



VILNIAUS UNIVERSITETAS  
MATEMATIKOS IR INFORMATIKOS FAKULTETAS  
INFORMATIKOS INSTITUTAS  
KOMPIUTERIO IR DUOMENŲ MODELIAVIMO KATEDRA

IV semestro projektinis darbas

**Diskų kopijų teisminė ekspertizė Android įrenginiuose tyrimas**  
Disk image forensics research in Android devices

Atliko:

Matas Niewulis

parašas

Vadovas:

Lekt. Virgilijus Krinickij

Vilnius  
2023

# Turinys

<b>Sutartinis terminų žodynas</b>	<b>3</b>
<b>Santrauka</b>	<b>4</b>
<b>Summary</b>	<b>5</b>
<b>Ivydas</b>	<b>6</b>
<b>1. Susijusių darbų analizė</b>	<b>7</b>
<b>2. Android įrengino architektūra</b>	<b>8</b>
2.1. Operacinės sistemos architektūra . . . . .	8
2.2. Versijos . . . . .	8
<b>3. Įrankio veikimas</b>	<b>8</b>
<b>4. Įranga bei jos paruošimas</b>	<b>9</b>
<b>5. Įrankio paleidimas bei duomenų išgavimas</b>	<b>10</b>
5.1. Įrankio atvaizdo gavimas automatinio (1) atveju . . . . .	11
5.2. Įrenginio atvaizdo gavimas rankiniu (2) atveju . . . . .	12
5.3. Įrenginio atvaizdo gavimas iš įrenginio jau paleisto „TWRP“ režime (3) atveju . . .	12
5.4. Duomenų išgavimas iš jau turimo userdata.img dd atvaizdo (4) atveju . . . . .	12
5.5. Duomenų bazių analizė ir duomenų išvedimas į skaitomus .txt failus (5) atveju . . .	12
<b>6. Įrankio panaudojimo rezultatai su skirtingais įrenginiais</b>	<b>13</b>
6.1. Rezultatai su Samsung Galaxy S3 NEO įrenginiu . . . . .	13
6.2. Rezultatai su Samsung Galaxy S5 įrenginiu . . . . .	13
6.3. Rezultatai su Google Nexus 5 ir Oneplus 2 įrenginiais . . . . .	14
<b>7. Ištrauktų duomenų failų struktūra</b>	<b>14</b>
7.1. Katalogų struktūra . . . . .	14
7.2. Išanalizuotų .db failų apžvalga . . . . .	16
<b>Išvados ir rekomendacijos</b>	<b>18</b>
<b>Ateities tyrimų planas</b>	<b>19</b>
<b>Literatūros šaltiniai</b>	<b>20</b>

