“ kasdien būsenos atnaujinimus skelbia 400 mln. vartotojų. Vieni įkelia savo pusryčių nuotraukas, o kiti dalijasi įkvepiančiomis žinutėmis. Per pastaruosius kelerius metus tyrėjai aiškinosi, ką socialinio tinklo vartotojų elgesys „Facebook“ parodo apie jų asmenybes ir savigarbą. Taip gauname papildoma I (indikatorių) dar vieną sąsajos patvirtinimą tarp Šarūno ir skaitmeninis.legionas, bei dar vieną telefono numerį. Čia pasitarnauja asmenybės įprotis skelbti asmeninę informaciją socialiniam tinkle.

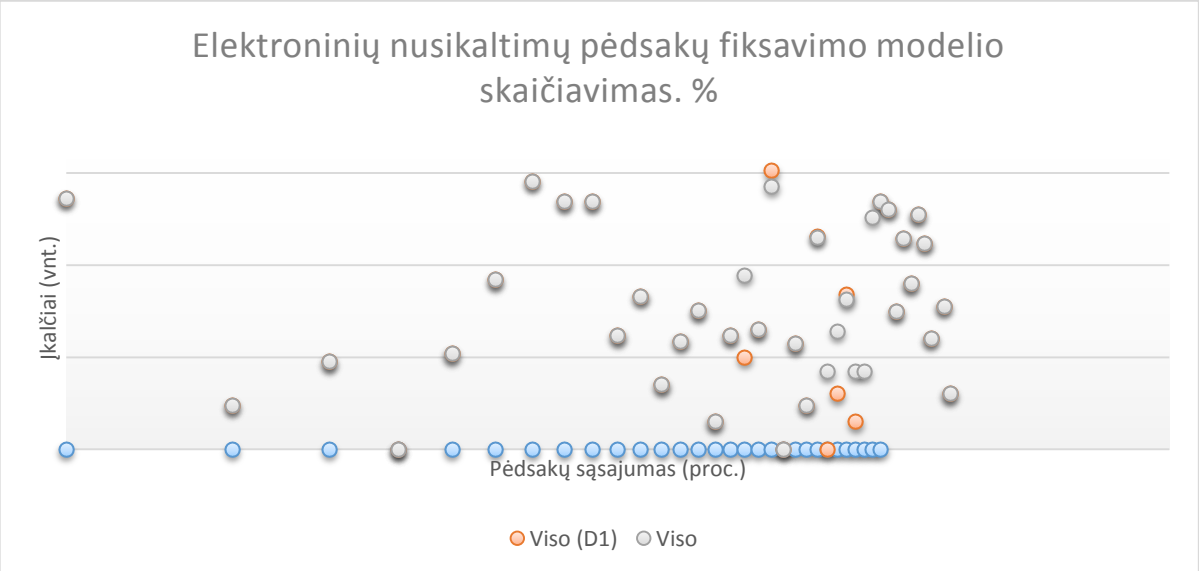
Tiriamojo vartotojo aprašymą Puc (di) sutampa su vartotojo profiliu Pu (di) ir informacija papildoma su socialiniu profiliu S(i), kuri skiriasi tik pagal apibrėžimą.

Iš tiesų, surinkti rodikliai bus naudojamas kaip filtrai ieškoti informacijos per sutampančius kitus įkalčius kitam snapshot, t. y. D1 ir D2. Išskirti tik tiek įkalčiai, kurie pasikartojo identiškai.

3.2 lentelė Įkalčių analizės rezultatas

Nr.	Tipas	Indikatorius	D1	D2	Viso (D1)	Viso
1	Tyrimo katalogas	... \Users\SG\Desktop\	1	1	533	533
2	Tyrimo katalogas	... \Users\SG\Desktop\KTYUML/KTU-UML-DARBAS/	1	1	3	3
3	Tyrimo katalogas	... \Users\SG\Documents\old\	1	1	9	9
4	Kelias	... \Users\SG\AppData\Local\Google\Chrome\User Data\Default\Cache	1	1	1	1
5	Kelias	... \Users\SG\Desktop\backup\IBJts	1	1	11	11
6	Kelias	... \c:\Users\SG\Documents\old\vmi\	1	1	69	69
7	Kelias	... \Users\SG\	1	1	814	814
8	Asmeninis failas	Paslaugu sutartis_ios - Copy.docx	1	1	487	487
9	Asmeninis failas	BZN.docx	1	1	487	487
10	Asmeninis failas	ID001-201311.ffdata	1	1	17	17
11	Asmeninis failas	Pazyma_apie_laikina_pavanimo_itraukima (1).pdf	1	1	46	46
12	Siuntėjo el. paštas	sarunas.grigaliunas@gmail.com	1	1	5	5
13	Siuntėjo el. paštas	sarunas.grigaliunas@ktu.edu	1	1	15	15
14	Vartotojo vardas	sargrig	1	1	32	32
15	Vartotojo vardas	ginvest912	1	1	2	2
16	Asmens kodas	37701260053	1	1	17	17
17	Adresas	Saulėgrąžų 1-80, Kaunas	1	1	10	78
18	UAB	Vidulus	1	1	20	20
19	MB	Disabled Enabled	1	1	1058	722

