KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS

Evaldas Skirgaila

ŠIFRUOTŲ IR SUSPAUSTŲ FAILŲ APTIKIMO METODŲ TYRIMAS

Baigiamasis magistro darbas

Vadovas
Doc. dr. Jevgenijus Toldinas

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS

INFORMATIKOS FAKULTETAS
KOMPIUTERIŲ KATEDRA

ŠIFRUOTŲ IR SUSPAUSTŲ FAILŲ APTIKIMO METODŲ TYRIMAS

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

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

Recenzentas
(parašas) Doc. dr. Ingrida Lagzdinytė-Budnikė
(data)

Projektą atliko
(parašas) Evaldas Skirgaila
(data)

KAUNAS, 2016

KAUNO TECHNOLOGIJOS UNIVERSITETAS

Informatikos fakultetas

(Fakultetas)

Evaldas Skirgaila

(Studento vardas, pavardė)

Informacijos ir informacinių technologijų sauga (kodas 621E10003)

(Studijų programos pavadinimas, kodas)

„Šifruotų ir suspaustų failų aptikimo metodų tyrimas“

AKADEMINIO SĄŽININGUMO DEKLARACIJA

2016 m. _____ mėn. __ d.

Kaunas

Patvirtinu, kad mano **Evaldo Skirgailos** baigiamasis projektas tema „Šifruotų ir suspaustų failų aptikimo metodų tyrimas“ 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)*

Skirgaila, E. „Šifruotų ir suspaustų failų aptikimo metodų tyrimas“. Magistro baigiamasis projektas / vadovas doc. dr. Jevgenijus Toldinas; Kauno technologijos universitetas, Informatikos fakultetas, kompiuterių katedra. Kaunas, 2016. 53 p.

SANTRAUKA

Mes gyvename tokiais laikais, kai kompiuterinės ir kompiuterių tinklų technologijos yra labai paplitusios. Mūsų gyvenimas tampa vis labiau ir labiau priklausomas nuo šių technologijų ir dažnas mūsų sunkiai įsivaizduotų kasdienį gyvenimo ritmą be kompiuterių ir interneto. Paplitus kompiuterių bei interneto technologijoms atsivėrė naujos galimybės vykdyti nusikaltimus ir atsirado naujos nusikaltimų rūšys. Pasaulinis kompiuterių tinklas atveria didžiules galimybes nusikaltėliams. Kasdieną vykdomi elektroniniai nusikaltimai daro didžiulius finansinius nuostolius tiek verslui tiek ir paprastiems vartotojams. Pastaruoju metu kompiuterių ekspertizė labai stipriai pasistūmėjo. Tyrėjai vis geriau supranta kompiuterines technologijas, įgauna vis daugiau patirties tirdami elektroninius nusikaltimus ir labai sparčiai vystoma programinė įranga skirta tirti tokius nusikaltimus.

Vykdant kompiuterinę ekspertizę labai svarbus yra operatyvumas bei efektyvi nusikalstamos veikos įrodymų paieška. Siekiant efektyviai vykdyti elektroninių įrodymų paiešką, skirtingų tipų ir būsenų informacijai reikia suteikti skirtingus prioritetus. Būtent šifruotoje ir suspaustoje informacijoje yra didesnė tikimybė aptikti nusikalstamos veikos įrodymus, todėl kompiuterinės ekspertizės metu prioritetas turi būti skiriamas šifruotos ir suspaustos informacijos paieškai ir identifikavimui.

Magistrinio darbo objektas – programinė įranga, kuri yra skirtas šifruotos ir suspaustos informacijos identifikavimui.

Darbo struktūra:

- Pirmoje darbo dalyje yra rašoma apie elektroninių nusikaltimų fiksavimo ir analizės metodus failų sistemoje. Šioje dalyje yra nagrinėjami elektroniniai nusikaltimai, jų atsiradimas ir augimas. Taip pat pirmoje dalyje yra analizuojama elektroninių nusikaltimų klasifikavimo svarba ir pats klasifikavimas. Šios dalies pabaigoje nagrinėjama kompiuterinė ekspertizė ir visi jos vykdymo etapai.
- Antroje darbo dalyje yra rašoma apie suspaustos ir šifruotos informacijos aptikimo bei atstatymo metodus. Šiame skyriuje yra analizuojama suspausta informacija bei jos suspaudimo metodai ir šifruota informacija bei kriptografiniai metodai.

- Trečioje darbo dalyje yra pateikiamas programinės įrangos skirtos šifruotų ir suspaustų failų identifikavimui projektas. Šioje dalyje yra pateikiami realizuotos programinės įrangos ir joje taikomų metodu aprašymai ir veiklos procesų diagramos.
- Ketvirtoje darbo dalyje yra pateikiami eksperimentiniai tyrimai ir jų rezultatai. Eksperimentinių tyrimų metu buvo nustatyti metodai, kurie leistų identifikuoti suspaustus ar šifruotus failus. Tyrimo metu taip pat buvo ištirtas realizuotos programos veikimas ir nustatyta kaip tiksliai yra identifikuojami suspausti ir šifruoti failai.
- Paskutinėje darbo dalyje yra pateikiamos darbo išvados.

Skirgaila, Evaldas. *Methods for Detecting Encrypted and Compressed Files: Master's* thesis / supervisor assoc. prof. Jevgenijus Toldinas. The Faculty of Informatics, Kaunas University of Technology. Kaunas, 2016. 53p.

Key words: cybercrime, computer crime, digital forensics, information encryption, information compression.

SUMMARY

Nowadays when computers and computer networks are wide spread, our lives become more and more dependent on these technologies. For many people nowadays it's hard to imagine everyday life without computers and internet. When computer networks became mainstream, new ways to commit existing crimes and new crime types arose. World wide web opened up new possibilities for criminals. Cybercrimes are being committed every day and computer crimes are the cause of huge financial losses for business and regular users. Recently computer forensics have been advancing rapidly and cybercrime investigators are becoming more experienced and various tools and applications are being developed to help fighting against cybercrime.

In computer forensics speed and efficiency are very important while looking for digital evidence. In order to effectively carry out investigation, different types of information must be given different priorities. It is more likely to detect evidence of criminal activity within compressed or encrypted files, therefore priority should be given to search and identification of compressed and encrypted information.

The aim of this work is to create a tool, which could identify compressed and encrypted files.

This paper is organized as follows:

- In the first section of the work, we discuss methods for detection of digital evidence in file system. In this section cybercrime, its growth and classification analysis is presented. Finally, in the end of this section we discuss digital forensics and investigation stages.
- In the second section of the work, we discuss methods for detecting and restoring encrypted and compressed files. In this part we also discuss compressed information, information compression, encrypted information and cryptographic methods.
- In the third section of the work, we present description of developed tool and methods used to detect encrypted and compressed files.

- In the fourth section of the work, we present the experiments and their results. During the experiments we studied and determined the methods of detecting compressed and encrypted information, on which developed application was based on. During the experiments we also studied the operation of the application to find out how precisely encrypted and compressed files are identified by the application.
- In the last section of the work, we present the conclusions of the work.

TURINYS

LENTELIŲ SĄRAŠAS

PAVEIKSLŲ SĄRAŠAS

ĮVADAS

Mes gyvename tokiais laikais, kai kompiuterinės ir kompiuterių tinklų technologijos yra labai paplitusios. Mūsų gyvenimas tampa vis labiau ir labiau priklausomas nuo šių technologijų ir dažnas mūsų sunkiai įsivaizduotų kasdienį gyvenimo ritmą be kompiuterių ir interneto. Asmeninių ir nešiojamų kompiuterių, išmaniųjų telefonų, planšečių bei kitų elektroninių įrenginių paplitimas bei paprasta prieiga prie interneto keičia mus ir mūsų gyvenimą – kaip leidžiame laisvalaikį ar dirbame.

Paplitus kompiuterių bei interneto technologijoms atsivėrė naujos galimybės vykdyti nusikaltimus ir atsirado naujos nusikaltimų rūšys. Pasaulinis kompiuterių tinklas atveria didžiules galimybes nusikaltėliams. Kasdieną vykdomi elektroniniai nusikaltimai daro didžiulius finansinius nuostolius tiek verslui tiek ir paprastiems vartotojams. Deja, teisėsaugos agentūros ilgą laiką atsilikinėjo nuo elektroninius nusikaltimus atliekančių asmenų ir nemaža dalis bylų nebūdavo ištirtos. Pagrindinė to priežastis yra tai, kad elektroniniams nusikaltimams nebūdavo skiriama pakankamai dėmesio. Kita didžiulė problema su kuria susidurdavo teisėsaugos pareigūnai ir informacinių technologijų profesionalai buvo programinės įrangos skirtos elektroniniams nusikaltimams tirti trūkumas. Trečiasis dalykas trukdantis ištirti bylas susijusias su elektroniniais nusikaltimais buvo įstatymai - paprastų įstatymų nebuvo galima taikyti elektroniniams nusikaltimams.

Pastaruoju metu kompiuterių ekspertizė labai stipriai pasistūmėjo. Tyrėjai vis geriau supranta kompiuterines technologijas, įgauna vis daugiau patirties tirdami elektroninius nusikaltimus ir labai sparčiai vystoma programinė įranga skirta tirti tokius nusikaltimus. Bene daugiausiai elektroninių nusikaltimų įrodymų yra randama failų sistemoje, todėl failų sistemos analizei reikia skirti daug dėmesio. Failų sistemų dydis nepaliaujamai auga ir norint efektyviai ieškoti nusikaltimų įrodymų reikia taikyti skirtingus informacijos analizės metodus priklausomai nuo informacijos paskirties. Vykdant kompiuterinę ekspertizę labai svarbus yra operatyvumas bei efektyvi nusikalstamos veikos įrodymų paieška. Siekiant efektyviai vykdyti elektroninių įrodymų paiešką, skirtingų tipų ir būsenų informacijai reikia suteikti skirtingus prioritetus. Būtent šifruotoje ir suspaustoje informacijoje yra didesnė tikimybė aptikti nusikalstamos veikos įrodymus, todėl kompiuterinės ekspertizės metu prioritetas turi būti skiriamas šifruotos ir suspaustos informacijos paieškai ir identifikavimui.

Magistrinio darbo tikslas – realizuoti ir ištirti programinį įrankį, kuris padėtų tyrėjui identifikuoti šifruotus bei suspaustus failus.

Darbo tikslui pasiekti iškelti uždaviniai:

- Atlikti elektroninių nusikaltimų fiksavimo ir analizės metodai failų sistemoje analizę;
- Atlikti suspaustos ir šifruotos informacijos aptikimo metodų analizę;
- Remiantis suspaustos iš šifruotos informacijos aptikimo metodų analize atlikti eksperimentinį tyrimą ir nustatyti, kurie metodai leidžia pakankamai tiksliai identifikuoti informacijos būseną;
- Realizuoti programinį įrankį, kuriame būti taikomi metodų tyrimo metu nustatyti metodai;
- Atlikti realizuoto programinio įrankio veikimo tyrimą, kurio metu būtų nustatyta ar teisingai buvo pasirinkti informacijos būsenos aptikimo metodai ir kaip tiksliai yra identifikuojami šifruoti bei suspausti failai;
- Išnagrinėti eksperimentų rezultatus ir pateikti išvadas.

1. ELEKTRONINIŲ NUSIKALTIMŲ FIKSAVIMO IR ANALIZĖS METODAI FAILŲ SISTEMOJE

Modernių technologijų pažanga padėjo daugybei šalių vystyti ir plėsti savo komunikacijų tinklus kartu sudarant sąlygas žymiai greitesniam ir paprastesniam apsikeitimui informacija. Mažiau nei per du dešimtmečius pasaulinis kompiuterių tinklas – internetas išaugo iš sistemos skirtos lengvesniam dalijimuisi informacija tarp mokslininkų ir universitetų į vieną svarbiausių modernaus gyvenimo elementų milijonams žmonių visame pasaulyje. Be socialinės ir ekonominės naudos kompiuterinės technologijos ir internetas labai pakeitė žmonių tarpusavio bendravimą. Kartu su pasaulinio tinklo augimu atsirado ir pradėjo vystytis nusikaltimai elektroninėje erdvėje.

1.1. Elektroninių nusikaltimų apibrėžimas

Elektroniniai nusikaltimai yra labai platus ir bendras terminas, kuris apima visus nusikaltimus atliktus naudojantis kompiuteriu ir internetu. Paprastai elektroniniai nusikaltimai yra laikomi viena iš kompiuterinių nusikaltimų subkategorijų. Elektroniniai nusikaltimai tai tokie nusikaltimai, kai internetas arba koks nors kitoks kompiuterių tinklas yra vienas iš nusikaltimo įgyvendinimo komponentų. Kompiuteriai ir jų tinklai gali būti susiję su nusikaltimais keliais atvejais: naudojami kaip įrankiai atlikti nusikaltimus; gali būti į juos taikomasi vykdant nusikaltimus; gali būti naudojami šalutiniams nusikaltimo tikslams (pvz. saugoti įvairią informaciją susijusią su atliekamais nusikaltimais).

Spartus skaitmeninių technologijų vystymasis bei kompiuterių ir komunikacijos prietaisų susiliejimas pakeitė žmonių bendravimą ir verslą. Nors kompiuterinių technologijų vystymas turėjo labai teigiamą poveikį žmonėms, tačiau yra ir tamsioji pusė. Nusikaltimai seka galimybes ir praktiškai bet kokią pažangą seka atitinkama niša, kuri yra išnaudojama nusikalstamai veikai vykdyti. Elektroninių nusikaltimų terminas gali būti naudojamas apibūdinti labai platų teisės pažeidimų ratą, kuriame yra nusižengimai prieš informaciją ar informacines sistemas (kompiuteriniai įsilaužimai), su kompiuteriai susijęs klastojimas ir sukčiavimas (angl. „phishing“), kompiuterinio turinio nusižengimai (tokie kaip vaikų pornografijos skleidimas) ir autorių teisių nusižengimai (tokie kaip nelegalaus piratinio turinio skleidimas) [1].

Elektroninė bankininkystė ir pardavimai internetu sukuria geras sąlygas sukčiavimui. Elektroninė komunikacija tokia kaip elektroniniai laiškai arba trumposios SMS žinutės gali būti ir yra naudojamos žmonių persekiojimui bei priekabiavimui. Elektroninio turinio pasidalinimo paprastumas privedė prie didžiulio autorių teisių pažeidinėjimo skleidžiant nelegalų

skaitmeninį turinį. Nuolat didėjantis žmonių priklausomumas nuo kompiuterių ir skaitmeninių tinklų paverčia pačias technologijas nusikaltėlių taikiniu: siekiant gauti privačią informaciją arba padaryti kuo didesnę žalą. Nauja nusikaltimų kategorija „kompiuteriniai nusikaltimai“ atsirado panašiu metu kai kompiuteriai paplito ir tapo plačiai naudojami [1].

Bendrai paėmus, kompiuteriai atlieka vieną iš trijų rolių nusikaltimuose: nusikaltimų objektai, nusikaltimų subjektai, nusikaltimų įrankiai. Kompiuteriai yra nusikaltimų objektai, kai jie būna sugadinami arba pavogiami. Yra gausybė atvejų kai kompiuteriai buvo sušaudyti, susprogdinti, sudeginti, sudaužyti, suspardyti ar suspausti. Padaryta žala gali būti tyčinė ir netyčinė, kaip pavyzdžiui užkliudytas ir nuverstas kompiuteris, ko pasėkoje jame saugoma informacija yra sugadinama ar bent jau tampa neprieinama. Kompiuteriai užima nusikaltimų subjektų rolę, kai jie yra ta aplinka, kurioje yra vykdomas nusikaltimas. Į šia kategoriją patenka kompiuterinių virusų atakos. Trečioji kompiuterių rolė nusikaltimuose yra kompiuterių kaip įrankių panaudojimas. Tai apima melagingos informacijos kūrimą, nusikalstamos veikos planavimą bei nusikalstamos veikos kontroliavimą [1].

Elektroniniams nusikaltimams galima priskirti nusikaltimus pradedant kompiuteriniu sukčiavimu, informacijos vagyste ir klastojimu, baigiant privatumo pažeidimais, žalingo turinio skleidimu bei organizuotu nusikalstamumu. Įstatymuose dažnai būna tam tikri elektroninių nusikaltimų apibrėžimai, tačiau jie ne visada teisingai apibrėžia elektroninius nusikaltimus. Kartais įstatymuose iš viso nebūna konkrečių elektroninių nusikaltimų apibrėžimo ir tada teisėsaugos agentūroms pačioms tenka spręsti apie elektroninius nusikaltimus, o galiausiai teismai padaro galutinį sprendimą. Vienas iš daugiausiai kritikos susilaukiančių kompiuterinių nusikaltimų apibrėžimų priklauso Jungtinių Amerikos Valstijų teisingumo departamentui. Kritikos šis apibrėžimas susilaukia dėl to, kad yra per daug platus. Jungtinių Amerikos Valstijų teisingumo departamentas kompiuterinius nusikaltimus apibrėžia taip: „Kompiuterinis nusikaltimas yra bet koks teisės pažeidimas, kuriam pasiruošti, tirti arba vykdyti baudžiamąjį persekiojimą yra naudojamos kompiuterinės technologijos“. Pagal tokį apibrėžimą praktiškai bet kokį nusikaltimą galima laikyti kompiuteriniu nusikaltimu vien dėl to, kad detektyvas tyrimo metu vykdė paiešką kompiuteriu duomenų bazėje [1].