## Sutartinis terminų žodynas

- **„ADB“** – „Android Debug Bridge“ – „Android“ diagnostikos tiltas, skirtas komunikuoti su „Android“ įrenginiais per komandinę eilutę ir vykdyti įvairius veiksmus, pvz., diegti programinę įrangą, siųsti komandas ir peržiūrėti įrenginio informaciją. Tai yra sujungimas tarp mobiliojo įrenginio ir kompiuterio
- **„Bash“** – Unix tipo operacinės sistemos komandinės eilutės interpretatorius, naudojamas vykdyti komandų rinkinius, automatizuoti užduotis ir kurti skriptus. Tai populiari komandinės eilutės programa, dažnai naudojama „Linux“ aplinkoje.
- **„Boot“** – Įrenginio ar kompiuterio operacinės sistemos ar programinės įrangos užkrovimo procesas, kuris vykdomas įjungus įrenginį. Tai pirmasis žingsnis paleidžiant įrenginį kuris užtikrina, kad operacinė sistema ar programa būtų įkrauta ir veiktų tinkamai.
- **CWD** - Current Working directory - esamasis darbo katalogas
- **„Device driver“** – įrenginio tvarkyklė – Programinės įrangos komponentas, kuris leidžia operacinės sistemai sąveikauti su konkrečiu įrenginiu. Įrenginio tvarkyklės užtikrina, kad įrenginys būtų tinkamai valdomas ir galėtų veikti su kitomis sistemomis.
- **Flashing (įrašymas)** - Šis terminas apibūdina procesą, kai įrenginio atmintyje esantis programinis įrašas (pavyzdžiui, Android operacinė sistema) yra pakeičiamas kitu programiniu įrašu (pavyzdžiui, „custom ROM“), naudojant specialų programinį įrankį. Tai gali būti naudinga tiems, kurie nori atnaujinti savo Android įrenginio operacinę sistemą, arba nori pasiekti papildomas funkcijas, kurių nėra standartinėje sistemoje. Įrašyti galime taip pat partcijų atvaizdus, pvz. TWRP atvaizdą.
- **„Loop device“** - Virtualus įrenginys, kuris leidžia naudoti failą ar atminties sritį kaip blokinį įrenginį. Yra naudingas, kai reikia sukurti virtualų įrenginį, kuris veiktų kaip realus blokinis įrenginys, pavyzdžiui disko atvaizdas.
- **Particija** – Fizinis arba loginis laikmenos skyrius, skaidinys, kuris yra paskirstytas išmaniuose telefonuose ar kituose įrenginiuose. Particijos leidžia atskirti ir organizuoti skirtingus duomenų segmentus.
- **Particijos atvaizdas** – Particijos bitinė kopija (\*.img failas).
- **„Root“** - Administratoriaus prieigos teisių aukščiausias lygis „Android“ operacinėje sistemoje. Šis lygis suteikia galimybę vykdyti privilegijuotas operacijas, pakeisti sistemą sudarančius failus ir valdyti įrenginį plačiau.
- **„Shell script“** – Eilutės komandų rinkinys, kuriuo gali būti automatizuojami įvairūs veiksmai. Skriptas yra parašytas „Shell“ (arba „Bash“) kalba ir leidžia komandas per komandinės eilutės interpretatorių (\*.sh failas)
- **Skriptas** - Programavimo kalbos tekstas, kuriame yra įrašytos instrukcijos ar komandos, skirtos vykdyti tam tikrus veiksmus. Skriptai yra naudojami automatizuoti procesus ir palengvinti tam tikrus užduotis, pavyzdžiui, duomenų išgavimą iš įrenginio arba atlikti operacijas su failais.

## Santrauka

Išmanieji telefonai tapo vienu iš dažniausiai naudojamų komunikacijos priemonių dėl jų geriausio ryšio, funkcionalumo ir produktyvumo. Nuolat tobulėjant išmaniųjų telefonų technologijoms, atsiranda naujų lygių pavojai. Didžioji rinkos dalis pasitiki „Android“ operacinės sistemos telefonais, kuri yra svarbi jėga konkurencinėje rinkoje, „Android“ ir „iOS“ duopolyje. „Android“ telefonai kaupia milžinišką duomenų kiekį, kurį galima saugoti tiek vietiniu, tiek nuotoliniu būdu, todėl teismo ekspertams jie suteikia patikimų duomenų, kurie yra labai svarbūs teismo ekspertizei.

Šiame darbe siekiama sukurti dinamišką įrankį, skirtą duomenų išgavimui, analizei ir parengimui teismo ekspertizei. Įrankis sukurtas atsižvelgiant į tai, jog dauguma esamų įrankių nėra suderinami su visais „Android“ mobiliaisiais įrenginiais. Įrankio programavimui buvo naudojama „Shell Script“ kalba. Visos komandos buvo automatizuotos ir suskirstytos į skirtingus skriptus, kurie palengvina teismo ekspertizės analizę. Šis įrankis gali būti paleistas „Linux“ ar „Windows“ (su „Windows Subsystem for Linux“) operacinėse sistemose. Norint išgauti duomenis, naudojama „ADB Shell“ komunikacija, naudojant root lygį, kuris pasiekiamas paleidus neoficialų atstatymo režimą. Tyrimo metu buvo atsižvelgta į skambučių žurnalo istoriją, SMS žinutes, naršyklės istoriją, nuotraukas ir kitus failus, kurie yra svarbūs teismo ekspertizei. Norint palengvinti tolimesnę duomenų analizę, jie yra suskirstomi į aplankus.

Darbo eigoje sukurta priemonė išgauna įrenginio duomenų particijos atvaizdą, jį išsaugo ir tinkamai suformatuoja išgautus duomenis taip, kad būtų patogu juos naudoti bylų sprendimui. Sukurtas įrankis veikia su dauguma „Samsung“ įrenginių, kurie neturi įjungto priverstinio šifravimo (angl. force encrypt) funkcijos. Jis taip pat gali būti pritaikytas duomenų ištraukimui iš kitų gamintojų įrenginių.