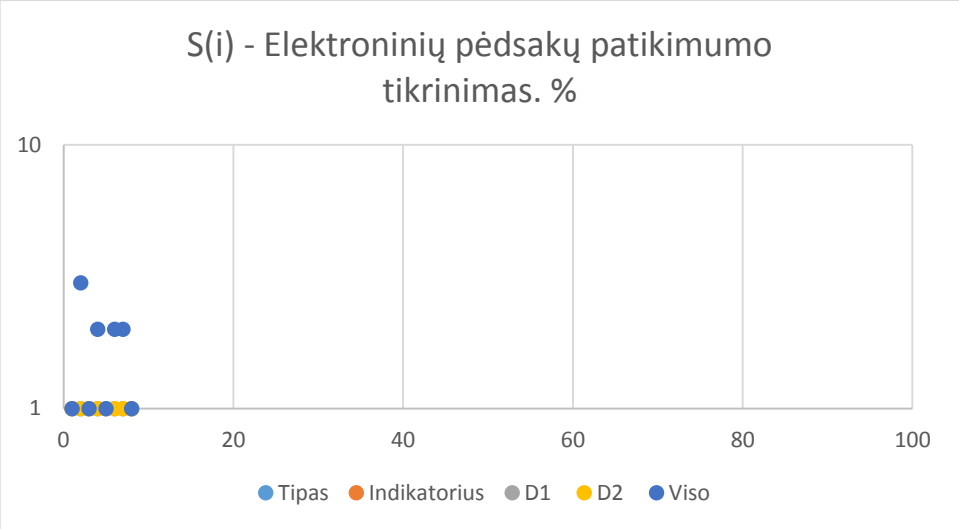
20	ID kortelės Nr.	12271358	1	1	1	1
21	Slapyvardis	grigaliunas	1	1	14	14
22	Slavyvardis	sarugrig	1	1	3	3
23	Vartotojo indentifikacija	Šarūnas Grigaliūnas	1	1	206	201
24	Telefonas	37061366588	1	1	1	7
25	Telefonas	37259519249	1	1	4	19
26	url	http://www.facebook.com/sarunas.grigaliunas	1	1	48	42
27	url	http://disabledenabled.eu	1	1	2	7
28	url	http://vidulus.lt	1	1	0	7
29	Įranga	USB HDD	1	1	15429	332
30	Programinė įranga	MS Office 2013	1	1	487	487
31	Vartotojo vardas	username	-1	-1	401	401
32	Vartotojo slaptažodis	passwd	-1	-1	31	31
33	Slaptažodžiai	slaptazodis	-1	-1	196	196
34	Vartotojo vardas	sarunas.grigaliunas	-1	-1	63	63
35	Telefonas	Tel.	-1	-1	350	350
36	Adresas	Adresas	-1	-1	172	172
37	URL	ktu.edu	-1	-1	16	16
38	Asmeninis failas	Paveiksliukai	-1	-1	2730	2730
39	Asmeninis failas	Archyvas	-1	-1	36	36
40	Asmeninis failas	Video	-1	-1	4	4



3.2 pav. Elektroninių nusikaltimų pėdsakų fiksavimas

3.3 lentelė Įkalčių, naudojant S(i), analizės rezultatas

Nr.	Tipas	Indikatorius	D1	D2	Viso	Kas rasta
1	Socialinis tinklas	Facebook	1	1	1	Telefono numeris
2	Socialinis tinklas	Facebook	1	1	3	El. paštas
3	Socialinis tinklas	Facebook	1	1	1	Asmens kodas
4	Socialinis tinklas	Facebook	1	1	2	Vartotojo vardas
5	Socialinis tinklas	Twitter	1	-1	1	Vartotojo vardas
6	Paieška	Google	1	1	2	Telefono numeris
7	Paieška	Google	1	1	2	Įmonė
8	Paieška	Google	1	1	1	Banko sąskaita



3.3 pav. Elektroninių nusikaltimų pėdsakų fiksavimo koreliacija su S(i)

3.3. **Eksperimentinio tyrimo rezultatų apibendrinimas**

Tiriamasis profilis Puc (D1) yra gautas iš vieno prietaiso, surinkti rodikliai yra naudojami kaip filtrai aptikti jungtis, sąsajas ir / arba skirtumus. Eksperimente poėmio metu užfiksuoti 15429 įkalčiai. Iš jų 332 iškart atmesti – sisteminiai (pvz. dll, h, exe) ir paleidžiamieji failai profiliavime nedalyvauja, kaip nenešantis aktualios informacijos.

Galutinis žingsnis, jei būtina tarp snapshot / modifikacijos / ištrynimo ar pridėjimo failų daromas dviejų prietaisų datos, kontrolinės sumos palyginimas, siekiant atstatyti vartotojo veiksmų istoriją įtaisuose (snapshot mūsų atveju). 3.1 lentelėje pavyzdys iliustruoja, kaip ieškoti rodiklių, iš prietaiso D1, failai saugomi (priedas Nr. 6.1) ir lyginami su prietaisu D2. Visi failai tinkamai įforminti išsaugant jų pirminę informaciją (žr. 6.1). Jų gavome 30 - Informacija vartotojo daliai, apibūdinanti (75% filtrų taikoma). Jie rodo, kad abu prietaisai buvo naudojamas to paties naudotojo. Tačiau šis palyginti tipas yra vienas iš būdų: charakteristikos informacijos paieška atliekama remiantis rodikliais

rasti viename įrenginyje (snapshot), vadinamas "pirminis", įvedant analizei papildomai S(i) socialinių tinklų esančia informaciją 10 %. Norint išspręsti “pirminio” įrodymo problemą, reikia imtis atlikti papildomą žingsnį, tikrinant profilius tarp kryžminių nuorodų, kuri yra prieinam įvedant socialinio tinklo profilio informaciją.

Rezultato vertinimas yra vykdoma kiekybine prasme (t. y., atsižvelgiant į sutampančių rodiklių, išmatuotų skaičių), ir kokybiškai (t. y., informacijos teisingumą) palyginant.

Tyrimo skaičiavimas vykdoma statistiniu būdu skaičiuojant sutampančių rodiklių rastą procentą kiekvienam snapshot’e, kurie vėliau naudojami kaip filtras visiems įkalčiams palyginti.

SKAIČIAVIMO PAVYZDYS:

Kiekybinis vertinimas gautų paprasto Palyginimo (bylos pateikta 3.2 lentele) būdu 1 užduotis rezultatai - Sukurti vartotojo profilis mėginio PCU (D1)

N. naudojami filtrai (paimta iš minimalaus įrodymų rinkinio) 44

Rezultatas: rodikliai išgauti 40

2 užduotis - Mokslinių tyrimų naudojant filtrai lyginant su snapshot D2 rodikliais:

N. filtrai taikomi (paimta iš įrodymų rinkinio) 40

REZULTATAS: sutampančių rodikliai Rasta 30 ir 4 socialinių ar paieškos tinklų

Dėl viso įrodymų rastą ir taikytą. 40 - filtras paprasta palyginti. Vėliau palyginus su socialiniu profiliu ir paieškos google mechanizmu, buvo aptikta 30 + 4 (tai sudaro 10 proc. nuo viso filtro) sutampančių rodikliu, ***kurie įrodo namų direktorijos priklausomumą Šarūnui Grigaliūnui net 75% - filtras ir 10 % nuo viso patikimumo (pertikrinta), 82,5 %patikimumu.***

3.4 pav. Profilio informacinis rezultatas

Ši analizė suteikia informacijos, gautos iš surinktų įrodymų ar remiantis atskirais rodikliais, susijusių su jų galimybę panaudoti įrodant įtariamojo įprotį. Atsižvelgiant skaitmeninio pobūdžio analizę, šaltinių vertinama: jie tinkamai ištraukti (yra galimybės snapshot ar fizinio poėmio) ar yra patikrinti maišos algoritmais, yra laikomi "visiškai patikimi" ir galima vėliau naudoti teismuose. Atsižvelgiant į gautą čia pateiktą informaciją, tai rodo kokybinį vertinimą (tačiau tai labai priklauso ir nuo tyrėjo atsakomybės, kompetencijos atliekant technologinį poėmį). Toliau pateiktas pavyzdžiu buvo siekiama tik surinkti sutampančią (t. y. turėti tik dvi vertės: galimybę lygintis), kuri gali įrodyti, kad tikrai to paties įtariamojo tapatybė yra nustatyta.