Vienas iš faktorių, kurie lemia tai, kad nėra paprasto ir aiškaus kompiuterinių nusikaltimų apibrėžimo yra jurisdikcijos problema. Įstatymai skirtingose jurisdikcijose terminus apibrėžia skirtingai, o tai yra svarbu teisėsaugos pareigūnams bei kompiuterių tinklų administratoriams, kurie nori dalyvauti elektroninių nusikaltimų, vykdytų prieš jų administruojamus tinklus, baudžiamajame persekiojime, nes jie turi susipažinti su taikomais įstatymais [1].

Viena didžiausių problemų adekvačiai apibrėžiant elektroninius nusikaltimus yra konkrečios statistinės informacijos trūkumas apie teisės nusižengimus susijusius su kompiuterinėmis technologijomis bei kompiuterių tinklais. Kadangi ne visi elektroniniai nusikaltimai būna aptinkami, o dalis jų būna nuslepiami siekiant, kad pasklidusi informacija nepakenktų įmonės įvaizdžiui, tai turima statistika rodo daug mažesnį nusikaltimų, susijusių su kompiuterių tinklais, skaičių nei yra iš tiesų [1].

Dažnu atveju įstatymų leidėjai elektroniniais nusikaltimais laiko paprastus nusikaltimus, kurie kaip nors yra susiję su kompiuterių tinklu. Kompiuterių tinklai suteikia nusikaltėliams naujas galimybes vykdyti jau egzistuojančias nusikalstamas veikas. Įstatymai kurie draudžia šias nusikalstamas veikas taip pat gali būti taikomi žmonėms, kurie naudojo kompiuterius ar kompiuterių tinklus vykdyti tuos pačius nusikaltimus. Tačiau be naujų galimybių vykdyti egzistuojančias nusikalstamas veikas, su kompiuterių tinklų paplitimu atsirado ir unikalių nusikaltimų. Vienas tokių pavyzdžių gali būti įsilaužimas į kompiuterius ir kompiuterines sistemas. Kompiuterinius įsilaužimus galima lyginti su įsilaužimu į namus ar įmonės patalpas, tačiau elementai, kurie suteikia galimybes neteisėtai pakliūti į kompiuterių sistema ir fizines patalpas yra visiškai skirtingi [1].

Dešimtojo Jungtinių Tautų Organizacijos kongreso metu buvo pasiūlytas elektroninių nusikaltimų apibrėžimas padalintas į dvi dalis: [1]

1. siaurąja prasme: bet kokia nelegali veika, kuriai vykdyti yra naudojamos elektroninės operacijos ir kuri yra nukreipta prieš kompiuterinių sistemų saugą bei jomis apdorojamą informaciją.
2. plačiąja prasme: bet kokia nelegali veika, kuriai vykdyti yra naudojamos kompiuterinės sistemos arba kompiuterių tinklai įskaitant tokias nusikalstamas veikas kaip nelegalios informacijos saugojimas ir platinimas pasitelkiant kompiuterines sistemas ir tinklus.

Elektroniniai nusikaltimai, pagal šiuos apibrėžimus, siejami su kompiuteriais ir tinklais. Elektroninių nusikaltimų termine žodis „elektroniniai“ paprastai reiškia naujas nelegalias veikas, kurios atsirado dėl informacinių technologijų paplitimo arba tradicines nelegalias veikas, kurios vykdyti buvo pasitelkta elektroninė erdvė.

1.2. Elektroninių nusikaltimų problemos augimas

Žinant kiek elektroninių nusikaltimų yra įvykdoma galima geriau nustatyti kiek lėšų reikia išleisti elektroniniam saugumui. Saugumo ekspertų vertinimu kasmet padaroma elektroninių nusikaltimų žala siekia nuo 555 milijonų iki 13 milijardų dolerių, tačiau nėra konkrečios elektroninių nusikaltimų padaromos žalos statistikos, nes nėra žinoma kiek kartų

apie tokius nusikaltimus būna nepranešama. Net ir žinantys dėl elektroninių nusikaltimų patirtą žalą asmenys ar įmonės dažniausiai siekia ją nuslėpti. Šių nusikaltimų aukos paprastai patirtų dar didesnę žalą pranešdamos apie prieš jas įvykdytus elektroninius nusikaltimus. Įkalčių paruošimas, darbuotojų paruošimas liudijimui teisme, teisiniai mokesčiai, padidėjusios draudimo išlaidos, pažeidžiamumų bei saugos spragų atskleidimas, visa tai gali būti pranešimo apie įvykdytus elektroninius nusikaltimus pasekmė [1].

Kaip kiekvienas prekybos ir komunikacijų aspektas buvo pakeistas atsiradus internetui, taip ir nusikaltimai pasikeitė, kad nusikaltėliai galėtų pasipelnyti iš milijonų potencialių prie pasaulinio tinklo prisijungusių aukų. Elektroninių nusikaltimų augimą lemia įvairios priežastys. Pirmiausiai tai technologijos naudojamos vykdyti elektroninius nusikaltimus tapo lengviau prieinamos. Įvairiausia programinė įranga, kuri yra skirta ieškoti atvirų tinklo sąsajų arba apeiti slaptažodžius bei vykdyti kitokią nelegalią veiką tinkle, gali būti nesunkiai surandama ir įsigyjama internete. Tokie įrankiai leidžia žymiai platesniam žmonių ratui vykdyti nusižengimus negu tik tiems asmenims, kurie gerai išmano kompiuterius ir programavimą. Elektroniniai nusikaltimai taip pat labai sparčiai auga todėl, kad terpė, kurioje jie yra vykdomi nuolat eksponentiškai didėja. Internetas tampa prieinamas vis didesniam žmonių ratui, nuolat didėjantis susisiekimas tarp žmonių ir naujų prie pasaulinio tinklo prijungtų technologijų skaičiaus didėjimas reiškia tai, kad nuolat didėja ir potencialių elektroninių nusikaltimų aukų skaičius. Lyginant su kitais nusikaltimais ir nusižengimais, elektroniniams nusikaltimams vykdyti paprastai reikia mažesnių investicijų, o jie vykdomi gali būti iš įvairiausių vietų nepaisant geografinių suvaržymų ar sienų tarp šalių [1].

1.3. Elektroninių nusikaltimų klasifikavimas

Terminas elektroniniai nusikaltimai yra toks platus ir viską apimantis, kad jį būtina suskirstyti į kategorijas. Nusikaltimų klasifikavimas yra naudingas todėl, kad padeda surūšiuoti konkrečius veiksmus, kurie buvo atlikti vykdant nelegalią veiklą, į grupes. Turint nusikaltimų kategorijas galima vesti vykdomų nusikaltimų statistiką, o tada įvairios teisėsaugos agentūros gali formuoti padalinius, kovojančius su tam tikrais nusikaltimų tipais. Taip pat teisėsaugos pareigūnai gali specializuotis tam tikroje nusikaltimų kategorijoje ir tapti tos kategorijos nusikaltimų ekspertais [2].

Daugumą įprastinių nusikaltimų būtų galima priskirti elektroniniams nusikaltimams ir tai labai trukdo norint suklasifikuoti elektroninius nusikaltimus kaip galima siauresnėmis kategorijomis. Labai svarbu yra atskirti nusikaltimus kuriuos atliekant gali būti naudojami kompiuterių tinklai ir nusikaltimus kurių be kompiuterių tinklų atlikti neįmanoma. Pastarieji

nusikaltimai tai yra tokie nusikaltimai kaip įsilaužimas į privačius kompiuterius ir konfidencialios informacijos pavogimas, internetinių puslapių vykdančių prekybinę veiklą nulaužimas, įsilaužimas į elektroninės bankininkystės paslaugas teikiančių svetainių serverius. Nors ir sudėtinga, tačiau būtina suskirstyti elektroninius nusikaltimus į kategorijas, nes tai labai padeda teisėsaugos agentūroms nustatyti kokių nusikaltėlių reikia ieškoti [2].

1.4. Elektroninių nusikaltimų kategorijos

Kalbant apie elektroninius nusikaltimus paprastai jie yra skirstomi į dvi dideles kategorijas: kompiuteriai prijungti prie tinklo yra nusikaltėlių taikiniai; kompiuteriai prijungti prie tinklo yra panaudojami vykdant neteisėtą veiką. Į pirmąją elektroninių nusikaltimų kategoriją patenka visi nusikaltimai, kurių taikiniai yra prie tinklo prijungti kompiuteriai. Ši kategorija apima nusikaltimus, kurių tikslas yra pažeisti kompiuteriuose saugomos informacijos konfidencialumą, vientisumą arba prieinamumą. I antrąją elektroninių nusikaltimų kategoriją patenka tradiciniai teisės nusižengimai, tokie kaip informacijos vagystė, sukčiavimas ir klastojimas, kuriems vykdyti buvo pasitekti prie tinklo prijungti kompiuteriai arba kompiuterių tinklai [2].

Elektroniniai nusikaltimai yra labai platus terminas todėl įvairios valstybinės bei nevalstybinės organizacijos, kurių veikla yra susijusi su kova su elektroniniais nusikaltimais interpretuoja įvairiai. Neretai elektroniniai nusikaltimai būna skirstomi kitaip - į dvi grupes: nusikaltimai, kuriuos vykdo smurtautojai arba potencialiai smurtaujantys asmenys ir nusikaltimai, kuriuos vykdo nesmurtaujantys asmenys [2].

1.4.1. Smurtautojų arba potencialiai smurtaujančių asmenų vykdomi nusikaltimai

Tiriant elektroninius nusikaltimus smurtautojų arba potencialiai smurtaujančių asmenų vykdomi nusikaltimai turi didesnį prioritetą nei nesmurtaujančius asmenų vykdomi nusikaltimai, nes tokie nusikaltimai kelia fizinį pavojų asmenims ar asmenų grupėms. Šie nusikaltimai gali būti skirstomi į smulkesnes kategorijas: elektroninis terorizmas, grasinimas susidoroti, elektroninis persekiojimas, vaikų pornografija [2].

Terorizmas tai organizuotų grupuočių sistemingas grasinimas ar smurto naudojimas prieš civilius asmenis siekiant ideologinių tikslų. Elektroninių terorizmu vadinamas toks terorizmas, kuris yra planuojamas, koordinuojamas ir vykdomas elektroninėje erdvėje naudojantis kompiuteriniais tinklais. Šiai kategorijai yra priskiriamas susirašinėjimas elektroniniais laiškais planuojant teroro aktus, asmenų verbavimas per internetines svetaines. Taip pat elektroninio terorizmo kategorijai galima priskirti oro erdvės kontrolės centro kompiuterinių sistemų nulaužimą siekiant, kad susidurtų arba sudužtų lėktuvai, vandens

valymo įrenginių kompiuterinių sistemų nulaužimas siekiant užteršti geriamąjį vandenį bei elektros tiekimo sutrikdymas siekiant vasarą sutrikdyti oro kondicionavimo sistemas arba žiemą sutrikdyti šildymo sistemas [2].

Grasinimai susidoroti gali būti siunčiami elektroniniais laiškais. Šių nusikaltimų tikslas priversti žmones bijoti dėl savo ar savo artimųjų sveikatos bei gyvybės. Šiai kategorijai taip pat galima priskirti ir grasinimus susprogdinti įmones arba valstybines įstaigas [2].

Elektroninis persekiojimas tai tokia elektroninio priekabiavimo forma, kai auka gauna daug žinučių elektroninėje erdvėje arba elektroninių laiškų su įvairiausiais grasinimais, kurie kelia aukai baimę ir galiausiai gali pavirsti į fizinį persekiojimą bei kelti realią grėsmę [2].

Vaikų pornografija apima įvairius aspektus: asmenys, kurie kuria šią medžiagą pasinaudodami nepilnamečiais vaikais; asmenys, kurie platina šią medžiagą; asmenys, kurie siunčiasi šią medžiagą. Vaikų pornografija yra laikoma smurtiniu nusikaltimu net jei niekas neturėjo fizinio kontakto su nepilnamečiais, nes tokiai medžiagai sukurti buvo išnaudojami vaikai [2].

1.4.2. Nesmurtaujančių asmenų vykdomi nusikaltimai

Didžioji dalis elektroninių nusikaltimų yra nesmurtaujančių asmenų vykdomi nusikaltimai todėl, kad šiems nusikaltimams įvykdyti yra naudojama elektroninė erdvė ir nereikalingas joks fizinis kontaktas. Trys kompiuterių tinklų savybės kurios daro elektroninę erdvę patrauklią asmenims vykdantiems nusikaltimus yra pakankamai didelis anonimiškumas, sunkus susekamumas ir virtualumas (nusikaltimui įvykdyti nereikia jokio fizinio kontakto). Nesmurtaujančių asmenų vykdomi nusikaltimai gali būti skirstomi į smulkesnes kategorijas: elektroninis įsiveržimas, elektroninė vagystė, elektroninis sukčiavimas, naikinantis elektroninis nusikaltimas, kiti elektroniniai nusikaltimai [2].

Elektroninio įsiveržimo metu, asmenys nulaužę asmeninių kompiuterių ar kompiuterinių tinklų apsaugą įgauna neautorizuotą prieigą prie kompiuterių ar privačių kompiuterių tinklų išteklių, bet nenaudoja šių išteklių savo tikslams ir negadina jiems prieinamos informacijos. Paprastai tokie asmenys į tinklus įsilaužia norėdami sau ar kitiems įrodyti, kad gali tai padaryti. Gavę prieigą prie kompiuterių tinklo jie skaito elektroninius laiškus ir dokumentus, žiūri kokia programinė įranga yra įdiegta bei kokius internetinius puslapius lankė tikrieji kompiuterių savininkai, bet niekur nenaudoja ir neskelbia šios informacijos. Nepaisant to šie veiksmai yra laikomi elektroniniais nusikaltimais [2].

Elektroninė vagystė yra vienas dažniausiai pasitaikančių elektroninių nusikaltimų, nes vagystė atneš ją vykdančiam asmeniui finansinės naudos bei bus vykdoma per atstumą, o tai

labai sumažina vagystės aptikimo ir asmens, vykdančio elektroninę vagystę, sugavimo galimybę. Galima išskirti kelias smulkesnes elektroninės vagystės kategorijas: grobstymas, neteisėtas pasisavinimas, industrinis šnipinėjimas, plagijavimas, piratavimas, tapatybės vagystė, DNS podėlio nuodijimas [2].

Grobstymas, tai yra pinigų ar kitų asmeniui patikėtų vertybių pasisavinimas. Neteisėtas pasisavinimas, tai yra panašu į grobstymą, bet skirtumas tas, kad asmeniui nebuvo patikėtas turtas, o asmuo, gavęs neautorizuotą prieigą prie kompiuterių tinklo, pervedė pinigus ar pakoregavo dokumentus ir taip neteisėtai pasisavino jam nepriklausantį turtą. Industrinis šnipinėjimas, tai yra kai asmuo, pasinaudodamas kompanijos tinklu, pavagia kompanijos komercines paslaptis, finansinę informaciją, klientų sąrašus, prekybos strategijas ar kitą informaciją, kuri padėtų tą kompaniją sužlugdyti arba suteiktų kitoms kompanijoms konkurencinį pranašumą. Plagijavimas, tai yra kito asmens ar asmenų sukurto darbo vagystė ir pateikimas kaip savo sukurto darbo. Piratavimas, tai yra neleistinas autorinių teisių saugomų objektų tokiu kaip programinė įranga, muzika, filmai, menas, knygos ir panašiai kopijavimas, kuris neigiamai finansiškai paveikia asmenis, kuriems priklauso autorinės teisės. Tapatybės vagystė, tai yra toks elektroninis nusikaltimas, kai naudojantis internetu yra nelegaliai gaunama privati informaciją apie asmenį, kuri gali būti naudojama atliekant kitus elektroninius nusikaltimus arba įgyti aukai priklausantį turtą. DNS podėlio nuodijimas, tai yra viena neautorizuoto perėmimo formų, kai yra pakoreguojamas domenų vardų sistemos podėlis ir taip tinklu keliaujantys duomenys nukreipiami į nusikaltėlių serverį [2].