# Summary

## **Disk image forensics research in Android devices**

Smartphones have become one of the most commonly used communication devices due to their improved connectivity, functionality, and productivity. As smart technologies continue to advance, new levels of potential risks emerge. The majority of the market relies on Android operating system phones, which holds a significant position in the competitive market, forming an Android-iOS duopoly. Android devices store a vast amount of data, which can be stored locally or remotely, providing forensic experts with reliable data that is crucial for forensic investigations.

The objective of this coursework is to develop a dynamic tool for data extraction, analysis, and preparation for forensic examination. The tool has been developed considering the fact that most existing tools are not compatible with all Android mobile devices. The tool has been programmed using the Shell Script language, utilizing commands that have been automated and divided into separate scripts, which facilitate forensic analysis. This tool can be used on Linux or Windows (with Windows Subsystem for Linux) operating systems. To access the data, ADB Shell communication is utilized on the root level, which can be achieved by booting into an unofficial recovery mode. During the development, considerations have been made for call log history, SMS messages, browser history, photos, and other files that are relevant to forensic examination. Data is organized into directories to facilitate further analysis.

The developed tool extracts the data partition image of the device, saves it, and properly formats the extracted data for convenient use in case resolution. This tool works with most Samsung devices that do not have the force encrypt feature enabled, and it can also be adapted for devices from other manufacturers.

# Ivyadas

**Darbo aktualumas** Mobilieji telefonai per pastaruosius metus tapo populiariūs dėl savo didelio funkcionalumo, prieinamumo ir produktyvumo. Tačiau šios pažangios technologijos taip pat atnešė naujų iššūkių ir pavojų, ypač kriminalistikoje. Kriminalistinėje veikloje mobilieji įrenginiai tapo duomenų kaupimo ir komunikacijos priemonėmis, o juose sukaupti duomenys tapo svarbia medžiaga teisminėse ekspertizėse.

**Darbo problema** Duomenų tyrimai rankiniu būdu užima daug laiko bei yra mažiau tikslūs ir saugūs, nes daugumą procedūrų norint išgauti duomenis yra pasikartojančios ir galėtų būti automatizuotos naudojant skriptus, kurie automatiškai išgautų duomenis iš atvaizdo. Be to, pats atvaizdo sukūrimas sudaro galimybes efektyvesnei analizei, nes keli darbuotojai gali dirbti su tuo pačiu atvaizdu, pasidalinti darbais. Deja, dėl žymių skirtumų tarp skirtingų mobiliųjų telefonų modelių bei operacinės sistemos variacijų, labai sunku sukurti įrankį, kuris automatiškai tikėtų kiekvienam telefonui, be jokių modifikacijų. „Android“ operacinėje sistemoje su kiekvienu atnaujinimu, duomenų pasiekimo kelias gali būti ribojamas. Mobilieji telefonai su „Android“ operacine sistema vis dažniau vartojami, todėl dažnai tenka daryti jų teisminę ekspertizę. Sukurtas įrankis palengvintų darbuotojams duomenų išgavimo procesą.

**Darbo objektas.** Prijungus telefoną, sukūrus jo disko atvaizdą, sumontavus (angl. mounted) jį bei išgavus ir apdorojus duomenis, tyrėjas galėtų atlikti daug kokybiškesnį bei greitesnį darbą, naudojant automatizuotą įrankį. Įrankio veikimo principas paprastas - kompiuteryje įrašytas įrankis prisijungia prie telefono, ištraukia atminties atvaizdą, pasiekia jame esančią informaciją, tvarkingai ją suformatuoja ir paruošia tolimesniam tyrimui. Įrankis turėtų išgauti duomenis vienu tisa tvarką, nes bet koks vientisumo pažeidimas sunaikintų duomenų integralumą.

**Darbo tikslas.** Darbo tikslas yra sukurti automatizuotą įrankį, kuris ištirtų „Android“ įrenginį ir palengvintų jo tyrimo procesą. Šis darbas aprašo, kaip galima atlikti mobiliųjų telefonų, veikiančių su „Android“ operacine sistema, teisminę ekspertizę.