Eksperimento tęstinumas

Pamąstymai ir įžvalgos. Eksperimentas parodė, kad galimas dar vienas tikrinimo šaltinis: informacijos šaltinio pasitikėjimas. 3.3 lentelėje pateikiami galimi matavimų apibūdinimai. Eksperimentą galima kartoti įvedant dar du indikatorius – informacijos siuntėjo pasitikėjimo koeficientas ir informacijos gavėjo koeficientas (I(source) ir I(destination)).

3.4 lentelė Šaltinio pasitikėjimo matavimo apibūdinimas

I (s) ir I (d)		Apibūdinimas
1	**Dydis**	Skaičius objektų, kuriais pasitikimas. Ar pasitikėjimas bus skirtas tik vienam ar išsiplės iki per daug? Ar grupė, kuri atliks bendrą sprendimą yra patikima?
2	**Simetrija**	Pasitikėjimo vektorius (kryptis). Pasitikėjimas gali būti vienos krypties (asimetriškas) ir reikia nurodyti kuria kryptimi pasitikėjimas turi eiti, arba abiejų krypčių (simetriškas). Asmuo kuris taip pat turi jumis pasitikėti turi sugalvoti bausmę už pasitikėjimo sulaužymą, kad pasitikėjimas nebūtų sulaužytas.
3	**Matomumas**	Visų taikinio ir jo aplinkos operacinių dalių ir procesų permatomumo lygis.
4	**Įtaka**	Taip pat vadinamas *kontrole*, operatoriaus įtaka apimtyje.
5	**Nuoseklumas**	Istoriniai įrodymai apie taikinio sukompromitavimą ir korupciją.
6	**Pastovumas**	Pasikeitimų taikinyje kiekis ir laikas.
7	**Kompensacija**	Atitinkamos garantijos kompensacija yra kompensacija pasitikėjimo suteikėjui arba bauda sulaužančiam pasitikėjimą. Tai yra dydis nustatytas pasitikėjimui taikiniu.
8	**Vertė**	Finansinė kompensacija dėl rizikos, laimėjimo ir naudos gavimo kiekis dėl kurio rizikos priėmimas suteikiant taikiniui pasitikėjimą yra pakankamas, kad kompensuoti nelaimės pasitikėjime riziką.
9	**Komponentai**	Elementų skaičius, kurie šiuo metu taikiniu teikia išteklius per tiesioginę arba netiesioginę sąveiką, panašiai kaip keturių taškų intervencijoje.
10	**Poringumas**	Atskyrimo, tarp taikinio ir išorinės aplinkos, kiekis.

Šaltinio patikimumą reiktų matuoti tam, kad iškart labai aiškiai išskirti surinkto informacijos svorį (pvz. jeigu informacijos šaltinis yra Valstybinė mokesčių inspekcija – tai tokio šaltinio patikimumas yra arti 100 proc. Tačiau, jei informacijos šaltinis yra „Facebook“ sienos pranešimas, tai jo koeficientas bus ženkliai mažesnis).

3.4. **Išvados**

Šioje analizėje, siūlome naują elektroninių pėdsakų tyrimo metodą, remiantis aibių teorija, kurios pagalba galima išgauti naudingos informacijos iš skaitmeninio pėdsako ar prietaiso, bei padėti nusikalstamų subjektų identifikavimui. Jis analizuoja duomenis ir metaduomenis įsimintinus į skaitmeninį prietaisą, taikant konkrečius metodus, kurių bus imtasi atliekant praktinį profiliavimo teorijos patikrinimą, siekiant gauti informaciją. Kaip jau minėta, procesas prasidės iš mokslinių tyrimų ir praktinės analizės atliktos visumos, kuri gali būti surinkta iš "skaitmeninių pėdsakų" paliko skaitmeniniu pavidalu jos galimas vartotojas. Tai įmanoma, nes kompiuterio vartotojas yra žmogus linksta pritaikyti visas aplinkas, su kuria jis ar ji sąveikauja. Taigi, šis metodas bus ypač naudingas atliekant elektroninių nusikaltimų tyrimams, taip pat kompiuterinių apgavysčių, sukčiavimo apsimetant atvejais, kiber persekiojimas, vaikų pornografija, įsilaužėlių atakų, ypač jei tai koreliuoja su kriminalistikos metodais, kai bandoma paslėpti ar ištrinti nusikaltimų įrodymus. Skaitmeninio profiliavimo metodas yra labai naudinga atliekant operacijas prieš organizuotą nusikalstamumą, kovos su terorizmu ir atliekant žvalgybos operacijas, taip pat galima būtų susieti su statistiniu tyrimo prognozavimo ir prevencijos nusikalstamiems įvykiams.

Paaiškinti sprendimai, diagramos ir jų elementai taip, kad jie būtų suprantami kitiems. Atskleistas sprendimas – kas jame ypatinga, reikšminga, naujoviška, svarbu.

Atliktas elektroninių pėdsakų sistemos projektavimas panaudojant įvairius modelius padėjo suprasti, veiklos procesų modelių pranašumą sistemų projektavimų etapuose. Naudojant tokią modeliavimo sistemą yra lengviau nustatyti galimus sprendimo būdus.

Sudaryta tyrimo įrankio skaičiavimų (poėmio metu užfiksuotų įkalčių): leis paprasčiau įrodyti įpročio valdyti savo informaciją ir įkalčių tapatumą ir priklausymą vienam asmeniui.

Eksperimentas įrodė, kad poėmio metu išnagrinėtos informacijos (įkalčių) priklausomumo **patikimumas yra net 82,5 proc**.

Numatytas eksperimento tęstinumas tam, kad informacija būtu ne vien tik patikima ar atitinkanti įtariamojo profilį, bet dar ir būtų galimybė sudaryti tos informacijos šaltinių pasitikėjimo medį, jei sąsajumo tarp įtariamojo ir informacijos šaltinio.

4. IŠVADOS

Apžvelgtas ir pasiūlytas kitoks būdas elektroninių pėdsakų įrodymo būdas – įtariamojo profiliavimas pagal gautus skaitmeninius pirštų anspaudus. Kurio esminis principas profilio ir įkalčio palyginimas.

Toks pirštų anspaudų sudarymo būdas yra koreliacija tarp: „įpročio“, „namų direktorijos“, „socialinio / paieškos tinklo informacijos dedamosios“ ir poėmio metu sulaikytos kompiuterinės / programinė įrangos.