Elektroninės vagystės yra labai susijusios su elektroniniu sukčiavimu, o kartais ir sutampa. Tai tampa akivaizdu kai susiduriama su elektroniniu sukčiavimu, kurio pasekmė yra neteisėtas turto pasisavinimas. elektroninis sukčiavimas tai asmenų ar įstaigų apgaudinėjimas siekiant pasisavinti ką nors vertingo. Tai yra labai panašu į elektroninę vagystę, tačiau šiuo atveju auka savanoriškai atiduoda nusikaltėliams vertybes ar turtą, kurių nebūtų atidavus jei nebūtų patikėjusi nusikaltėlių melu. Elektroninio sukčiavimo schemos dažnai sutampa su paprasto sukčiavimo schemomis, tačiau naudojantis internetu gali daug kartų padidinti sukčiavimo mastus. Elektroninis sukčiavimas gali įgauti kitą formą – neteisėtas kompiuterių tinkle esančios informacijos koregavimas siekiant gauti naudos [2].

Naikinančių elektroninių nusikaltimų terminas apima nusikaltimus, kurių metu yra sutrikdomas kompiuterių tinklų paslaugų teikimas arba sugadinama, sunaikinama kompiuteriuose saugoma informacija. Tokius nusikaltimus galima suskirstyti į smulkesnes kategorijas: įsilaužimas į kompiuterių tinklą ir informacijos ištrynimas; įsilaužimas į interneto svetainių serverius ir juose saugomų puslapių sudarkymas; kompiuterio arba kompiuterių tinklo

apkrėtimas virusais, kirminais arba kitokiu kenkėjišku kodu; atsisakymo teikti paslaugas (DoS) atakos vykdymas su tikslu neleisti vartotojams naudotis tinklo resursais [2].

Kiti nesmurtiniai elektroniniai nusikaltimai, kurie nepatenka į anksčiau minėtas kategorijas ir kurie gali būti vykdomi nesinaudojant internetu yra: prostitucijos paslaugų ieškojimas arba siūlymas internetu; internetiniai lošimai; narkotinių medžiagų pardavimas internetu; elektroninis pinigų plovimas; elektroninė kontrabanda [2].

1.5. Kompiuterių ekspertizė

Šiais laikais, kai žmonės yra priklausomi nuo technologijų labiau nei bet kada, dauguma žmonių kas dieną susiduria su elektroninėmis technologijomis (elektroniniai laiškai ir žinutės, elektroninė bankininkystė, skaitmeninė muzika bei filmai ir pan.). Ši priklausomybė turi pasekmių ir kitose gyvenimo srityse, kur ji yra ne taip akivaizdžiai pastebima. Viena tokių sričių yra teisėsauga, o konkrečiau – nusikaltimų tyrimas. Istoriškai nusikaltimų tyrimuose vyravo tokios sąvokos kaip fiziniai įrodymai, įvykių liudininkai ir nusikaltėlių prisipažinimai, tačiau šiais laikais nusikaltimų tyrėjams tenka pripažinti, kad nemaža įrodymų dalis yra skaitmeninio pavidalo. Didelės dalis nusikaltimų šiais laikais yra vykdoma kompiuteriais, kuriuose gali būti saugoma daug nelegalios veiklos įrodymų. Kompiuterių teismo ekspertizė nors ir dar labai nauja mokslo šaka, tačiau labai aktyviai vystosi – kuriami metodai ir taisyklės, kad būtų užtikrinta jog tyrimo metu nebus praleisti jokie skaitmeniniai nelegalios veiklos įrodymai bei surasti asmenys vykdę tą veiklą [2].

1.5.1. Mokslinio metodo taikymas kompiuterinei teismo ekspertizei

Skaitmeninių įrodymų analizė labai priklauso nuo tiriamo nusikaltimo konteksto bei tyrėjo žinių, patirties bei kruopštumo. Nors kiekviena analizė turi skirtingus aspektus priklausomai nuo tiriamų duomenų, tyrimo tikslų ir turimų išteklių, tačiau tyrimo eiga iš esmės visad išlieka ta pati [3].

Informacijos surinkimas ir pastebėjimų užfiksavimas. Tyrimo pradžioje tikrinamas surinktų duomenų vientisumas ir autentiškumas bei apžvelgiami duomenys norint nustatyti kaip efektyviausiai būtų galima tęsti analizę. Taip pat šiame žingsnyje atliekamas duomenų apdorojimas siekiant surasti ištrintus duomenis, išfiltruoti tyrimui nesvarbius duomenis bei išgauti surinktos informacijos meta duomenis [3].

Hipotezės suformavimas pasitelkiant tyrimo pradžioje užfiksuotas pastabas. Daromos prielaidos apie vykdytą nelegalią veiklą atsižvelgiant į surinktus skaitmeninius įrodymus. Nors tokiems spėjimams nemažai įtakos turi tyrėjo žinios ir patirtis, tačiau reikia atsiriboti nuo išankstinio nusistatymo ir vadovautis faktais [3].

Hipotezės vertinimas. Įvairiausi spėjimai gali išsivystyti iš suformuotos hipotezės ir tyrėjas privalo nustatyti, ar yra pakankamai įrodymų patvirtinančių tuos spėjimus. Analizės rezultatai priklauso nuo to kaip nuodugniai buvo patikrinta suformuota hipotezė, todėl yra svarbu apsvarstyti visus galimus variantus ir pabandyti paneigti hipotezę. Jei surinkti įrodymai nepatvirtina pirminės hipotezės reikia ją iš naujo apsvarstyti. Padaromos išvados pagal anksčiau surinktą informaciją ir perduodami rasti įrodymai. Kai yra nustatomi galimi įvykių, susijusių su nusikalstama veika, paaiškinimai, tyrėjai perduoda visą surinktą informaciją teisėsaugos pareigūnams [3].

Mokslinis metodas yra ciklinis, o tai reiškia, kad tyrėjai turi pakartoti žingsnius vis iš naujo, kol gali padaryti išvadas. Jei surinkti duomenys nepatvirtina hipotezės, tai nauja hipotezė yra formuojama ir patikrinama. Net jei surinkta informacija patvirtina hipotezę, atsiradus naujiems duomenims yra būtina patikrinti ir nustatyti, ar hipotezė vis dar pasitvirtina. Naudojant mokslinį metodą paprastai yra išvengiama neteisingų išvadų, nes tik tikrinant, ar teorija pasitvirtina, nebandant jos paneigti, padidina klaidingų išvadų šansą [3].

1.6. Kompiuterinės teismo ekspertizės vykdymas

Vykdomi tyrimai gali būti susiję su įvairiausiais elektroniniais nusikaltimais, tačiau yra nemažai tyrimo elementų yra bendri visiems tyrimams. Vykdant kompiuterinę teismo ekspertizę reikia manyti, kad šio proceso rezultatai ir rasti skaitmeniniai įrodymai atsidurs teisme, kur gali būti bandoma juos užginčyti. Būtent todėl tyrimo metu yra svarbu laikytis nustatytų procedūrų [2].

Po nusikaltimo vietos apsaugojimo ir pirminės liudininkų apklausos tyrėjai surenka, apsaugo ir perveža įrodymus. Visi rasti įrodymai prieš jų tyrimą, įskaitant ir skaitmeninius įrodymus rastus kietuosiuose kompiuterių diskuose ir kituose įrenginiuose, turi būti įvertinti. Tyrimo metu dokumentacijas yra vienas iš esminių dalykų, nes visus atliktus veiksmus reikia surašyti į galutinę ataskaitą. Kompiuterinė teismo ekspertizė yra ilgas procesas, kurio metu svarbu laikytis procedūrų, kad nebūtų praleisti svarbūs įrodymai arba surinkti įrodymai nebūtų atmesti teismo metu [2].

1.6.1. Kompiuterinės ekspertizės vykdymo etapai

Kompiuterinė ekspertizė yra sudėtingas procesas, kurį gali labai apsunkinti tyrimo vykdymas verslo aplinkoje kur kompiuterinės sistemos yra esminė verslo dalis ir todėl negali būti išjungiamos. Esant tokiai situacijai reikia sekti visas ekspertizės procedūras, bet tuo pačiu ir nešvaistyti laiko svarstant kokių veiksmų paskiau imtis. Tyrimo metu atliekant žemiau paminėtus etapus eilės tvarka yra užtikrinama, kad įvykęs incidentas nepavirs dar didesne

problema ir bus pasiekti tyrimo tikslai. Šeši kompiuterinės ekspertizės vykdymo etapai: pasiruošimas, aptikimas, izoliavimas, panaikinimas, atstatymas, vėlesnis tyrimas [2].

1.6.2. Pasiruošimas

Kaip ir kitose srityse, kurios yra siejamos su saugumu, vienas svarbiausių dalykų yra tai, kad grėsmės būtų pašalintos ir užkirstas kelias joms kilti ateityje. Jei reagavimo į incidentą metu reagavimo komanda neturės reagavimo strategijos, procedūrų ar reikalingų įrankių, tada bus švaistomas laikas bandant viską suorganizuoti. Pasiruošimas yra tyrimo pagrindas. Reagavimo komanda turi būti kvalifikuota, komandos nariai – mokėti identifikuoti ir panešti apie problemas bei mokėti atlikti visas užduotis, kurias tikimasi, kad jie atliks [2].

Avarinės situacijos metu svarbi informacija kuri turėtų būti prieinama reagavimo komandai yra sistemos slaptažodžiai ir kritinės šifruotos informacijos šifravimo raktai, kurie suteiktų prieigą prie visos sistemos. Po incidento tyrimo įmonė toliau vykdys veiklą, todėl reguliariai kuriant atsargines duomenų kopijas incidento metu pakeistą, sugadintą arba ištrintą informaciją būtų galima atstatyti. Incidentų aptikima galima supaprastinti registruojant visus sistemos įvykius. Kuo daugiau informacijos yra užregistruojama apie įvykius sistemoje, tuo daugiau įrodymų apie incidentus turės reagavimo komanda ir atitinkamai galės į juos reaguoti. Normaliai veikiančios sistemos parametrai tokie kaip tinklo duomenų srautas, atminties bei procesoriaus panaudojimas taip pat tūrėtų būti registruojami, kad būtų galima juos palyginti su sistemos parametrais įtariamo incidento metu ir taip aptikti incidento įrodymus [2].

1.6.3. Aptikimas

Antrasis kompiuterinės ekspertizės etapas yra aptikimas, kurio metu bandoma nustatyti, ar yra įvykę incidentai. Vien dėl to, kad kažkas pranešė apie incidentą dar nereiškia, kad jis tikrai įvyko. Šiame etape yra tiriami tokie pranešimai ir nustatoma, ar reikia imtis tolimesnių veiksmų. Aptikimo etape yra peržiūrimi sistemos įvykių registrai ir nustatoma, ar buvo atlikti nepageidaujami veiksmai sistemoje. Sistemos įvykiu registravimas turi būti pradėtas kaip galima anksčiau, nes šie įrašai gali padėti patvirtinti liudininkų parodymus. Kita priežastis, kam reikalingi įvykių žurnalai, yra ta, kad jie gali padėti nustatyti veiksmų šabloną. Jei programišiai bando į sistemą įsilaužti kelis kartus tada, nustačius įvykių sekos pasikartojimus, galima aptikti sistemos pažeidžiamumus arba išsiaiškinti kas nori įsibrauti į sistemą. Taip pat įvykių sekos pasikartojimas gali atskleisti blogai apmokytus darbuotojus, kurie nuolat daro tas pačias klaidas. Be įvykių registracijos, dalies incidentų, piktavališkų ar netyčinių, aptikti neįmanoma [2].

Kai yra aptinkamas incidentas, tai pirmas veiksmas yra padaryti pažeistos sistemos kietojo disko kopiją ir tada ją tirti. Tiriama yra kietojo disko kopija, o ne originalus kietasis diskas, nes tyrimo metu gali būti modifikuota informacija. Vien tik atveriant įvairius elektroninius dokumentus yra modifikuojami tu dokumentų meta duomenys tokie kaip paskutinio atvėrimo data ir tai gali neigiamai paveikti tolesnį tyrimą. Taip pat svarbu padaryti kietojo disko kopija kuo anksčiau todėl, kad visa informacija yra tarsi užkonservuojama ir jei bus bandoma vėl įsibrauti į sistemą su tikslu pašalinti pėdsakus to padaryti nepavyks [2].

1.6.4. Izoliavimas

Nustačius, kad į sistemą buvo įsibrauta vienas svarbiausių tikslų yra sistemos izoliavimas. Izoliuojant pažeistus sistemos kompiuterius yra apsaugomi kiti tinklo kompiuteriai ir įsibrovėliai negali pasiekti kitų sistemos kompiuterių bei jų pažeisti. Kaip vyks izoliavimas priklauso nuo incidento tipo, kokie tinklo kompiuteriai buvo pažeisti ir kokia yra pažeistų kompiuterių svarba visai sistemai. Jei buvo įsilaužta į tinklo failų serverį, tai logiškas spendimas yra pašalinti pažeistą serverį iš tinklo ištraukiant tinklo kabelį. Tai padarius įsilaužėliai nebegalėtų padaryti daugiau žalos failų serveriui ar pašalinti įsilaužimo pėdsakų. Kitu atveju, jei įmonės darbuotojas siuntinėja grasinančius elektroninius laiškus, tai neleisti visiems įmonės darbuotojams naudotis komunikacijų paslaugomis būtų per daug stipri izoliavimo priemonė. Tokiu atveju suradus šį asmenį reikėtų nebeleisti naudotis kompiuteriu ir jį prižiūrėti, kad nebandytų pasišalinti iš įvykio vietos kol atvažiuos policija [2].

1.6.5. Pašalinimas

Incidento priežasties pašalinimas, kad ateityje jis vėl nepasikartotų yra lygiai tiek pat svarbus kaip ir incidento izoliavimas. Pašalinimo metu yra panaikinama grėsmės priežastis, kad nebūtų daroma žala kompiuterių sistemai. Įvykdžius šį kompiuterinės ekspertizės etapą, kompiuterių sistema tampa saugesnė ir yra išvengiama grėsmės pasikartojimų ateityje. Pašalinimą galima įvykdyti naudojant įvairius metodus. Jei sistemoje buvo aptiktas kompiuterinis virusas, tai yra nuskanuojama visa sistema su antivirusine programine įranga ir pašalinamas virusas. Situacijose kuriose yra pažeidžiami įstatymai arba įmonės politika yra imamasi griežtų veiksmų – atleidžiamas darbuotojas arba jam pateikiami kaltinimai. Pašalinimo metodas priklauso nuo to kas yra grėsmės priežastis [2].

1.6.6. Atstatymas

Po incidento aptikimo, izoliavimo ir pašalinimo eina atstatymo etapas. Šio etapo tikslas yra užtikrinti, kad visa informacija, programinė įranga ir kompiuterinės sistemos būtų atstatytos į normalią būseną. Taip pat šiame etape yra nustatoma, ar kokie nors sistemos

elementai nebuvo neatstatomai pažeisti bei ar atstatyta sistema veikia taip pat kaip ir prieš incidentą. Atstatymas yra svarbus, nes incidento metu informacija galėjo būti modifikuota, sugadinta arba ištrinta bei pakeista sistemos konfigūracija. Neatstačius informacijos yra rizikuojama, kad sistemoje liks įsilaužimo metu įkeltas kenkėjiškas programinis kodas. Toks kodas ateityje gali būti aktyvuotas įvykus tam tikriems įvykiams sistemoje arba nustatytu laiku, kai bus manoma, jog sistema nėra pažeista. Dėl galimų grėsmių ateityje reikia nustatyti, ar sistemai padaryta žala buvo pilnai pašalinta. Atstatymą galima vykdyti įvairiais būdais. Vienais atvejais sistemos gali būti iš naujo sukonfigūruojamos, patikrinamas informacijos vientisumas. Kitais atvejais sistemas reikia atstatinėti iš atsarginių kopijų. Jei kokia nors informacija buvo sugadinta, ištrinta arba modifikuota, tai atstačius sistemą yra prarandama visa informacija, kuri buvo patalpinta sistemoje po paskutinio atsarginės kopijos darymo [2].

1.6.7. Vėlesnis tyrimas

Vėlesnio tyrimo metu yra nustatoma, ar galima pagerinti incidentų tyrimo procedūras. Šiame etape yra tiriami prieš tai buvę kompiuterinės ekspertizės etapai ir apžvelgiamas kas bei kodėl buvo atlikta. Šio tyrimo metu analizuojamos detalės yra: pasiruošimas tyrimui bei ar yra reikalingas papildomas pasiruošimas; komunikacijos kokybė bei ar visa reikiama informacija buvo pasiekiama laiku; tyrimo metu atlikti veiksmai ir nustatytos problemos; incidento aptikimo greitis bei tikslumas; kaip gerai buvo izoliuotas incidentas; tyrimui atlikti naudoti įrankiai [2].