Skaitmeninio pėdsako ir įpročio koreliacijos algoritmas leidžia palyginti bet kokią gautą informaciją tarp sudaryto įtariamojo profilio ir gauto įrenginio Tai gali būti atsarginė kopija „debesyje“, išoriniame diske, kitoje laikmenoje. Taip pat gauta galimybė pertikrinti duomenys naudojant dar vieną, papildomą kintamąjį – socialinių tinklų (ar gautų paieškų rezultatų) profilį. Toks modelis leidžia *dar padidinti* informacijos patikimumą iki 10 procentų. Toks modelis leidžia ne vien tik nustatyti skaitmeninio nusikaltimo „pirštų anspaudų“ savininką, bet ir panaudoti prevencijos tikslais – nustatyti grupę asmenų veikiančiu kartu ar planuojant skaitmeninį nusikaltimą. Taip pat šį modelį galima naudoti, kai atsiranda būtinybė nustatyti autorystės teises. Pagal profilio sudarymo metodą galima labai aiškiai išskirti kas konkrečiai dirbo prie išeities tekstų, redagavo konkrečius failus (video, audio, foto, dokumentai).

Sudaryta tyrimo įrankio skaičiavimų (poėmio metu užfiksuotų įkalčių): leis paprasčiau įrodyti įpročio valdyti savo informaciją ir įkalčių tapatumą ir priklausymą vienam asmeniui.

Eksperimentas įrodė, kad poėmio metu išnagrinėtos informacijos (įkalčių) priklausomumo **patikimumas yra net 82,5 proc**.

Numatytas eksperimento tęstinumas tam, kad informacija būtu ne vien tik patikima ar atitinkanti įtariamojo profilį, bet dar ir būtų galimybė sudaryti tos informacijos šaltinių pasitikėjimo medį, jei sąsajumo tarp įtariamojo ir informacijos šaltinio.

5. LITERATŪRA

[1] D. Štitilis, „Kibernetinio saudumo teisinis reguliavimas: kibernetinio saugumo strategijos," Socialinės technologijos ISSN 2029-7564, pp. 189-207, 2013, 3(1).

[2] D. Štitilis, P. Pakutinskas, I. Dauparaitė, M. Laurinaitis, „Teisinė aplinka siekiant išvengti tapatybės vagystės elektroninėje erdvėje: JAV ir Lietuvos teosės aktų lyginamoji analizė," Socialinės technologijos ISSN 2029-7564, pp. 61-80, 2011.

[3] D. Stitilis, V. Klisauskas, „Peculiarities of the legal regulation of cybersecurity in the National Laws of Lithuania, Russia and the USA:cybersecurity strategies," Matters of Russian and International Law 7-8, pp. 80-91, 2013.

[4] N. Goranin ir D. Mažeika, Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos, 2011, p. 9-11.

[5] N. Goranin ir D. Mažeika, Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos, 2011, p. 17.

[6] N. Goranin ir D. Mažeika, Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos, 2011, p. 50-55.

[7] „LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMAS," 11 gruodžio 2014. [Tinkle]. Available: https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4 . [Kreiptasi 11 sausio 2015].

[8] N. Goranin ir D. Mažeika, Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos, 2011, p. 105-113.

[9] A. Reyes ir J. Wiles, Cybercrime and Digital Forensics:Forensics Software and Hardware, USA, 2007, p. 177-241.

[10] FTK. [Tinkle]. Available: http://accessdata.com/product-download . [Kreiptasi 11 sausio 2015].

[11] S. Mittakanti, „Forensics Analysis of the Lustre File System," 2011. [Tinkle]. Available: http://sci.tamucc.edu/~cams/projects/377.pdf . [Kreiptasi 2 gruodžio 2013].

[12] Live View. [Tinkle]. Available: http://www.cert.org/digital-intelligence/tools/liveview.cfm . [Kreiptasi 11 sausio 2014].

[13] Disk2vhd. [Tinkle]. Available: https://technet.microsoft.com/en-us/sysinternals/ee656415.aspx . [Kreiptasi 11 sausio 2015].

[14] D. Valatkevičius, "Nusikaltimų informatikai pėdsakų apibūdinimas," VU Teisės fakulteto Kriminalistikos ir baudžiamojo proceso katedra ISSN 1392-1274, p. 64-134, 2007.

[15] S. Yong-Dal, „New Model for Cyber Crime Investigation Procedure," Journal of Nex Generation Information Technology. Volume 2, Number 2, 2011.

[16] D. Bem, E. Huebner, „Computer Forensics Analysis in Virtual Environment," International Journal of Digital Evidence. Volume 6, Issue 2, 2007.

[17] D. Manson, A. Carlin, S. Ramos, A. Gyger, M. Kaufman, J. Treichelt, „Is the Open Way a Better Way? Digital Forensics using Open Source Tools," 2007. [Tinkle]. Available: http://dl.acm.org/citation.cfm?id=1256043 . [Kreiptasi 2 gruodžio 2013].

[18] C. Colombini, A. Colella, "Digital profiling: A computer forensics approarch," įtraukta *6th International Conference on Availability, Realiability and Security*, p. 330-343, 2011.

[19] S. Jastiuginas, „Integralaus informacijos saugumo valdymo modelio taikymas Lietuvos valstybės institucijose," Informacijos mokslai ISSN 1392-00561, pp. 31-58, 2012.

[20] R. Adams, V. Hobbs, G. Mann, „The advanced data acquisition model (ADAM): a process model for digital forensics proctice," 2013.[Tinkle]. Available: https://www.researchgate.net/publication/258224615_The_Advanced_Data_Acquisition_Model_%28ADAM%29_A_process_model_for_digital_forensic_practice . [Kreiptasi 2 gruodžio 2013].

[21] R. Leigland, A. W. Kings, "A formalization of Digital Forensics," 2004. [Tinkle]. Available: http://people.cis.ksu.edu/~sathya/formalizing-df.pdf . [Kreiptasi 2 gruodžio 2013].

[22] V. Roussev, Data Fingerprinting with Similarity Digests, Hong Kong, China, 2010, p. 207.

[23] K. Tadano, M. Kawato, R. Furukawa, F. Machida ir Y. Maeno, Digital Watermarking of Virtual Machine Images, Hong Kong, China, 2010, p. 257.
[24] E. Huebner ir S. Zanero, Open Source Software for Digital Forensics: The Case for Open Source Software in Digital Forensics, New York, 2010, p. 3.
[25] D. Bem, Open Source Software for Digital Forensics:Virtual Machine for Computer Forensics – Open Source Perspective, New York, 2010, p. 25.
[26] D. Dittrich, "Basics Steps in Forensic Analysis of Unix Sytem," 2013. [Tinkle]. Available: https://staff.washington.edu/dittrich/misc/forensics . [Kreiptasi 2 gruodžio 2013].
[27] K. Ruan, J Carthy, T. Kenchadi ir M. Crosbie, Cloud Foensics: Advances in Digital Forensics VII, Springer, 2011, p. 35-46.
[28] G. Grispos, W. B. Glisson, T. Storer, „Cloud Security Challenges: Investigation Policies, Standards, and Guidelines in a Fortune 500 Organization," 2013.
[29] H. Carvey ir D. Hull, Windows Registry Forensics: Tools, 2011, p. 35.
[30] L. A. Holt, M. Hammoudeh, „Cloud Forensics a Technical Approach to Machine Acquisition," įtraukta *2013 European Intelligence and Security Informatics Conference*, 2013.
[31] N. Clarke, Computer Forensics. A pocket Guide, UK, 2010, p. 64.
[32] H. Carvey ir E. Casey, Windows Forensics Analysis: Performing Analysis on a Budget, 2009, p. 443-466.
[33] Š. Grigaliūnas, "Intelektuali nuosavybė – turtas kurį irgi reikia saugoti," Technologija ISSN 1648-1717, p. 83-86, 2006.

6. PRIEDAI

6.1. priedas. Tyrimo profilio gauti įkalčiai ir jų fiksavimas

Informacija yra pateikiama kompaktinėje plokštelėje:

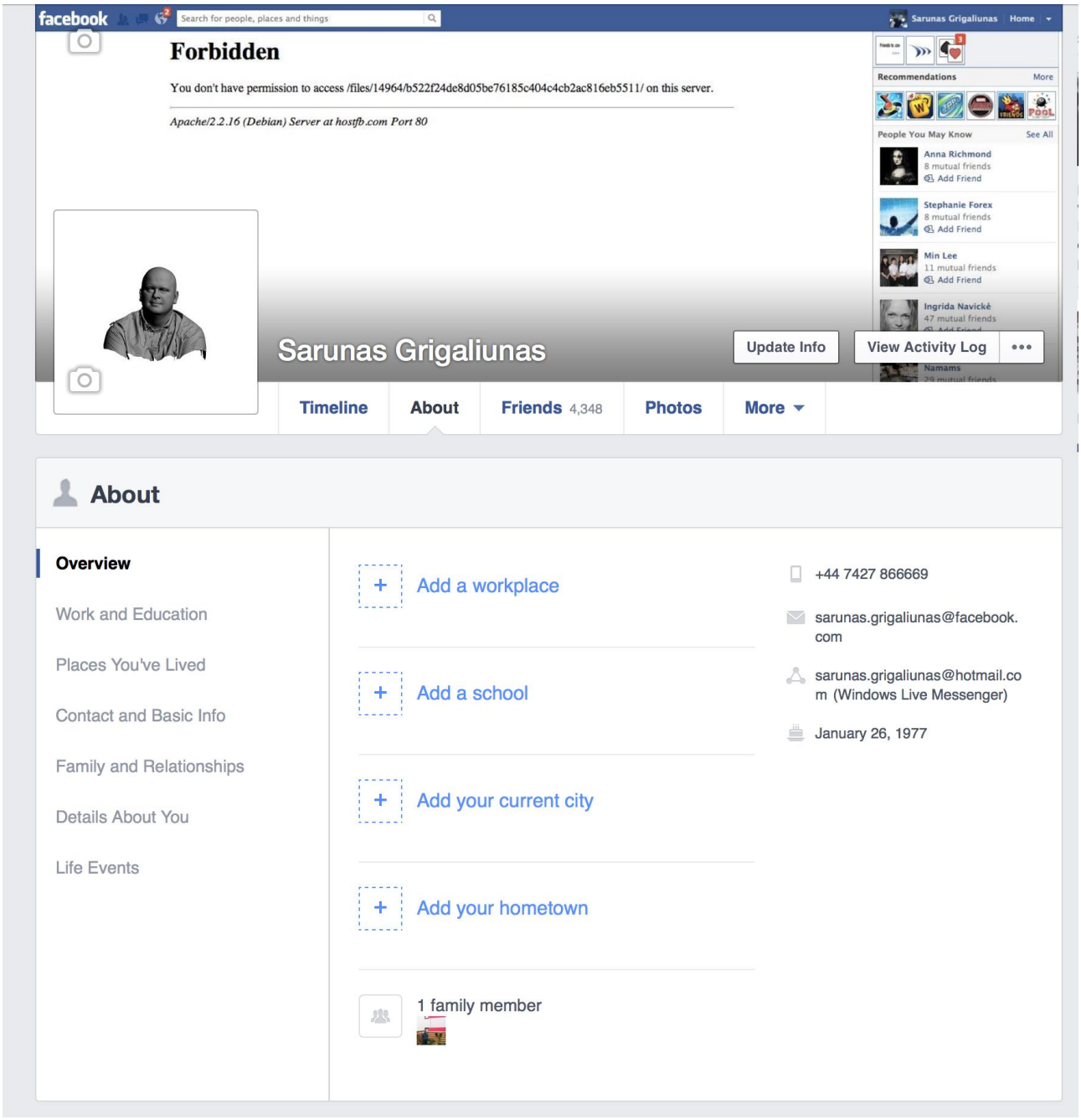
Namų direktorijos analizei paimti įkalčiai	398 psl.
Tyrimui fiksuoti failai (tyrimui panaudota: 15 097 failai)	918 psl.

6.2. priedas. Įkalčių fiksavimo realizavimas

Informacija yra pateikiama kompaktinėje plokštelėje:

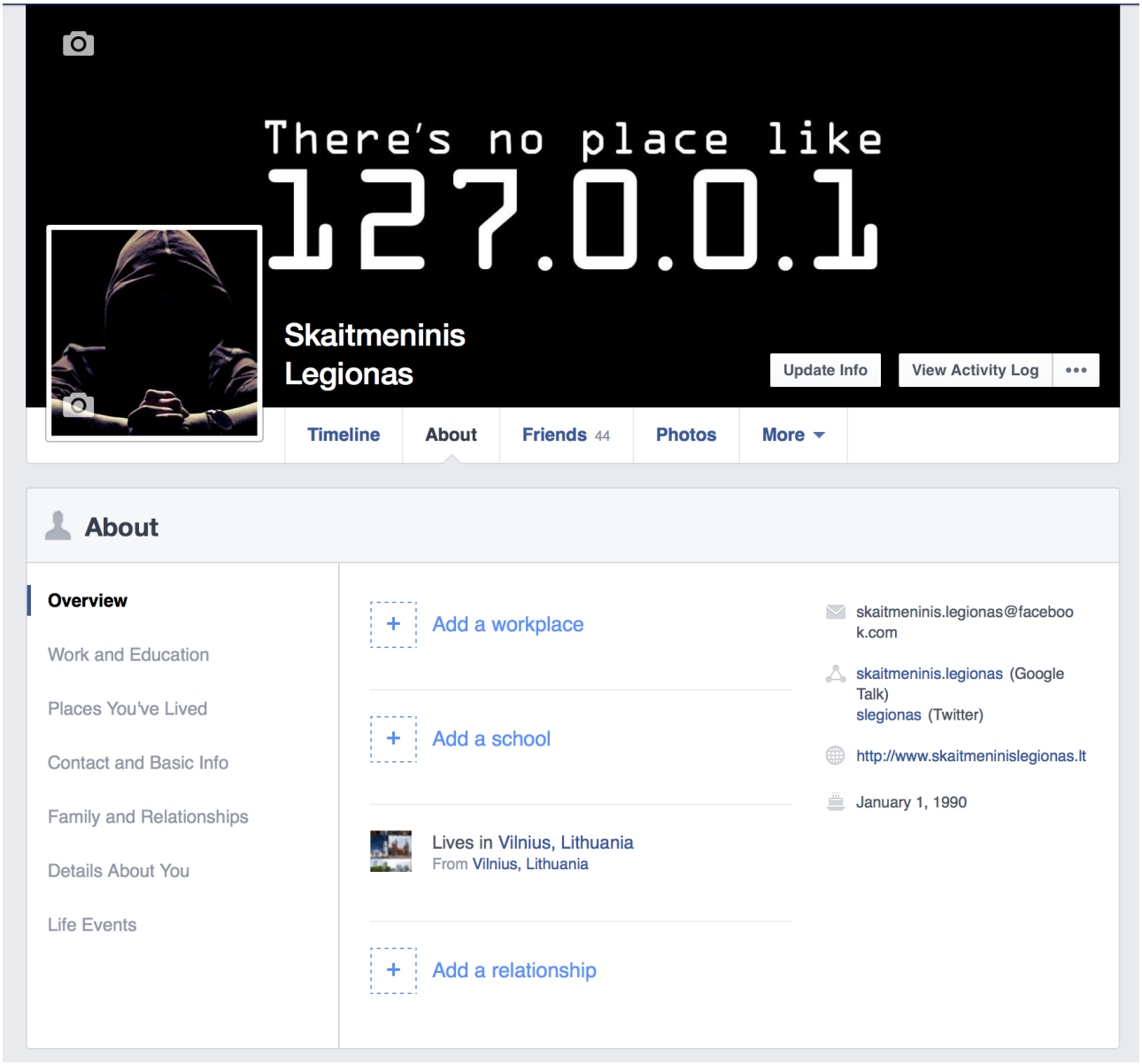
Įkalčių fiksavimo realizavimas (programinio kodo eilučių sk.: 2036)	43 psl.

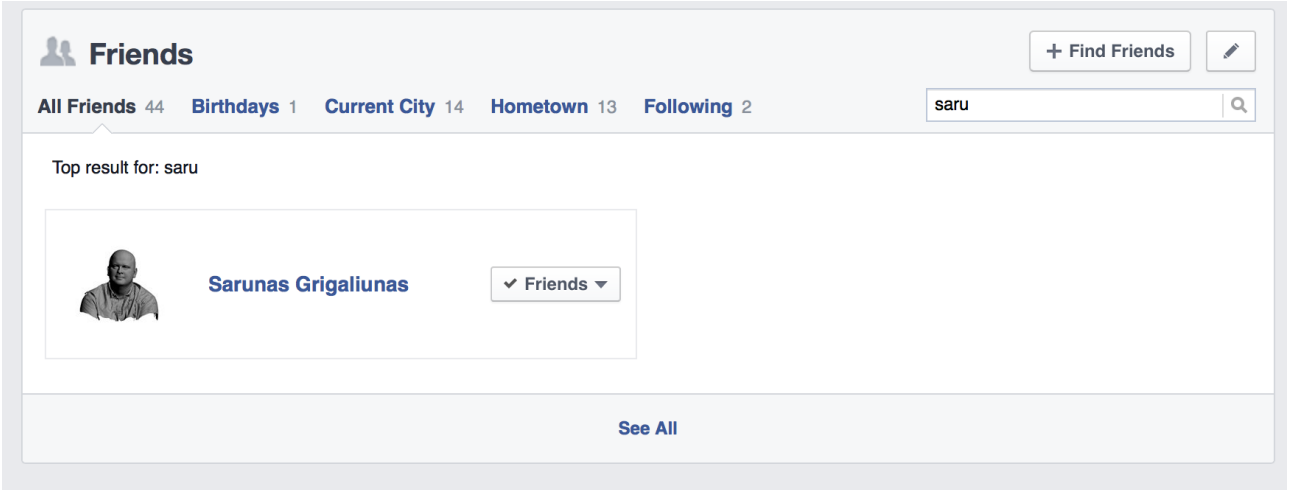
6.3. **priedas. S(i) – socialinio tinklo sąsajumas**