Įmonėms svarbu nustatyti kiek kainavo incidentas ir padaryti pakeitimus biudžete, kad būtų efektyviai pašalinamos rizikos susijusios su atitinkamais incidentais. Incidento kaina susideda iš įmonės prastovų, darbuotojų atlyginimo, prarastos informacijos vertės, sugadintos kompiuterinės įrangos ir kitų su tyrimu susijusių išlaidų [2].

2. SUSPAUSTOS IR ŠIFRUOTOS INFORMACIJOS APTIKIMO METODAI

Kriptografiniai metodai yra naudojami žmonių ar įmonių konfidencialiai informacijai apsaugoti. Yra daug aplinkybių, dėl kurių reikia imtis papildomos apsaugos – būtinybė apsaugoti komercines paslaptis, įmonės klientų ir darbuotojų duomenis ir panašiai. Tačiau tie patys kriptografiniai metodai gali būti ir yra naudojami nusikaltėlių, kurie bando paslėpti juos inkriminuojančius duomenis. Atliekant kompiuterinę ekspertizę yra svarbu atkreipti dėmesį į suspaustą bei šifruotą informaciją, nes didesnė tikimybė, kad būtent tarp šifruotų ir suspaustų failų yra nusikalstamos veikos pėdsakų bei įrodymų. Tyrimo metu reikia nustatyti, ar tiriama informacija yra suspausta, ar šifruota, nes turint tokią informaciją apie failus, galima taikyti atitinkamus metodus bandant juos išskleisti arba iššifruoti.

2.1. Suspaustos informacijos atstatymas

Šiais laikais, kai suspausti failai yra labai plačiai paplitę, jie, be abejonės, yra svarbus inkriminuojančių duomenų šaltinis tyrėjams. Kompiuterinėje ekspertizėje informacijos atstatymo metodai yra labai reikšmingi, nes jie leidžia išgauti informaciją, kuri teisme gali tapti skaitmeniniais nusikalstamos veikos įrodymais. Failų atstatymas yra viena pamatinių kompiuterinės ekspertizės proceso sudedamųjų dalių. Taip yra todėl, kad kompiuterinėje ekspertizėje svarbus yra kiekvienas potencialių skaitmeninių įrodymų šaltinis, net jei duomenys iš pirmo žvilgsnio atrodo nesuprantami ir neperskaitomi. Neabejotinai, nustatyti originalaus nesuspausto kompiuterinio failo formatą yra sudėtinga. Formato nustatymą sunkina aukštas informacijos entropijos lygis, kuris yra gerai žinomas suspaustų kompiuterinių failų požymis. Suspaustiems failams atstatyti yra sukurta įvairiausių tiek komercinių, tiek ir atvirojo kodo taikomųjų programų, tačiau ne visus suspaustus failus lengva atstatyti. Tai padaryti ypač sunku, jei yra sugadintos tokių failų antraštės, kuriose yra aprašytos visų suspaustų informacijos blokų pozicijos. Sugadintų suspaustų failų atstatymo problemą bent iš dalies galima spręsti taikant „bitas po bito“ metodą, kai yra iš eilės yra tikrinami visi bitai ir pašalinami visi sugadinti. Toks metodas leidžia atstatyti dalį nesugadintos informacijos, kuri buvo saugoma suspaustame faile.

2.2. Šifruotos informacijos atstatymas

Kriptografijos taikymas lėmė kriptoanalizės atsiradimą. Kriptoanalizė – tai procesas, kurio metu yra dešifruojami šifruoti failai. Kriptoanalizė nors ir yra kriptografijos priešingybė, tačiau kriptoanalizė papildo kriptografiją, nes geras kriptoanalizės supratimas leidžia kurti saugesnius kriptografijos metodus. Kriptografinėje sistemoje paprastai silpniausia sistemos vieta yra slaptažodis ar raktas. Tokiu atveju yra naudojama nuoseklios paieškos metodas –

grubios jėgos ataka, kai yra išbandomi visi galimi slaptažodžio ar rakto variantai. Simetrinio rakto kriptografijai yra naudojami tiesinės ir diferencinės kriptoanalizės metodai. Kriptoanalizėje egzistuoja tam tikri limitai: jei šifravimui naudotas raktas yra ne trumpesnis nei šifruojamas tekstas, tai tokio teksto kriptoanalizė yra neįmanoma. Taip pat jei šifravimui naudotas raktas yra pakankamai sudėtingas ir ilgas, tai priimtiną laiko tarpą dešifravimas tampa neįmanomas.

Kriptoanalizės metodai:

1. **Žinomo teksto analizė.**
   Kai kriptoanalitikui yra žinoma nešifruoto teksto dalis, kuri buvo užšifruota žinomu šifru, tai kartais yra įmanoma nustatyti šifravimo raktą analizuojant šifruotą tekstą.
2. **Diferencialinė kriptoanalizė.**
   Kai kriptoanalitikui yra žinoma nešifruoto teksto dalis, šifravimo raktas gali būti nustatomas lyginant šifruotą tekstą su nešifruotu.
3. **Šifruoto teksto analizė.**
   Kai kriptoanalitikui yra žinomas tik šifruotas tekstas.
4. **Laiko / energijos sąnaudų analizė.**
   Kai kriptoanalitikas matuoja energijos sąnaudų pokyčius tol, kol yra vykdomas šifravimas ir bando nustatyti šifro rakto skaičiavimus.
5. **Rakto perėmimo (žmogaus viduryje) ataka.**
   Kriptoanalitikas apgauna abi suinteresuotas puses ir priverčia jas persiųsti savo šifravimo raktus joms manant, kad yra vykdomas apsikeitimas raktais.

2.3. Šifruotų failų atskyrimas nuo suspaustų failų

Metodai, kurie yra skirti atskirti šifruotą informaciją nuo suspaustos yra dar tik ankstyvoje stadijoje ir jie turi būti tobulinami. Analizuotoje literatūroje minimi tyrimų rezultatai yra nepakankami, o tyrimų sritis yra laikoma sudėtinga. Informacijos būsenos tyrimų rezultatai dažniausiai remiasi pasikartojančiomis informacijos struktūromis failuose, tačiau suspaustuose ir šifruotose failuose nėra pasikartojančių informacijos struktūrų. Jei suspausti failai turi pasikartojančių informacijos struktūrų, tai tokie failai nėra suspausti maksimaliai ir juos galima dar labiau suspausti. Jei šifruotose failuose yra pasikartojančių informacijos struktūrų, tai jie tampa pažeidžiami kriptoanalizei. Dėl šių priežasčių, bandant identifikuoti suspaustus ir šifruotus failus, reikia tirti tokius metodus, kurie nesiremia pasikartojančiomis informacijos struktūromis failuose.

Viename iš analizuotoje literatūroje minimų tyrimų, pasitelkiant NIST statistinių testų paketą, buvo analizuojami įvairūs suspausti ir šifruoti failai, tiriant informacijos atsitiktinumą juose. Tyrimo metu buvo nustatyta, kad nei vienas iš suspaustų failų nebuvo identifikuotas kaip atsitiktinė informacija. Siekiant išvengti dalies kriptoanalizės atakų, kuriant saugius šifravimo algoritmus vienas iš svarbiausių tikslų yra tai, kad tais algoritmais šifruota informacija būtų matematiškai neatskiriama nuo atsitiktinės informacijos.

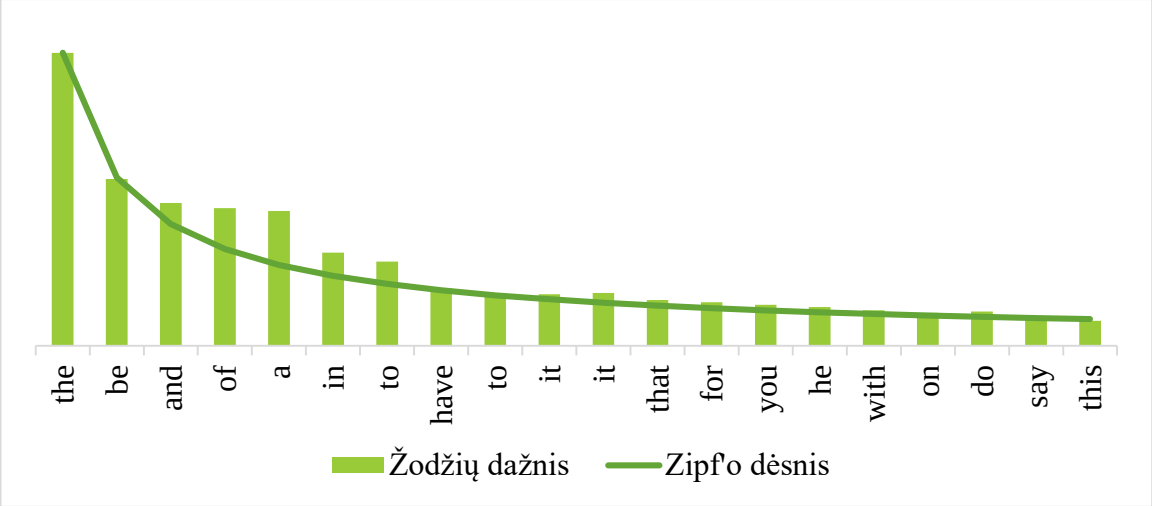
Vėliau tyrimo metu įvairiais algoritmais buvo užšifruoti ir suspausti septyni 100 megabaitų dydžio failai. Visi šie failai buvo tiriami naudojant visus 188 NIST statistinių testų paketo testus. Tokio masto tyrimas leido gerai atskirti šifruotus failus nuo suspaustų. Šio tyrimo rezultatai veda prie hipotezės, kad yra įmanoma atskirti šifruotus failus nuo suspaustų tiriant juose esančios informacijos atsitiktinumą.

Atsitiktine bitų seka gali būti laikoma tik tada, kai jos negalima suspausti. Bet koks failas, kuris negali būti suspaustas ir dar nėra suspaustas, ko gero yra šifruotas, todėl ir nėra įmanoma suspausti šifruotos informacijos. Tačiau suspaudimo algoritmuose turi būti kompromisas tarp suspaudimo lygio ir suspaudimo greičio. Praktiškai nei vienas failas nebūna optimaliai suspaustas ir tai reiškia, kad visi suspausti failai gali būti suspaudžiami dar labiau. Ši suspaustų failų savybė leidžia atskirti suspaustus failus nuo šifruotų, taikant statistinius, failuose saugomos informacijos, testus.

2.4. Informacijos entropija

Nustatyti šifruotus ir suspaustus failus galima pagal juose saugomos informacijos entropiją. Entropija informacijos moksle yra informacijos tankis arba, kitaip sakant, – kiek reikia vidutiniškai bitų viename baite saugoti naują nežinomą informaciją. Kuo labiau atsitiktinė informacija – tuo entropija yra arčiau aštuonių bitų baite.

Kompiuterinėse sistemose atsitiktinė informacija yra saugoma tik išimtiniais atvejais, nes paprastai saugoti atsitikinę informaciją kompiuteriuose nėra jokio tikslo. Kompiuterinėse sistemose saugomi tiek vartotojų, tiek ir operacinės sistemos failai turi tam tikrą struktūrą ir turinį. Visa informacija, nepaisant jos formato, paklūsta Zipfo dėsniui (žr. 1 pav.), kuris skelbia, kad dažniausiai sutinkamų žodžių ar objektų pasikartojimo tikimybė yra neįprastai didelė ir šie žodžiai bei objektai užima neproporcingai didelę viso turinio dalį.



***1 pav**. Dažniausiai naudojami anglų kalbos žodžiai ir Zipfo dėsnis.*

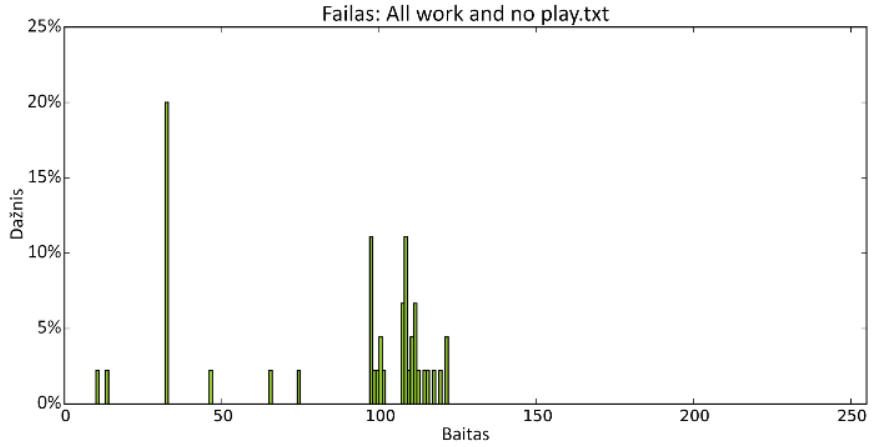
Paprastų failų, lyginant su šifruotais ir suspaustais, entropija yra mažesnė būtent dėl Zipfo dėsnio, nes dalis informacijos pasikartoja. Maža informacijos entropija reiškia, kad ją galima smarkiai suspausti ir todėl suspausto failo entropija yra didesnė už paprasto failo. Šifruojant informaciją yra siekiama ją paslėpti, kad iš šifruotos informacijos nebūtų įmanomą atstatyti informacijos be šifravimo rakto, o tai reiškia, kad šifruotų failų entropija yra labai didelė. Taip pat dėl šios priežasties norint suspausti ir paslėpti informaciją pirmiausiai reikia ją suspausti ir tik tada šifruoti, nes priešingu atveju šifruotos informacijos suspausti nepavyks.

2.5. Suspausta informacija

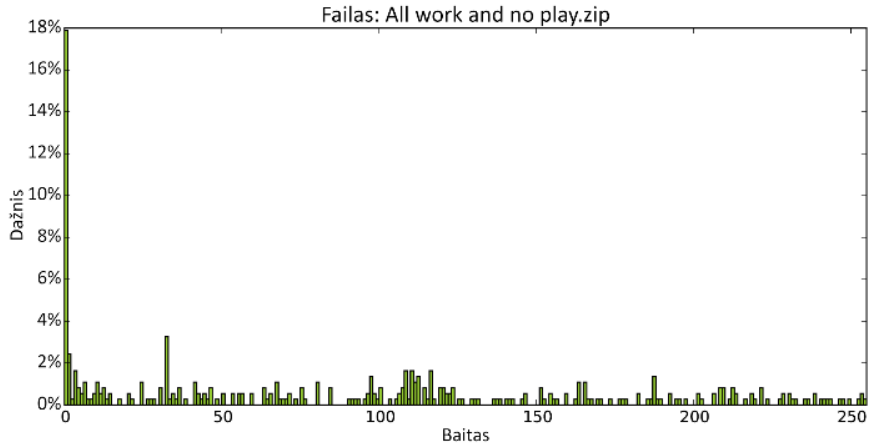
Entropija yra visada susijusi su tam tikru modeliu. Ji yra ne konkrečios bitų eilutės, bet galimų bitų eilučių ypatybė. Modelis, kuris suteikia mažiausią entropiją konkrečiai bitų eilutei, geriausiai nuspėja tos eilutės bitų reikšmes ir todėl gali labiausiai suspausti juose saugomą informaciją. Suspaustuose failuose yra saugoma: modelis, kuris buvo naudojamas suspausti informaciją ir jo parametrai (jei tokių yra) bei pagal tą modelį suspausta informacija.

Informacijai suspausti skirta programinė įranga dažniausiai naudoja vienokią ar kitokią Lempel–Zivo algoritmo variaciją. LZ algoritmai yra naudojami suspausti informaciją jos neprarandant ir todėl ją galima visiškai atstatyti išskleidžiant. LZ algoritmai yra paremti prisitaikančiu žodynu. Informacijos suspaudimas yra pasiekiamas visą pasikartojančią informaciją pakeičiant nuorodomis į tą informaciją žodyne. Nuorodos į informaciją žodyne yra saugomos poslinkio nuo informacijos pradžios pavidalu. Būtent dėl pasikartojančios informacijos pakeitimo nuorodomis į žodyną, suspausta informacija tampa labiau atsitiktinė ir padidėja jos entropija. Žemiau pateikti du pavyzdžiai. Viršutinis grafikas yra tekstinio failo (449998 baitų dydžio), kuriame yra dešimt tūkstančių eilučių su tekstu „All work and no play

makes Jack a dull boy.“ entropijos grafikas (žr. 2 pav.). Apatinis grafikas yra to paties tik jau suspausto failo (369 baitų dydžio) entropijos grafikas (žr. 3 pav.). Suspaudžiant informaciją buvo naudotas „zip“ archyvas, „ultra“ suspaudimo lygmuo ir „LZMA“ suspaudimo metodas.