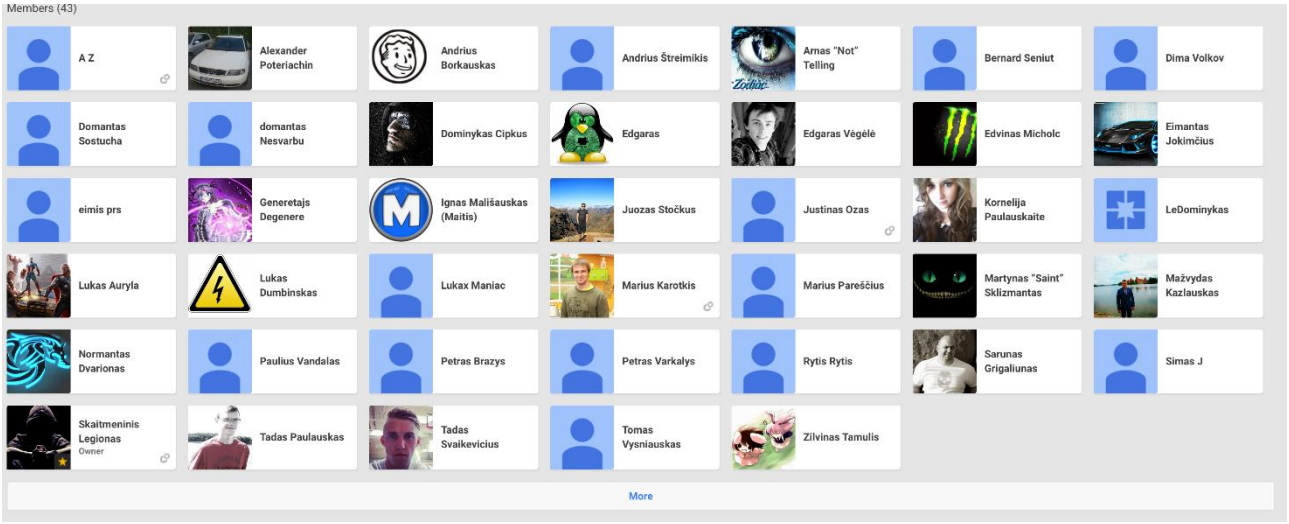


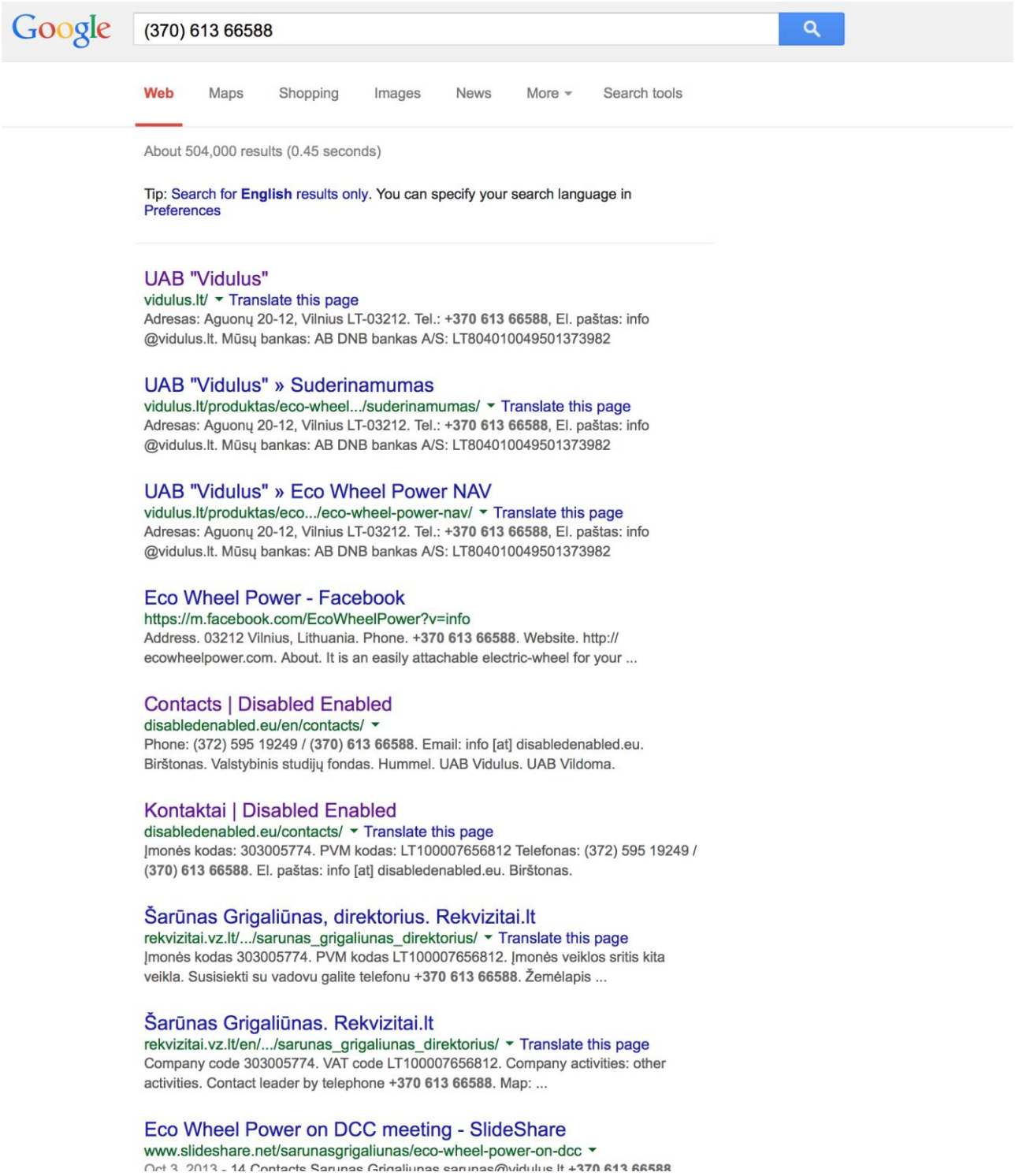
Informacija gauna iš URL įkalčiuose

http://www.facebook.com/sarunas.grigaliunas

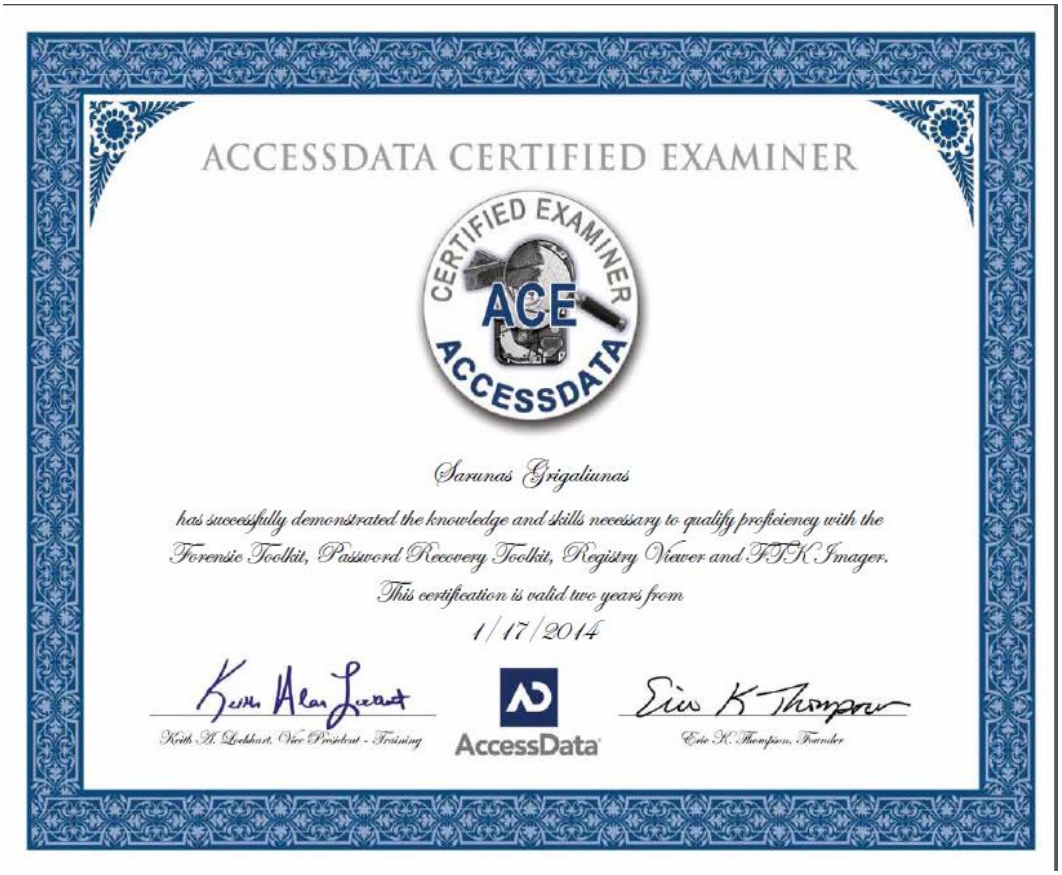

There's no place like
127.0.0.1
Skaitmeninis
Legionas
Update Info
View Activity Log
Timeline
About
Friends 44
Photos
More
About
Overview
Work and Education
Places You've Lived
Contact and Basic Info
Family and Relationships
Details About You
Life Events
Add a workplace
Add a school
Lives in Vilnius, Lithuania
From Vilnius, Lithuania
Add a relationship
skaitmeninis.legionas@facebook.com
skaitmeninis.legionas (Google Talk)
slegionas (Twitter)
http://www.skaitmeninislegionas.lt
January 1, 1990


Friends
+ Find Friends
All Friends 44
Birthdays 1
Current City 14
Hometown 13
Following 2
saru
Top result for: saru
Sarunas Grigaliunas
Friends
See All


Members (43)
A Z
Alexander Poteriachin
Andrius Borkauskas
Andrius Štreimikis
Arnas "Not" Telling
Bernard Seniut
Dima Volkov
Domantas Sostucha
domantas Nesvarbu
Dominykas Cipkus
Edgaras
Edgaras Vėgėlė
Edvinas Micholc
Eimantas Jokimčius
eimis prs
Generetajs Degenere
Ignas Mališauskas (Maitis)
Juozas Stočkus
Justinas Ozas
Kornelija Paulauskaite
LeDominykas
Lukas Auryla
Lukas Dumbinskas
Lukax Maniac
Marius Karotkis
Marius Pareščius
Martynas "Saint" Sklizmantas
Mažvydas Kazlauskas
Normantas Dvarionas
Paulius Vandalas
Petras Brazys
Petras Varkalys
Rytis Rytis
Sarunas Grigaliunas
Simas J
Skaitmeninis Legionas
Owner
Tadas Paulauskas
Tadas Svaikevicius
Tomas Vysniauskas
Zilvinas Tamulis
More


Google
(370) 613 66588
Web
Maps
Shopping
Images
News
More
Search tools
About 504,000 results (0.45 seconds)
Tip: Search for English results only. You can specify your search language in Preferences
UAB "Vidulus"
vidulus.lt/ Translate this page
Adresas: Aguonų 20-12, Vilnius LT-03212. Tel.: +370 613 66588, El. paštas: info @vidulus.lt. Mūsų bankas: AB DNB bankas A/S: LT804010049501373982
UAB "Vidulus" » Suderinamumas
vidulus.lt/produktas/eco-wheel.../suderinamumas/ Translate this page