2 pav. *Tekstinio failo entropijos grafikas*



3 pav. *Suspausto failo entropijos grafikas*

2.6. Kriptografija

Šifravimas yra procesas, kurio metu yra naudojami šifravimo algoritmai ir šifravimo raktai, o šio proceso metu informacija tampa užšifruota – prieinama tik asmenims ar taikomosioms programoms, kurios turi šifravimo raktus. Saugiai užšifruotos informacijos neįmanoma atskleisti neturint šifravimo rakto. Yra dvi šifravimo algoritmų kategorijos: simetriniai ir asimetriniai šifrai. Simetrinis algoritmas naudoja ta patį šifravimo raktą tiek informacijos šifravimui, tiek ir jos dešifravimui. Simetriniai šifravimo algoritmai yra labai greiti, tačiau jie apsunkina dalijimąsi šifruota informacija. Taikant simetrinį šifravimą reikia visiems suinteresuotiems asmenims atskleisti tą patį šifravimo raktą arba kiekvieną kartą naudoti vis kitą šifro raktą. Dalinimasis simetriniu šifru šifruota informacija yra apsunkinamas,

nes negalima atšaukti prieigos tam tikram asmeniui nepakeičiant bendro šifravimo rakto, o kiekvienam asmeniui šifruojant informaciją vis kitais raktais yra eikvojama disko vieta.

Asimetriniai šifravimo algoritmai naudoja skirtingus, tačiau tarpusavyje susijusius, šifravimo bei dešifravimo raktus. Paprastai naudojant asimetrinį šifravimą vienas raktas yra paskelbiamas viešai, o kitas yra laikomas paslaptyje. Dėl šios priežasties viešojo rakto šifravimo sistemos yra plačiai taikomos. Jos gali būti taikomos pasiekti du skirtingus tikslus: užtikrinti informacijos konfidencialumą arba jos autentiškumą. Kai informacija yra užšifruojama viešuoju raktu ir ją dešifruoti galima tik slaptuoju, tai yra užtikrinamas informacijos konfidencialumas, nes tokią informaciją gali perskaityti, tik asmenys turintys atitinkamą slaptąjį raktą. Kai informacija yra užšifruojama privačiuoju raktu, tai yra užtikrinamas informacijos autentiškumas, nes tokią informaciją gali perskaityti bet kas pasinaudojęs viešai skelbiamu raktu, tačiau užšifruoti gali tik asmenys turintys atitinkamą privatųjį raktą. Taikant asimetrinius šifravimo algoritmus yra supaprastinamas dalinimasis šifruota informacija, tačiau šie šifravimo algoritmai yra lėtesni nei simetriniai šifrai.

Simetriniai ir asimetriniai šifravimo algoritmai turi tiek pranašumų, tiek ir trūkumų – simetriniai šifrai yra žymiai spartesni, o asimetriniai šifrai leidžia naudoti viešojo rakto infrastruktūrą bei apsikeitimo raktais sistemas. Siekiant pasinaudoti abiejų sistemų pranašumais buvo sukurta hibridinė šifravimo sistema, kurioje yra taikomi simetriniai ir asimetriniai šifravimo algoritmai.

Šifravimo ir dešifravimo procesai hibridinėje šifravimo sistemoje:

1. Siuntėjas sugeneruoja simetrinio šifravimo raktą ir juo užšifruoja konfidencialią informaciją;
2. Siuntėjas užšifruoja simetrinį raktą asimetriniu šifravimo algoritmu;
3. Užšifruota konfidenciali informacija bei užšifruotas simetrinio šifro raktas siunčiami gavėjui;
4. Gavėjas iššifruoja simetrinio šifro raktą su savo privačiuoju raktu;
5. Gavėjas dešifruoja jam skirtą konfidencialią informaciją su dešifruotu simetrinio šifro raktu.

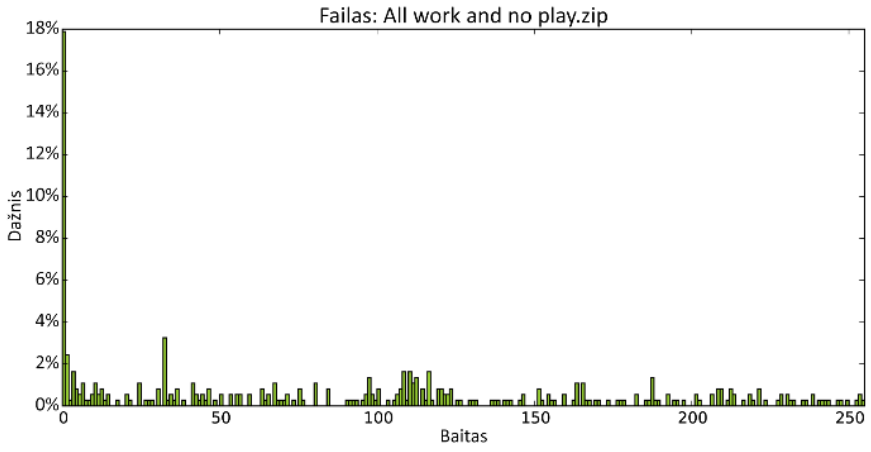
Naudojant hibridinę šifravimo sistemą yra išvengiama lėto šifravimo proceso, nes asimetriniu šifravimo algoritmu šifruojamas santykinai labai nedidelis duomenų kiekis – simetrinio šifro raktas. Tai reiškia, kad didžioji duomenų dalis yra šifruojama žymiai spartesniu simetriniu šifravimo algoritmu. Tuo pačiu yra išlaikomas šifruotos informacijos pasidalinimo paprastumas, nes yra naudojama viešojo rakto kriptografinė bei raktų apsikeitimo sistemos.

2.7. Šifruota informacija

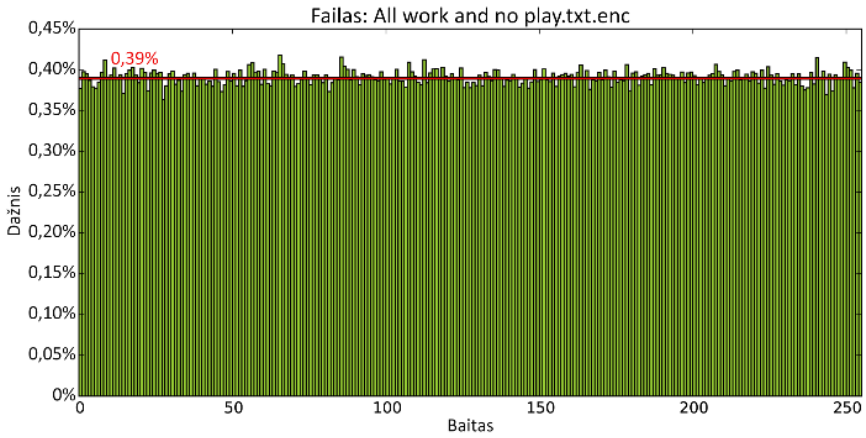
Šifravimas yra procesas, kai informacija yra užkoduojama taip, kad būtų perskaitoma tik asmenims, kurie turi šifravimo raktą ir perėmus tokią informaciją be šifravimo rakto ji išlieka konfidenciali. Teoriškai, pasitelkiant įvairias šifro atakas galima atskleisti šifruotos informacijos turinį, tačiau jei informacija yra tinkamai užšifruota su pakankamai ilgais raktais, tai jos atskleidimas tampa praktiškai neįmanomas per priimtiną laiko tarpą.

Kriptografijoje unikalumo atstumu yra vadinamas šifruoto teksto ilgis, kuris yra reikalingas nulaužti šifrą, sumažinant netikrų šifro raktų skaičių iki nulio kai yra vykdoma grubios jėgos ataka (angl. Brute-force attack). Šis atstumas priklauso nuo pasikartojančios informacijos šifruojamame tekste. Siekiant apsunkinti šifro nulaužimą reikia padidinti šifruojamos informacijos unikalumo atstumą. Prieš informacijos šifravimą atlikus informacijos suspaudimą ne tik reikės šifruoti mažiau informacijos, bet ir tokio šifro nulaužimas bus labai apsunkintas.

Kaip prieš tai esančiame skyriuje buvo rašyta, šifruojant informaciją, pagrindinis tikslas yra ją palėpti, kad iš šifruotos informacijos nebūtų galima nustatyti originalios informacijos ar kokių nors jos požymių. Dėl šios priežasties šifruotos informacijos entropija yra labai aukšta ir artima aštuoniems bitams baite. Informacijos entropijos matavimas bitais baite nusako kiek vidutiniškai reikia bitų viename baite saugoti visą naudingą informaciją faile. Visiškai atsitiktinės informacijos entropija yra aštuoni bitai baite. Tekstinio failo, kuriame yra dešimt tūkstančių eilučių su tekstu „All work and no play makes Jack a dull boy.“ Entropija yra 3.997 bitai baite, to paties suspausto failo entropija yra 6.366 bitai baite, o šio failo šifruoto AES256-CBC šifru entropija yra 7.9996 bitai baite. Žemiau bus patiekti to pačio suspausto ir šifruoto failo entropijos grafikai.



4 pav. *Suspausto failo entropijos grafikas*



5 pav. *Šifruoto failo entropijos grafikas*

Iš entropijos grafikų matosi, kad šifruota informacija yra labai panaši į atsitiktinę. Skaičiuojant informacijos entropiją visi failo bitai yra padalijami po aštuonis ir tada kiekvienam baitui pagal lentelę yra priskiriamas vienas iš 256 simbolių. Visiškai atsitiktinės informacijos atveju visų 256 simbolių dažnis būtų 0,39% (1/256*100%).

2.8. Kompiuterinė ekspertizė ir duomenų šifravimas

Šifravimo technologijų taikymas kompiuterių apsaugai auga, o tai apsunkina darbą, kompiuterių ekspertizę atliekantiems, tyrėjams. Taip yra dėl to, kad neturint dešifravimo rakto, negalima naudoti jokių įrankių skirtų nusikalstamos veikos įrodymų paieškai. Šifravimo technologijų taikymas turi didelį poveikį kompiuterinei ekspertizei. Tyrėjai gali dirbti tik su ta informacija, kuri jiems yra prieinama. Jei visas kietasis diskas yra šifruotas, tai tyrėjai negali prieiti prie tame kietajame diske saugomos informacijos ir tyrimas praktiškai tampa neįmanomas. Tyrimo metu tyrėjas pirmiausiai turi nustatyti šifravimo technologijų taikymą ir apimtį tiriamame kietajame diske. Silpni slaptažodžiai gali būti nulaužiami, tačiau, jei vartotojas naudojo stiprų slaptažodį, tai slaptažodžio nulaužimas, pasitelkiant grubios jėgos atakas, yra negalimas. Gali būti ir kitokia situacija, kai kietajame diske yra šifruoti tik tam tikri failai ir jų nešifruotos kopijos saugomos kitose disko vietose. Taip pat gali būti, kad vartotojas turi įprotį naudoti tą patį slaptažodį ar slaptažodžių rinkinį visiems šifruojamiems failams. Tokius slaptažodžių rinkinius paprastai nesunku aptikti tiriamoje sistemoje.

Vartotojams yra prieinama gausybė įrankių skirtų pilnam kietojo disko šifravimui, disko dalies šifravimui arba individualių failų šifravimui. Jei tiriamas kietasis diskas nėra pilnai šifruotas, tai galima ieškoti individualiai šifruotų failų. Jei kietajame diske yra aptikta tam tikra programinė įranga skirta failų šifravimui, tai tyrėjas gali tikėtis diske surasti šifruoto turinio. Kompiuterinės ekspertizės metu aptikęs failų šifravimui skirtus įrankius tyrėjas gali išsiaiškinti

kaip dažnai ir kada buvo tais įrankiais pasinaudota, o tai veda prie failų, kurie buvo sukurti arba atidaryti panašiu metu, paieškos.

Aptikus šifruotą informaciją, sekantis tyrėjo veiksmas yra bandymas išsiaiškinti koks yra dešifravimo raktas. Labai dažnai žmonės iš įpročio arba dėl patogumo naudoja vieną ar kelis slaptažodžius visiems šifruojamiems failams, prisijungimui prie interneto puslapių ir panašiai. Tokius slaptažodžius yra nesunku aptikti tiriamoje sistemoje. Vienas tokių pavyzdžių yra interneto naršyklės, kurios automatiškai saugo vartotojo slaptažodžius. Tokios slaptažodžių saugyklos paprastai yra nesunkiai įveikiamos. Tyrėjai turi daugiau galimybių atkurti tam tikro tipo failus. Kompiuteriuose paprastai yra saugoma nemažai nereikalingų failų – tam tikros programos, darbo metu, sukuria laikinas modifikuojamų failų kopijas bei atsargines failų kopijas, kurios nebūna užšifruojamos šifruojant originalų failą. Taip pat dalis šifravimo įrankių šifravimo metu sukuria laikinus failus, kurie būna ištrinami baigus šifravimą, tačiau ištrintus failus galima atstatyti. Ne visada galima rasti nešifruotas šifruotų failų kopijas, tačiau tyrėjai gali ir turi ieškoti nešifruotų kopijų visuose susijusiuose įrenginiuose.

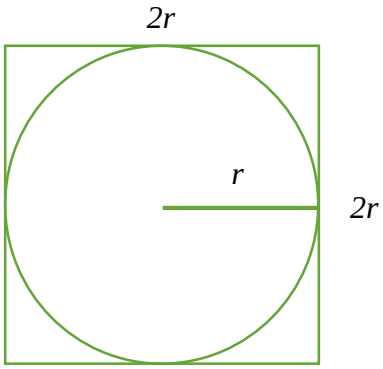
2.9. Monte Karlo metodas Pi aproksimacijai

Monte Karlo metodai – tai yra grupė skaičiavimo algoritmų, kurie yra pagrįsti statistiniu modeliavimu ir gautų rezultatų apdorojimu statistiniais metodais. Monte Karlo metodai yra naudojami, kai nėra konkrečiai žinomi tyrimo įvesties duomenys. Taikant Monte Karlo metodus įvesties duomenys priklauso tam tikram galimų įvesčių intervalui. Skaičiavimai pasitelkiant kompiuterius atliekami šimtus ar tūkstančius kartų (priklausomai nuo sprendžiamos problemos) vis su kitomis įvesčių intervalo reikšmėmis, todėl ir išvestis yra ne konkreti reikšmė, bet galimų reikšmių intervalas. Nors ir yra įvairių Monte Karlo metodų, tačiau paprastai juos galima suskirstyti į keturis etapus:

1. Įvesties reikšmių srities, intervalo apibrėžimas;
2. Sugeneruojamos atsitiktinės reikšmės iš įvesties reikšmių intervalo;
3. Atliekami deterministiniai skaičiavimai su sugeneruotomis reikšmėmis;
4. Atliekama gautų rezultatų suvestinė.

Monte Karlo metodą taikant Pi reikšmės aproksimacijai galima nustatyti, ar įvesties duomenys yra atsitiktiniai. Laikykime, kad įvesties duomenų sritis yra kvadratas (žr. 6 pav.), kurio kraštinė yra *2r* ilgio, o plotas yra $4r^2$. Šiame kvadrate nupiešiame apskritimą, kurio spindulys yra *r*, o jo plotas πr^2. Šiame kvadrate išdėliojame atsitiktinai taškus ir suskaičiuojame, kiek iš jų pateko į apskritimo plotą. Apskritimo ploto ir kvadrato ploto santykis yra $\pi r^2/4r^2$, o

tai yra lygu π/4. Suskaičiuojame į apskritimo plotą patekusių taškų ir visų kvadrate išdėliotų taškų santykį. Galiausiai padauginus šį santykį iš 4 yra gaunama aproksimuota π reikšmė.



6 pav. *Monte Karlo π aproksimacijos testo įvesčių sritis*

Įvertinus aproksimuotos π reikšmės paklaidą procentais galima nustatyti tyrimo įvesčių atsitiktinumą. Kuo mažesnė apskaičiuota π reikšmės paklaida, tai yra – kuo tiksliau apskaičiuota π reikšmė, tuo labiau atsitiktinės įvesties reikšmės. Faile saugoma informacija, kuri yra labai panaši į atsitiktinę indikuoja, kad toks failas yra galimai šifruotas. Taip pat galima spręsti, kad failas yra suspaustas, jei atlikus π aproksimacijos testą, gauta paklaida yra didelė. Konkrečios ribinės paklaidų reikšmės, pagal kurias galima nustatyti, ar failas yra šifruotas ar suspaustas, bus aprašytos tyrimo rezultatų skyriuje.

2.10. Pearsono chi-kvadrato testas

Chi-kvadrato testas yra statistinis testas, kuriuo galima nustatyti, ar yra reikšmingas skirtumas tarp stebėtų ir lauktų kokio nors bandymo rezultatų. Atlikus chi-kvadrato testą galima pasakyti, ar bandymo rezultatai iš tiesų buvo atsitiktiniai, ar priklausė, nuo kokių nors bandymo metu buvusių kintamųjų. Pearsono chi-kvadrato testas yra vienas labiausiai paplitusių chi-kvadrato testų, kurių rezultatai yra įvertinami lyginant juos su chi-kvadrato kritinių reikšmių lentele (žr. 1 lentelė). Pearsono chi-kvadrato testas susideda iš penkių etapų:

1. Apskaičiuojama chi-kvadratu reikšmė, kuri yra lygi visų nuokrypių kvadratu nuo teorinių reikšmių sumai.
2. Nustatomas laisvės laipsnių skaičius, kuris nurodo kiek reikšmių gali įgauti tiriami įvesties duomenys.
3. Pasirenkamas norimas reikšmingumo lygis, kuris nurodo kokiu tvirtumu galima pasakyti, kad tyrimo rezultatai buvo atsitiktiniai ir nepriklausomi.

4. Palyginama apskaičiuota chi-kvadratu reikšmė su kritine reikšme chi-pasiskirstymo lentelėje (žr. 1 lentelė). Kritinė reikšmė yra nustatoma pagal laisvės laipsnių skaičių ir pasirinktą reikšmingumo lygį.
5. Priimama arba atmetama hipotezė, kad tyrimo rezultatai yra atsitiktiniai. Jei chi-kvadratu reikšmė viršija kritinę reikšmę lentelėje, tada galima atmesti hipotezę, kad tyrimo rezultatai yra atsitiktiniai su atitinkamu patikimumu. Dažniausiai naudojamas reikšmingumo lygis yra 0,05, o tai reiškia, kad neviršijus kritinės reikšmės galime sakyti 95% patikimumu, kad tyrimo rezultatai yra atsitiktiniai ir nepriklausomi.

1 lentelė. *Chi-kvadrato kritinių reikšmių lentelė.*

		Reikšmingumo lygis					
		0,1	**0,05**	**0,025**	**0,01**	**0,005**	**0,001**
Laisvės laipsnis	**1**	2,706	3,841	5,024	6,635	7,879	10,828
	2	4,605	5,991	7,378	9,210	10,597	13,816
	3	6,251	7,815	9,348	11,345	12,838	16,266
	4	7,779	9,488	11,143	13,277	14,860	18,467
	5	9,236	11,070	12,833	15,086	16,750	20,515
	6	10,645	12,592	14,449	16,812	18,548	22,458
	7	12,017	14,067	16,013	18,475	20,278	24,322
	8	13,362	15,507	17,535	20,090	21,955	26,124
	9	14,684	16,919	19,023	21,666	23,589	27,877
	10	15,987	18,307	20,483	23,209	25,188	29,588

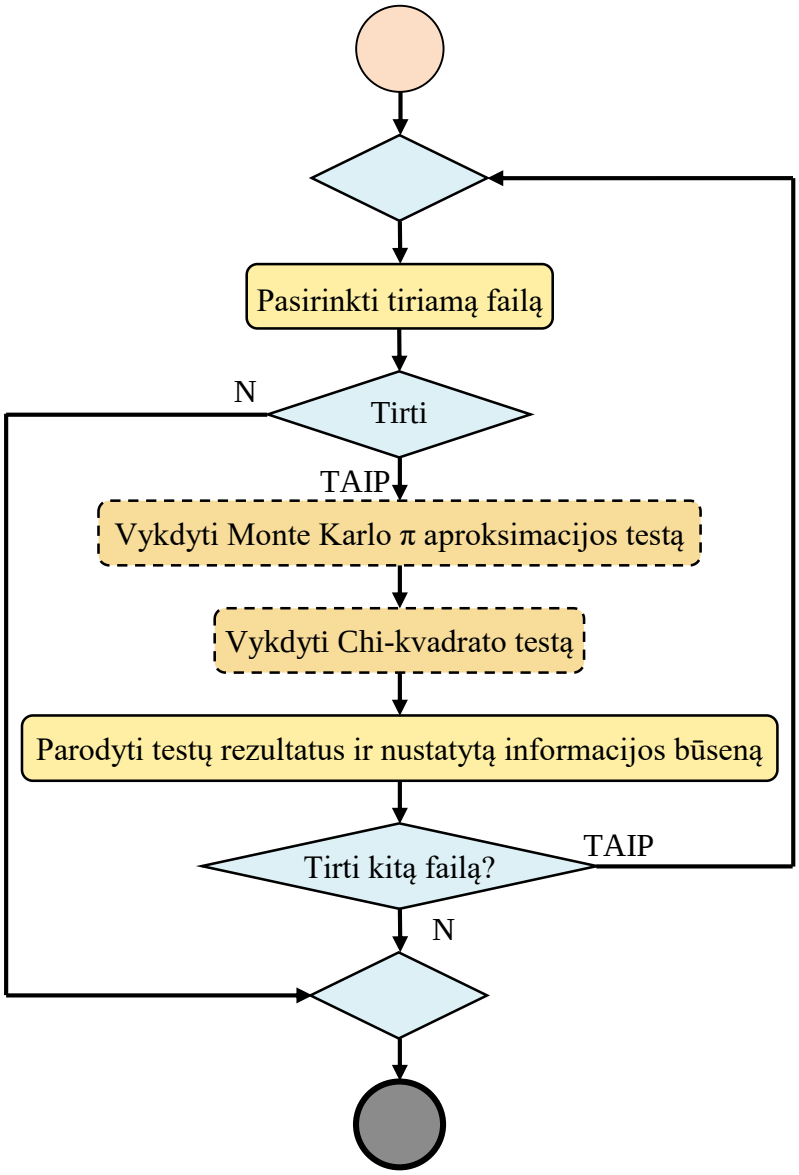
2.11. Analizės išvados

1. Vykdant kompiuterinę ekspertizę svarbus yra operatyvumas ir efektyvi nusikaltimų įrodymų paieška.
2. Kompiuterinės ekspertizės metu svarbu suteikti prioritetą suspaustiems ir šifruotiems failams, nes yra didesnė tikimybė, kad tokiuose failuose bus rasti nusikalstamos veikos įrodymai
3. Šifruotus failus nuo suspaustų galima atskirti tiriant failuose saugomos informacijos atsitiktinumą.
4. Informacijos atsitiktinumas yra nustatomas taikant statistinius testus.

3. PROGRAMINĖS ĮRANGOS SKIRTOS ŠIFRUOTŲ IR SUSPAUSTŲ FAILŲ APTIKIMUI PROJEKTAS

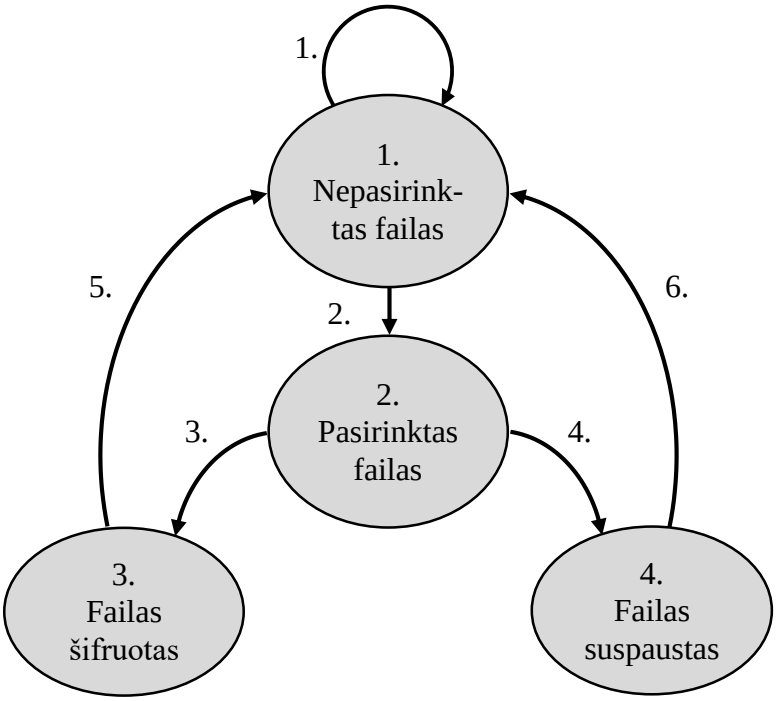
3.1. Programos aprašymas

Programinis įrankis yra skirtas tiriamų kompiuterinių failų analizei ir juose saugomos informacijos būsenos nustatymui. Šis įrankis yra skirtas kompiuterinę ekspertizę atliekantiems tyrėjams. Įrankyje yra realizuoti du statistiniai informacijos analizės testai, kurių tinkamumas buvo nustatytas bandymų metu. Vykdant programą yra taikomas Pearsono chi-kvadrato testas bei Monte Karlo metodas Pi aproksimacijai. Šių testų rezultatai yra skaitinės reikšmės, kurias pasitelkiant galima spręsti tiriamame faile saugoma informacija yra suspausta ar šifruota. Žemiau bus pateiktas programos veiklos procesų modelis (žr. 7 pav.).



7 pav. *Programos veiklos procesų modelis*

Iš veiklos procesų modelio matyti, kad programos veikimas yra gan paprastas – tyrėjas pasirenka tiriamą failą, tada yra vykdomi statistiniai testai ir parodomi jų rezultatai.



8 pav. *Realizuotos programos būsenų diagrama*

Aukščiau (žr. 8 pav.) yra programos būsenų diagrama, kurioje matoma, kad programa gali būti vienoje iš keturių būsenų. Pirmoji ir paskutinė būsena yra „Nepasirinktas failas“. Šioje būsenoje programa būna kai ji yra paleidžiama ir kai nėra tiriami jokie failai. Visi perėjimai tarp būsenų yra aprašyti žemiau (žr. 2 lentelė).

2 lentelė. *Realizuotos programos būsenų perėjimai*

Pokyčio numeris	Pradinė būsena	Pokytis	Sekanti būsena	Rezultatas
1.	Nepasirinktas failas	Nepasirenkamas joks failas	Nepasirinktas failas	Rodoma failų pasirinkimo opcija
2.		Pasirenkamas tiriamas failas	Pasirinktas failas	Failo tyrimo opcija tampa aktyvuota
3.	Pasirinktas failas	Vykdomi statistiniai testai	Failas šifruotas	Parodomi tyrimo rezultatai ir failas identifikuojamas kaip šifruotas
4.		Vykdomi statistiniai testai	Failas suspaustas	Parodomi tyrimo rezultatai ir failas identifikuojamas kaip suspaustas

5.	Failas šifruotas	Pasirenkama opcija tirti kitą failą	Nepasirinktas failas	Rodomas failų pasirinkimo dialogas
6.	Failas suspaustas	Pasirenkama opcija tirti kitą failą	Nepasirinktas failas	Rodomas failų pasirinkimo dialogas

3.2. Statistinių metodų taikymas šifruotos ir suspaustos informacijos nustatymui

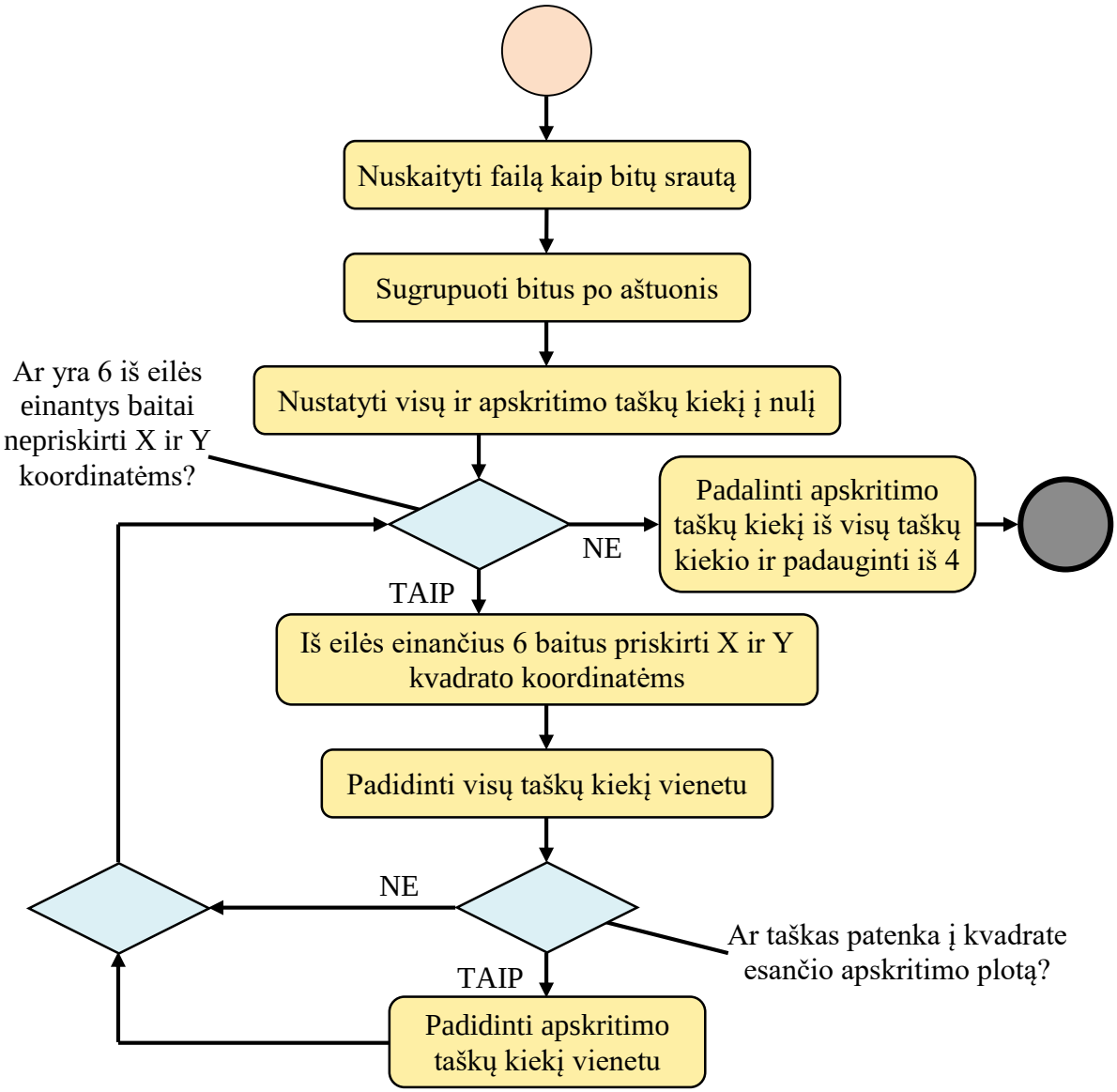
Failuose saugomos informacijos būsenai nustatyti galima taikyti įvairius statistinius testus ir metodus, kurie parodo informacijos tankį. Tarp šių testų yra:

1. **Shannono entropija**, kuri parodo kiek vidutiniškai reikia bitų viename baite saugoti informacijai faile.
2. **Pearsono chi-kvadrato testas**, kuris leidžia įvertinti bandymo reikšmių paklaidas ir pasakyti, ar tiriama informacija yra atsitiktinė ir nepriklausoma.
3. **Aritmetinio vidurkio testas**, kurio metu yra sudedami visi faile saugomos informacijos baitai ir paskaičiuojamas jų vidurkis. Kuo vidurkis yra arčiau 127.5 (baite galima saugoti reikšmes [0:255]), tuo labiau atsitiktinė yra tiriama informacija.
4. **Monte Karlo metodas Pi aproksimacijai**, kurio metu faile saugoma informacija yra panaudojama π reikšmės apskaičiavimui. Kuo mažesne paklaida apskaičiuojamas π, tuo labiau atsitiktinė yra tiriama informacija.
5. **Serijinės koreliacijos testas**, kuris kaip labai priklausomas kiekvienas informacijos baitas nuo prieš tai buvusio baito.

Atlikus bandymus buvo nustatyta, kad aiškiausi ir reikšmingiausi rezultatai yra gaunami kartu taikant du metodus – Pearsono chi-kvadrato testą ir Monte Karlo metodą Pi aproksimacijai.

3.2.1. Programoje taikomas Monte Karlo metodas Pi aproksimacijai

Vienas iš programoje taikomų testų yra Monte Karlo metodas Pi aproksimacijai. Šio testo rezultatas yra aproksimuota Pi reikšmė. Kuo tiksliau yra apskaičiuojama Pi reikšmė, tuo labiau atsitiktiniai yra testo įvesties duomenys, o tai indikuoja, kad analizuojama informacija yra šifruota.