Adresas: Aguonų 20-12, Vilnius LT-03212. Tel.: +370 613 66588, El. paštas: info @vidulus.lt. Mūsų bankas: AB DNB bankas A/S: LT804010049501373982
UAB "Vidulus" » Eco Wheel Power NAV
vidulus.lt/produktas/eco.../eco-wheel-power-nav/ Translate this page
Adresas: Aguonų 20-12, Vilnius LT-03212. Tel.: +370 613 66588, El. paštas: info @vidulus.lt. Mūsų bankas: AB DNB bankas A/S: LT804010049501373982
Eco Wheel Power - Facebook
https://m.facebook.com/EcoWheelPower?v=info
Address. 03212 Vilnius, Lithuania. Phone. +370 613 66588. Website. http:// ecowheelpower.com. About. It is an easily attachable electric-wheel for your ...
Contacts | Disabled Enabled
disabledenabled.eu/en/contacts/
Phone: (372) 595 19249 / (370) 613 66588. Email: info [at] disabledenabled.eu. Birštonas. Valstybinis studijų fondas. Hummel. UAB Vidulus. UAB Vildoma.
Kontaktai | Disabled Enabled
disabledenabled.eu/contacts/ Translate this page
Įmonės kodas: 303005774. PVM kodas: LT100007656812 Telefonas: (372) 595 19249 / (370) 613 66588. El. paštas: info [at] disabledenabled.eu. Birštonas.
Šarūnas Grigaliūnas, direktorius. Rekvizitai.lt
rekvizitai.vz.lt/.../sarunas_grigaliunas_direktorius/ Translate this page
Įmonės kodas 303005774. PVM kodas LT100007656812. Įmonės veiklos sritis kita veikla. Susisiekti su vadovu galite telefonu +370 613 66588. Žemėlapis ...
Šarūnas Grigaliūnas. Rekvizitai.lt
rekvizitai.vz.lt/en/.../sarunas_grigaliunas_direktorius/ Translate this page
Company code 303005774. VAT code LT100007656812. Company activities: other activities. Contact leader by telephone +370 613 66588. Map: ...
Eco Wheel Power on DCC meeting - SlideShare
www.slideshare.net/sarunasgrigaliunas/eco-wheel-power-on-dcc

6.4. **priedas. Tyrimo metu įgytos kompetencijos siejamos su tyrimo atlikimu**



6.5. **priedas. Straipsniai**

Š. Grigaliūnas, „ELEKTRONINIŲ NUSIKALTIMŲ PĖDSAKŲ IR ĮTARIAMOJO ĮPROČIŲ KORELIACIJA,“ 2015. [Tinkle]. Available: http://www.researchgate.net/publication/276460814_ELEKTRONINI_NUSIKALTIM_%2A_PDSAK_IR_TARIAMOJO_PROI_KORELIACIJA . [Kreiptasi 19 gegužės 2015].

Š. Grigaliūnas, “Intelektuali nuosavybė – turtas kurį irgi reikia saugoti,” Technologija ISSN 1648-1717, p. 83-86, 2006.