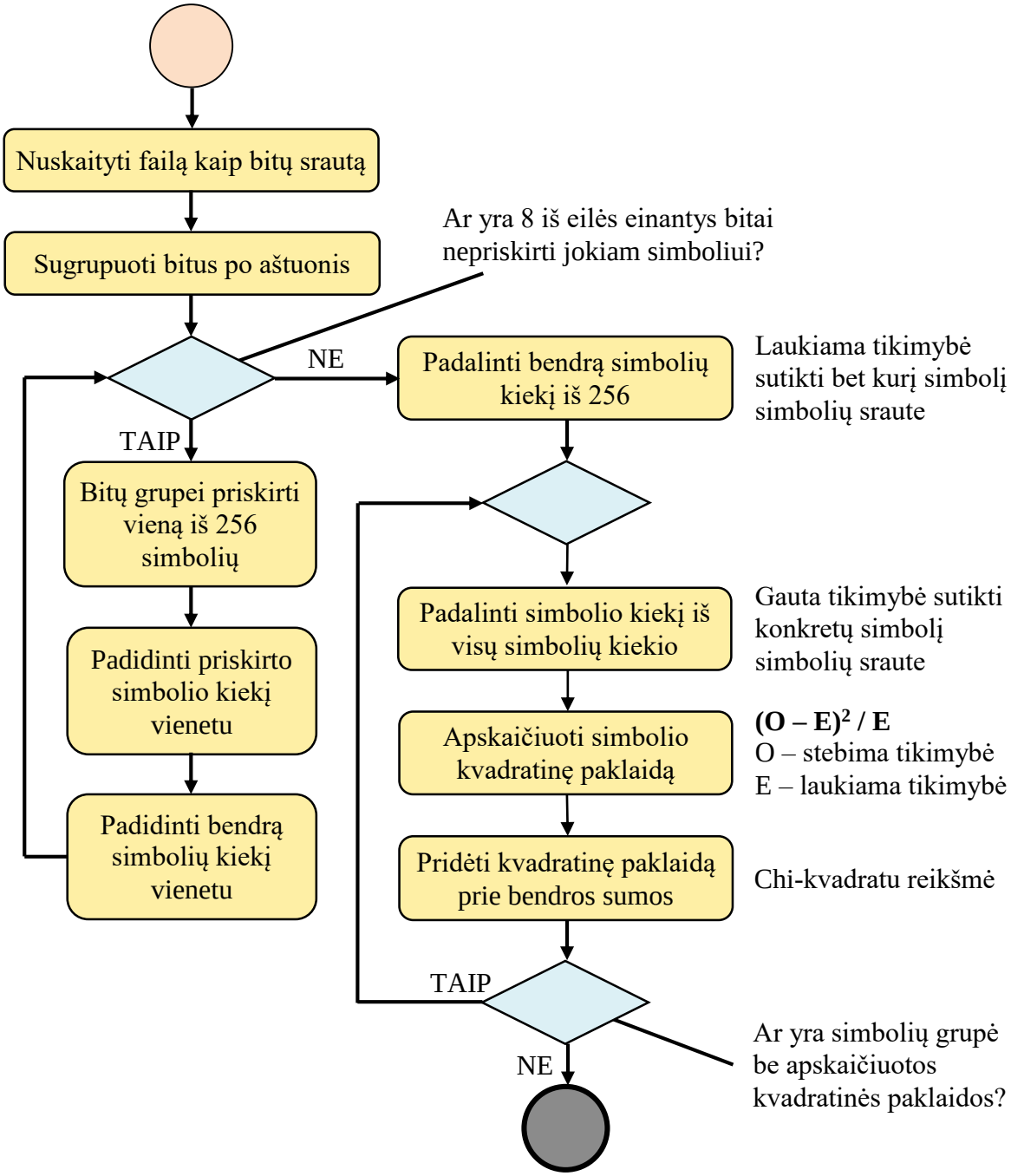
9 pav. *Monte Karlo Pi aproksimacijos testo veiklos procesų diagrama*

Veiklos procesų diagramoje (žr. 9 pav.) yra matomi visi testo metu vykdomi žingsniai nuo failo nuskaitymo iki Pi reikšmės apskaičiavimo. Pirmiausiai yra vykdomas failo nuskaitymas kaip bitų srautas ir bitai yra sugrupuojami baitais. Vėliau visi iš eilės einantys šeši baitai yra priskiriami kvadrato X ir Y koordinatėms (po 3 baitus) ir nustatoma, ar taškas patenka į apskritimo, nubrėžto kvadrate, plotą (žr. 6 pav.). Sekančiame žingsnyje yra apskaičiuojamas į apskritimo plotą patekusių taškų ir visų taškų santykis. Kadangi apskritimo ir kvadrato plotų santykis yra išreiškiamas $\pi/4$, tai norint gauti π reikšmę, apskritimo taškų ir visų taškų santykis yra padauginamas iš 4.

3.2.2. Programoje taikomas Pearsono chi-kvadrato testas

Antrasis programoje taikomas statistinis testas yra Pearsono chi-kvadrato testas. Šio testo rezultatas yra chi-kvadratu reikšmė. Norint įvertinti testo rezultatus, jie yra lyginami su

chi-kvadrato kritinių reikšmių lentele (žr. 1 lentelė). Kadangi norima nustatyti, ar tiriama informacija yra šifruota, tai šiam testui taikoma hipotezė teigia, kad įvesties duomenys yra atsitiktiniai. Jei testo rezultatai neviršija nustatytos kritinės reikšmės kritinių reikšmių lentelėje, tai galima, su tam tikru tvirtumu, teigti, kad tiriama informacija yra atsitiktinė (šifruota). Paprastai yra pasirenkamas 0,05 reikšmingumo lygis, kuris reiškia, kad galima patvirtinti arba paneigti hipotezę 95% tvirtumu.



10 pav. *Pearsono chi-kvadrato testo veiklos procesų diagrama*

Veiklos procesų diagramoje (žr. 10 pav.) yra matomi visi testo metu vykdomi žingsniai, kurie yra reikalingi norint nustatyti chi-kvadratu reikšmę. Pirmame žingsnyje yra vykdomas failo kaip bitų srauto nuskaitymas ir jų grupavimas į baitus. Vėliau visi baitai po

vieną yra priskiriami vienam iš 256 ASCII simbolių (bitas gali įgauti 256 skirtingas reikšmes). Simbolių, kuriems yra priskiriami bitai, lentelė bus pateikta žemiau (žr. 3 lentelė). Sekančiame žingsnyje yra apskaičiuojama laukiama (teorinė) tikimybė sutikti kiekvieną simbolį simbolių sraute. Kadangi hipotezė teigia, kad duomenys atsitiktiniai, tai ir teorinė tikimybė simbolių sraute sutikti tam tikrą simbolį, visiems 256 simboliams yra vienoda. Tada yra apskaičiuojama stebima (praktinė) kiekvieno simbolio tikimybė jį sutikti simbolių sraute. Paskutiniame žingsnyje, apskaičiavus laukiamą ir stebimą tikimybes, yra apskaičiuojamos kvadratinės paklaidos kiekvienam simboliui ir jos visos sudedamos.

3 lentelė. *ASCII simbolių lentelė*

0	NULL	32		64	@	96	`	128	Ç	160	á	192	└	224	Ó
1	SOH	33	!	65	A	97	a	129	ü	161	í	193	┴	225	ß
2	STX	34	"	66	B	98	b	130	é	162	ó	194	┬	226	Ô
3	ETX	35	#	67	C	99	c	131	â	163	ú	195	├	227	Ò
4	EOT	36	$	68	D	100	d	132	ä	164	ñ	196	─	228	õ
5	ENQ	37	%	69	E	101	e	133	à	165	Ñ	197	┼	229	Õ
6	ACK	38	&	70	F	102	f	134	å	166	ª	198	ã	230	µ
7	BEL	39	'	71	G	103	g	135	ç	167	º	199	Ã	231	þ
8	BS	40	(	72	H	104	h	136	ê	168	¿	200	╚	232	Þ
9	HT	41	)	73	I	105	i	137	ë	169	®	201	╔	233	Ú
10	LF	42	*	74	J	106	j	138	è	170	¬	202	╩	234	Û
11	VT	43	+	75	K	107	k	139	ï	171	½	203	╦	235	Ù
12	FF	44	,	76	L	108	l	140	î	172	¼	204	╠	236	ý
13	CR	45	-	77	M	109	m	141	ì	173	¡	205	═	237	Ý
14	SO	46	.	78	N	110	n	142	Ä	174	«	206	╬	238	¯
15	SI	47	/	79	O	111	o	143	Å	175	»	207	¤	239	´
16	DLE	48	0	80	P	112	p	144	É	176	░	208	ð	240	
17	DC1	49	1	81	Q	113	q	145	æ	177	▒	209	Ð	241	±
18	DC2	50	2	82	R	114	r	146	Æ	178	▓	210	Ê	242	‗
19	DC3	51	3	83	S	115	s	147	ô	179	│	211	Ë	243	¾
20	DC4	52	4	84	T	116	t	148	ö	180	┤	212	È	244	¶
21	NAK	53	5	85	U	117	u	149	ò	181	Á	213	ı	245	§
22	SYN	54	6	86	V	118	v	150	û	182	Â	214	Í	246	÷
23	ETB	55	7	87	W	119	w	151	ù	183	À	215	Î	247	¸
24	CAN	56	8	88	X	120	x	152	ÿ	184	©	216	Ï	248	°
25	EM	57	9	89	Y	121	y	153	Ö	185	╣	217	┘	249	¨
26	SUB	58	:	90	Z	122	z	154	Ü	186	║	218	┌	250	·
27	ESC	59	;	91	[	123	{	155	ø	187	╗	219	█	251	¹
28	FS	60	<	92	\	124	|	156	£	188	╝	220	▄	252	³
29	GS	61	=	93	]	125	}	157	Ø	189	¢	221	¦	253	²
30	RS	62	>	94	^	126	~	158	×	190	¥	222	Ì	254	■
31	US	63	?	95	_	127	DEL	159	*ƒ*	191	┐	223	▀	255	nbsp

4. TYRIMAI IR JŲ REZULTATAI

4.1. Tyrimas

Tyrimo metu buvo taikomi statistiniai testai įvairiais šifravimo algoritmais šifruotiems failams bei įvairiais suspaudimo algoritmais suspaustiems failams. Tyrimas susidėjo iš dviejų etapų. Pirmame etape pasirinktas tyrimui failas buvo šifruotas ir suspaustas taikant skirtingus algoritmus. Antrame etape buvo analizuojami pirmojo etapo metu sukurti failai naudojant statistinius testus.

Tyrimui pasirinktas „intro.mp4“ vaizdo įrašo failas, kuris yra 15,3 megabaitų dydžio.

Failo suspaudimui buvo naudojamos taikomosios programos:

1. 7-Zip versija 9.20
2. PowerArchiver versija 15.04.03
3. WinRAR versija 5.21

Failo šifravimui buvo naudojama atvirojo kodo įrankis:

OpenSSL versija 1.0.2g

Tyrimui pasirinktas failas buvo užšifruotas dvidešimt dviem skirtingais metodais (įskaitant skirtingus šifravimo rėžimus) bei buvo naudojamas saugus dvidešimties simbolių iš keturių grupių (specialūs simboliai, skaičiai, mažosios raidės, didžiosios raidės) slaptažodis. Taip pat tyrimo metu naudotas failas buvo suspaustas naudojant dvidešimt du skirtingus suspaudimo metodus.

Tyrimo metu buvo tirti dvidešimt du šifruoti (žr. 4 lentelė) ir dvidešimt du suspausti failai (žr. 5 lentelė).

4 lentelė. *Tyrimo metu naudoti šifravimo algoritmai*

Šifruoto failo pavadinimas	Šifravimo algoritmo pavadinimas	Šifravimo rėžimas	Bloko dydis
aes-128-cbc	Advanced Encryption Standard (AES)	Grandinės rėžimas (CBC)	128 bitai
aes-256-cbc	Advanced Encryption Standard (AES)	Grandinės rėžimas (CBC)	256 bitai
aes-256-cfb	Advanced Encryption Standard (AES)	Grįžtamojo ryšio rėžimas (CFB)	256 bitai
aes-256-ctr	Advanced Encryption Standard (AES)	Skaičiuotuvo rėžimas (CTR)	256 bitai

aes-256-ecb	Advanced Encryption Standard (AES)	Elektroninės užrašų knygutės rėžimas (ECB)	256 bitai
aes-256-ofb	Advanced Encryption Standard (AES)	Grįžtamojo išeities ryšio rėžimas (OFB)	256 bitai
bf-cbc	Blowfish	Grandinės rėžimas (CBC)	64 bitai
cast-cbc	CAST	Grandinės rėžimas (CBC)	64 bitai
cast5-cbc	CAST-128	Grandinės rėžimas (CBC)	64 bitai
des-cbc	Data Encryption Standard (DES)	Grandinės rėžimas (CBC)	64 bitai
des-ede3-cbc	Triple Data Encryption Standard (3DES)	Grandinės rėžimas (CBC)	64 bitai
idea-cbc	International Data Encryption Algorithm (IDEA)	Grandinės rėžimas (CBC)	64 bitai
idea-cfb	International Data Encryption Algorithm (IDEA)	Grįžtamojo ryšio rėžimas (CFB)	64 bitai
idea-ecb	International Data Encryption Algorithm (IDEA)	Elektroninės užrašų knygutės rėžimas (ECB)	64 bitai
idea-ofb	International Data Encryption Algorithm (IDEA)	Grįžtamojo išeities ryšio rėžimas (OFB)	64 bitai
camellia-128-cbc	Camellia	Grandinės rėžimas (CBC)	128 bitai
camellia-256-cbc	Camellia	Grandinės rėžimas (CBC)	256 bitai
camellia-256-cfb	Camellia	Grįžtamojo ryšio rėžimas (CFB)	256 bitai
camellia-256-ecb	Camellia	Elektroninės užrašų knygutės rėžimas (ECB)	256 bitai
camellia-256-ofb	Camellia	Grįžtamojo išeities ryšio rėžimas (OFB)	256 bitai
seed-cbc	SEED	Grandinės rėžimas (CBC)	128 bitai
rc2-cbc	Rivest Cipher 2	Grandinės rėžimas (CBC)	64 bitai

5 lentelė. *Tyrimo metu naudoti suspaudimo algoritmai ir metodai*

Suspausto failo pavadinimas	Archyvo formatas	Suspaudimo metodas	Žodyno dydis
7z_BZip2	7-Zip	BZip2	900 KB
7z_LZMA	7-Zip	LZMA	64 MB
7z_LZMA2	7-Zip	LZMA2	64 MB
7z_PPMd	7-Zip	PPMd	192 MB
bzip2_BZip2	BZip2	BZip2	900 KB
gzip_Deflate	Gzip	Deflate	32 KB
xz_LZMA2	xz	LZMA2	64 MB
zip_BZip2	Zip	BZip2	900 KB
zip_Deflate	Zip	Deflate	32 KB
zip_Deflate64	Zip	Deflate64	64 KB
zip_LZMA	Zip	LZMA	64 MB
zip_PPMd	Zip	PPMd	128 MB
bh_Deflate	BlakHole (BH)	Deflate	32 KB
cab_LZX	Cabinet (CAB)	LZX	48 MB
cab_MsZIP type	Cabinet (CAB)	MsZIP type	48 MB
tar_Store	Tar	Store	4 MB
wim_Store	Wim	Store	4 MB
lzh_Frozen6	LHA	Frozen6	64 KB
lzh_Frozen5	LHA	Frozen5	64 KB
rar_RAR4	RAR	RAR4	32 MB
rar_RAR5	RAR	RAR5	32 MB
zpaq_LZ77	ZPAQ	LZ77	32 MB

4.2. Tyrimo rezultatai

Taikant realizuotą programą buvo ištirti keturiasdešimt keturi failai. Pusė tiriamų failų buvo suspausti, o kita pusė – šifruoti.

6 lentelė. *Šifruotų failų tyrimo rezultatai*

Šifruotas failas	Entropija	Chi-kvadratu	Aproksimuota π	π paklaida
aes-128-cbc	7,999987	279,49	3,141438021	0,005%
aes-256-cbc	7,999989	233,49	3,142179903	0,019%
aes-256-cfb	7,999990	204,92	3,142035268	0,014%
aes-256-ctr	7,999988	251,02	3,142832047	0,039%
aes-256-ecb	7,999989	239,59	3,143782872	0,070%
aes-256-ofb	7,999986	291,56	3,140694233	0,029%
bf-cbc	7,999988	249,24	3,141144718	0,014%
cast5-cbc	7,999988	250,44	3,141640352	0,002%
des-cbc	7,999989	242,13	3,140702412	0,028%
idea-cbc	7,999989	237,62	3,139736240	0,059%
idea-cfb	7,999987	271,84	3,141384356	0,007%
idea-ecb	7,999950	247,00	3,139321210	0,072%
idea-ofb	7,999987	284,91	3,142410131	0,026%
camellia-128-cbc	7,999989	235,79	3,141207457	0,012%
camellia-256-cbc	7,999989	237,35	3,139322166	0,072%
camellia-256-cfb	7,999986	292,49	3,141113012	0,015%
camellia-256-ecb	7,999988	257,05	3,141743871	0,005%
camellia-256-ofb	7,999988	244,35	3,140706781	0,028%
cast-cbc	7,999988	250,30	3,143304491	0,054%
des-ede3-cbc	7,999988	263,83	3,142441837	0,027%
seed-cbc	7,999990	203,06	3,141538402	0,002%
rc2-cbc	7,999986	290,56	3,141881896	0,009%

7 lentelė. *Suspaustų failų tyrimo rezultatai*

Suspaustas failas	Entropija	Chi-kvadratu	Aproksimuota π	π paklaida
7z_BZip2	7,999783	4491,86	3,152385463	0,344%
7z_LZMA	7,999988	253,91	3,141185221	0,013%
7z_LZMA2	7,999604	9246,87	3,145291173	0,118%
7z_PPMd	7,999988	266,54	3,140592240	0,032%
bzip2_BZip2	7,999783	4482,18	3,152735423	0,355%
gzip_Deflate	7,999832	3757,69	3,144623841	0,096%
xz_LZMA2	7,999604	9227,86	3,143598714	0,064%
zip_BZip2	7,999783	4494,82	3,151748673	0,323%
zip_Deflate	7,999831	3780,00	3,142323047	0,023%
zip_Deflate64	7,999848	3392,03	3,142749040	0,037%
zip_LZMA	7,998018	52850,93	3,148840662	0,231%
zip_PPMd	7,998018	52850,93	3,148840662	0,231%
bh_Deflate	7,999740	5922,58	3,142170569	0,018%
cab_LZX	7,999680	7348,69	3,143776475	0,070%
cab_MsZIP type	7,999766	5307,82	3,143293252	0,054%
tar_Store	7,997928	55554,16	3,148664120	0,225%
wim_Store	7,997977	54095,16	3,148445449	0,218%
lzh_Frozen6	7,998021	52759,97	3,148832418	0,230%
lzh_Frozen5	7,998021	52759,95	3,148832418	0,230%
rar_RAR4	7,999939	1301,68	3,136831940	0,152%
rar_RAR5	7,999965	732,20	3,144792245	0,102%
zpaq_LZ77	7,997886	56808,58	3,150603680	0,287%

Iš šifruotų failų lentelės (žr. 6 lentelė) matoma, kad šifruotų failų chi-kvadratu reikšmės yra pakankamai mažos ir neviršija 300, o π apskaičiuotas labai tiksliai – paklaidos yra mažesnės nei 0,1%. Suspaustų failų lentelėje (žr. 7 lentelė) matomos visiškai kitokios reikšmės. Suspaustų failų chi-kvadratu reikšmės yra gerokai didesnės nei šifruotų failų ir paprastai siekia kelis tūkstančius. Ištyrus suspaustus failus taip pat matoma, kad π yra apskaičiuojamas

mažesniu tikslumu nei šifruotų failų. Iš rezultatų suvestinės (žr. 8 lentelė) aiškiai matomas reikšmių skirtumas

8 lentelė. *Tyrimo rezultatų suvestinė*

	Šifruoti failai	**Suspausti failai**
Vidutinė chi-kvadratu reikšmė	252,64	20076,66
Vidutinė π paklaida	0,028 %	0,157 %

Pearsono chi-kvadrato testo rezultatai yra įvertinami lyginant gautas chi-kvadratu reikšmes su kritinėmis reikšmėmis (žr. 9 lentelė). Norint išsiaiškinti kritinę reikšmę yra svarbūs du kintamieji. Pirmiausiai reikia nustatyti laisvės laipsnių skaičių. Kadangi kiekvienas tiriamo failo bitas yra priskiriamas vienam ASCII lentelės (žr. 3 lentelė) simboliui ir gali įgauti vieną iš 256 reikšmių, tai laisvės laipsnių yra 255. Paskiau reikia pasirinkti reikšmingumo lygį (paprastai 0,05), kuris parodo kokiu tvirtumu galima patvirtinti iškeltą hipotezę. Lyginant pasirinktus parametrus ir kritinių reikšmių lentelę (žr. 9 lentelė) kritinė chi-kvadratu reikšmė yra **293,248**, tačiau toks tikslumas nėra būtinas ir galima šią reikšmę apvalinti iki **300**.

9 lentelė. *Kritinių reikšmių lentelė*

		Reikšmingumo lygis					
		0,1	**0,05**	**0,025**	**0,01**	**0,005**	**0,001**
Laisvės laipsnis	**1**	2,706	3,841	5,024	6,635	7,879	10,828
	2	4,605	5,991	7,378	9,210	10,597	13,816
	3	6,251	7,815	9,348	11,345	12,838	16,266
	4	7,779	9,488	11,143	13,277	14,860	18,467
	5	9,236	11,070	12,833	15,086	16,750	20,515
	6	10,645	12,592	14,449	16,812	18,548	22,458
	7	12,017	14,067	16,013	18,475	20,278	24,322
	8	13,362	15,507	17,535	20,090	21,955	26,124
	9	14,684	16,919	19,023	21,666	23,589	27,877
	10	15,987	18,307	20,483	23,209	25,188	29,588
	100	118,498	124,342	129,561	135,807	140,169	149,449
	127	147,805	154,302	160,086	166,987	171,796	181,993
	255	284,336	293,248	301,125	310,457	316,919	330,520

	511	552,374	564,696	575,530	588,298	597,098	615,515
	1023	1081,379	1098,521	1113,533	1131,159	1143,265	1168,497

4.3. Tyrimo išvados

1. Nustatyta kritinė chi-kvadratu reikšmė (300), kuri leidžia spręsti apie tiriamo failo būseną.
2. Mažesnė nei 300 chi-kvadratu reikšmė indikuoja, kad tiriamas failas yra šifruotas.
3. Didesne nei 300 chi-kvadrato reikšmė indikuoja, kad tiriamas failas yra suspaustas.
4. Labai tiksliai apskaičiuota π reikšmė – paklaida mažesnė nei 0,01% stipriai indikuoja, kad tiriamas failas yra šifruotas.
5. Pakankamai tiksliai apskaičiuota π reikšmė – paklaida mažesnė nei 0,03% indikuoja, kad tiriamas failas yra šifruotas.
6. Netiksliai apskaičiuota π reikšmė – paklaida didesnė nei 0,03% indikuoja, kad tiriamas failas yra suspaustas.
7. Ne visi suspausti failai atitiko nustatytas suspaustų failų charakteristikas.
8. „7-zip“ formato archyvas suspaustas „LZMA“ metodu turi charakteristikas, kurios visiškai atitinka šifruoto failo charakteristikas.
9. „7-zip“ formato archyvo suspausto „PPMd“ metodu viena charakteristika - chi-kvadratu reikšmė indikuoja, kad šis failas yra šifruotas, tačiau π paklaida indikuoja, kad tai suspaustas failas.
10. Pasirinkti statistiniai tyrimo metodai leidžia nustatyti tiriami failai yra suspausti ar šifruoti.

4.4. Programos veikimo tyrimas

Programos veikimo tyrimo metu buvo tiriami šifruoti ir suspausti failai bei registruojami visi rezultatai, kuriuos pateikdavo programa. Šiam tyrimui buvo naudojamas dvidešimties failų rinkinys (žr. 10 lentelė).

10 lentelė. *Tyrimo metu naudoti failai*

	Formatas	**Dydis, KB**		**Formatas**	**Dydis, KB**
Garso takeliai	FLAC	13652	**Paveikslėliai**	GIF	918
	MP3	3087		JPG	395
	OGG	4328		PNG	18022
	WAV	14802		TGA	6751
	WMA	5314		TIFF	3022

Dokumentai	DOCX	13	**Vaizdo įrašai**	AVI	73102
	PPTX	194		MKV	212
	XLSX	35		MOV	12875
	PDF	979		MP4	4581
	TXT	440		MPEG	5851

Septyniolika tyrimo failų buvo užšifruoti, o trylika suspausti naudojant skirtingus algoritmus. Visiems suspaustiems ir šifruotiems failams buvo priskirti atsitiktiniai dešimties skaitmenų pavadinimai bei panaikinti failų plėtiniai. Galiausiai šie failai buvo analizuojami naudojant realizuotą programinę įrangą ir registruojami gauti rezultatai, kuriuos sudaro chi-kvadratu reikšmė, aproksimuota Pi reikšmė bei nustatyta failo būsena. Pagal metodų tyrimo metu nustatytus dydžius, programinė įranga pateikia vieną iš keturių būsenos reikšmių: „suspaustas“, „suspaustas (stipri indikacija)“, „šifruotas“, „šifruotas (stipri indikacija)“.

11 lentelė. *Programos veikimo tyrimo rezultatai*

Formatas	Metodas	Chi-kvadratu	II paklaida	Nustatyta būsena
FLAC	rar – rar5	19299.42	0,992%	suspaustas (stipri indikacija)
MP3	aes-256-cbc	228.81	0,014%	šifruotas (stipri indikacija)
OGG	des-ede3-cbc	277.63	0,069%	šifruotas
WAV	idea-ofb	238.44	0,049%	šifruotas
WMA	cab – LZX	3967.18	1,405%	suspaustas (stipri indikacija)
DOCX	cast5-cbc	295.64	1,089%	šifruotas
PPTX	LHA – Frozen6	510.48	1,079%	suspaustas (stipri indikacija)
XLSX	rc2-cbc	233.56	0,481%	šifruotas
PDF	bf-cbc	260.85	0,112%	šifruotas
TXT	idea-cbc	270.31	0,103%	šifruotas
GIF	camellia-256-ecb	236.01	0,220%	šifruotas
JPG	seed-cbc	268.69	0,144%	šifruotas
PNG	ZPAQ – LZ77	358.12	0,026%	suspaustas
TGA	7zip – Bzip2	15705.99	0,243%	suspaustas (stipri indikacija)
TIFF	BH – Deflate	6234.20	2,369%	suspaustas (stipri indikacija)
AVI	des-cbc	230.53	0,013%	šifruotas (stipri indikacija)

MKV	aes-128-cbc	250.96	0,234%	šifruotas
MOV	camellia-128-cbc	228.82	0,027%	šifruotas (stipri indikacija)
MP4	Zip – Deflate64	494.34	0,185%	suspaustas (stipri indikacija)
MPEG	GZip – Deflate	8286.75	1,425%	suspaustas (stipri indikacija)
OGG	7zip – LZMA	197371.17	6,829%	suspaustas (stipri indikacija)
MP4	XZ – LZMA2	444.64	0,232%	suspaustas (stipri indikacija)
MKV	BZip2 – bzip2	301.98	0,238%	suspaustas (stipri indikacija)
MPEG	idea-cfb	257.89	0,095%	šifruotas
GIF	aes-256-ctr	260.64	0,171%	šifruotas
MP3	aes-256-ofb	260.31	0,028%	šifruotas (stipri indikacija)
PDF	Zip – PPMd	286.99	0,066%	šifruotas
WMA	Zip – LZMA	240.94	0,028%	šifruotas (stipri indikacija)
TGA	cast-cbc	231.56	0,018%	šifruotas (stipri indikacija)
FLAC	camellia-256-ofb	245.89	0,009%	šifruotas (stipri indikacija)

Iš tyrimo rezultatų (žr. 11 lentelė) matoma, kad realizuota programinė įranga teisingai nustatė dvidešimt aštuonis iš trisdešimties tirtų failų. Iš septyniolikos tirtų šifruotų failų teisingai identifikuoti buvo visi šifruoti failai, tačiau iš trylikos tirtų suspaustų failų du failai buvo identifikuoti kaip šifruoti. Du rečiau naudojami „Zip“ formato suspaudimo metodai „PPMd“ ir „LZMA“ buvo tyrimo metu identifikuoti kaip šifruoti, taip yra todėl, kad jų tirtos charakteristikos atitiko šifruotų failų charakteristikas. Viso teisingai identifikuoti buvo 93% tirtų failų.

4.5. Programos veikimo tyrimo išvados

1. Realizuota programinė įranga teisingai identifikavo visus septyniolika šifruotų failų.
2. Realizuota programinė įranga teisingai identifikavo vienuolika iš trylikos suspaustų failų.
3. Pasirinkti šifruotų ir suspaustų failų nustatymo metodai pasirinkti teisingai ir juos taikant galima pakankamai tiksliai nustatyti tiriamo failo būseną.
4. Aštuoniolikos iš trisdešimties tirtų failų būsena nustatyta su stipria indikacija.
5. Tyrimo metu buvo nustatyta, kad „Zip“ archyvo suspaudimo metodai „PPMd“ ir „LZMA“ buvo identifikuoti neteisingai.

5. DARBO IŠVADOS

1. Šifruotų ir suspaustų failų nustatymui yra taikomi statistiniai juose saugomos informacijos testai.
2. Šifruotus ir suspaustus failus galima pakankamai tiksliai identifikuoti taikant du statistinius metodus – „Monte Karlo metodas Pi aproksimacijai“ ir „Pearsono chi-kvadrato testas“.
3. Metodų tyrimo metu buvo nustatyta, kad kritinė chi-kvadratu reikšmė Pearsono chi-kvadrato teste yra 300, o tai reiškia, kad jei failo analizės metu ji nėra viršijama, tai tiriamas failas yra šifruotas. Jei chi-kvadratu reikšme yra lygi arba viršija 300, tai failas yra suspaustas.
4. Metodų tyrimo metu buvo nustatyta, kad antrinis šifruotų ir suspaustų failų požymis yra Monte Karlo metodo aproksimuotos Pi reikšmės paklaida. Jei Pi paklaida yra mažesnė nei 0,01%, tai galima daryti išvadą, kad analizuojamas failas yra šifruotas.
5. Metodų tyrimo metu buvo nustatyta, kad norint identifikuoti šifruotus ir suspaustus failus galima remtis dviem požymiais chi-kvadratu reikšme ir aproksimuotos Pi reikšmės paklaida. Jei chi-kvadratu reikšmė yra mažesnė nei 300 ir Pi paklaida mažesnė nei 0,03%, tai parodo su stipria indikacija, kad tiriamas failas yra šifruotas. Jei chi-kvadratu reikšmė yra lygi arba didesnė nei 300, o Pi paklaida lygi arba didesnė nei 0,03%, tai parodo su stipria indikacija, kad tiriamas failas yra suspaustas.
6. Tiriant įvairius šifruotus ir suspaustus failus, buvo nustatyta, kad „PPMd“ ir „LZMA“ suspaudimo metodais suspausti failai turi ne suspaustų failų, tačiau šifruotų failų charakteristikas, todėl realizuota programinė įranga šiuos suspaudimo metodus identifikuoja neteisingai.
7. Pasirinkti šifruotų ir suspaustų failų nustatymo metodai pasirinkti teisingai ir juos taikant galima pakankamai tiksliai nustatyti tiriamo failo būseną.
8. Realizuota programinė įranga teisingai identifikavo visus 17 šifruotų failų.
9. Realizuota programinė įranga teisingai identifikavo 11 iš 13 suspaustų failų.
10. 18 iš 30 tirtų failų būsena nustatyta su stipria indikacija.
11. Ateityje, tęsiant metodų tyrimus galima ieškoti papildomų metodų, kurie leistų analizuoti papildomas failų charakteristikas ir teisingai identifikuoti visus suspaudimo algoritmus, kurie dabar yra neteisingai identifikuojami.

LITERATŪRA

[1] M. Chawki, A. Darwish, M. A. Khan ir S. Tyagi, „Cybercrime, Digital Forensics and Jurisdiction (Studies in Computational Intelligence),“ Springer, 2015.

[2] M. Cross ir D. L. Shinder, „Science of the Cybercrime, Second Edition,“ Syngress Publishing, Inc., 2008.

[3] E. Casey, „Handbook of Digital Forensics and Investigation,“ Elsevier Academic Press, 2009.

[4] H. Carvey, „Windows Forensic Analysis Toolkit, Third Edition: Advanced Analysis Techniques for Windows 7,“ Syngress Publishing, Inc., 2012.

[5] B. Carrier, „File System Forensic Analysis,“ Addison-Wesley Professional, 2005.

[6] N. Goranin ir D. Mažeika, „Nusikaltimai elektroninėje erdvėje ir jų tyrimo metodikos,“ 2011.

[7] D. B. Parker, „Fighting Computer Crime: A New Framework for Protecting Information,“ Wiley, 1998.

[8] A. Spruill, „Evidence Technology Magazine - Digital Forensics and Encryption,“ [Tinkle]. Available: http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=656. [Kreiptasi 17 Balandžio 2016].

[9] M. Delgado, M. Aparicio ir C. Costa, „Using Open Source for Forensic Purposes,“ 2012.

[10] M. Nelson, „LZW Revisited,“ [Tinkle]. Available: http://www.marknelson.us/2011/11/08/lzw-revisited. [Kreiptasi 14 Kovo 2016].

[11] P. Penrose, R. Macfarlane ir W. J. Buchanan, „Approaches to the classification of high entropy file fragments,“ Elsevier, 2013.