## Darbo uždaviniai:

- Apžvelgti Android įrenginio architektūrą
- Pademonstruoti veikimo modelį
- Apžvelgti sukurto įrankio funkcionalumą
- Aprašyti ateities planus tyrimui

# 1. Susijusių darbų analizė

Sparčiai besivystančioms informacinėms technologijoms reikalingi metodai skirti atlikti efektyvią kompiuterinių ar mobiliųjų diskų ekspertizę. Šioje srityje yra sukurti keli programinės įrangos įrankiai, tačiau dauguma jų yra mokami, komerciniai ar uždaro kodo. Negalime naršyti šių įrankių šaltinio kodų ir giliau nagrinėti jų veikimo principo.

„Android“ įrenginių ekspertizėms sunku sukurti universalų programinį įrankį, nes „Android“ įrenginiai skiriasi savo architektūromis, duomenų kaupimo būdu ar operacinės sistemos versijomis (pvz. 9,10,11...) ir variantais (pvz. MIUI, Samsung OneUI, Huawei EMUI...). Skirtumai sutinkami taip pat sistemos saugumo lygiuose, failų struktūrose. Remiantis kitų mokslinių tyrėjų darbų išvadomis, galime teigti jog universalus ir automatizuotas įrankis dar nesukurtas [1] [2]

Net jau ir sukurti įrankiai, po „Android“ įrenginio sistemos atnaujinimo, gali nustoti veikti. Kadangi įrenginiai yra dažniausiai naujinami per 2-3 metus gamintojo teikiama saugumo naujiniais. Gali iškilti atvejis, kai įrenginys veikiantis su 2023m gegužės naujiniu bus sėkmingai panaudotas su įrankiais, o toks pats įrenginys su 2023m. birželio naujiniu jau nesuveiks. Policija ir kitos valstybės saugumo institucijos turi sukurtus tam tikrus įrankius, tačiau jie plačiai visuomenei nėra prieinami. Greičiausiai naudojamos CVE ar „zero-day“ spragos, kurios suteikia galimybę pasiekti duomenis daugumoje įrenginiu. Dėja tai reikalauja žinių bei skirti daug laiko kiekvienam atvejui.

Tokių problemų nėra kompiuterių srityje. Galima teigti jog visi kompiuteriai, kuriuos naudojame, veikia su viena iš trijų pagrindinių operacinių sistemų: „Windows“, „Linux“ bei „MacOS“. Šios operacinės sistemos duomenis užrašo į atskirą diską (mechaninį HDD ar puslaidinikinį SSD), kurį galime atskirai atjungti nuo įrenginio ir analizuoti jį su daugeliu pažengusių įrankių leidži. Tokie įrankiai leidžia išgauti ištrintus failus, praleisti slaptažodžius ar lengvai sukurti bitines disko kopijas. Remiantis „Windows Surface RT tablet forensics“ moksliniu darbu, galime teigti jog „Windows“ įrenginiams yra sukurta daug ekspertizių metodų. [3] Sukurtų įrankių yra daug, bet deja jie veikia tik su kompiuteriais, o ne mobiliais įrenginiais. Kompiuterių tyrimo atvejams yra sukurta metodika bei programinė įranga, kuria sekant galime lengvai atlikti tyrimą. „Android“ įrenginiams tokia metodika dar nėra sukurta

## 2. Android įrengino architektūra

Šiame skyriuje apžvelgiami operacinės sistemos veikimo principai bei versijos, kurios yra esminė informacija reikalinga sėkmingam duomenų

### 2.1. Operacinės sistemos architektūra

Įrenginiai su „Android“ operacine sistema, skiriasi nuo tradicinių kompiuterių. Architektūrų skirtumai matomi tiek apatinėje įrangoje (angl. hardware) tiek skirtingose operacinėse sistemose. „Android“, kaip ir „Linux“, priklauso tai pačiai „UNIX“ operacinių sistemų šeimai, tačiau ji žymiai skiriasi nuo tradicinės Linux aplinkos.[4]

Mobiliųjų telefonų ekspertizės atveju, duomenų išgavimo procesas žymiai skiriasi nuo kompiuterių diskų analizės. [5] Analizuojant nešifruotus Linux ar Windows kompiuterių diskus, galima juos gan lengvai prijungti prie kito kompiuterio ir išgauti juose esančius duomenis. „Android“ įrenginiuose duomenų išgavimo procesas gali būti žymiai sudėtingesnis, dėl skirtingų operacinės sistemos versijų, bei saugumo ar paleidimo įkroviklio (angl. bootloader), kuris yra atsakingas už įrenginio operacinės sistemos paleidimą, variacijų [6].

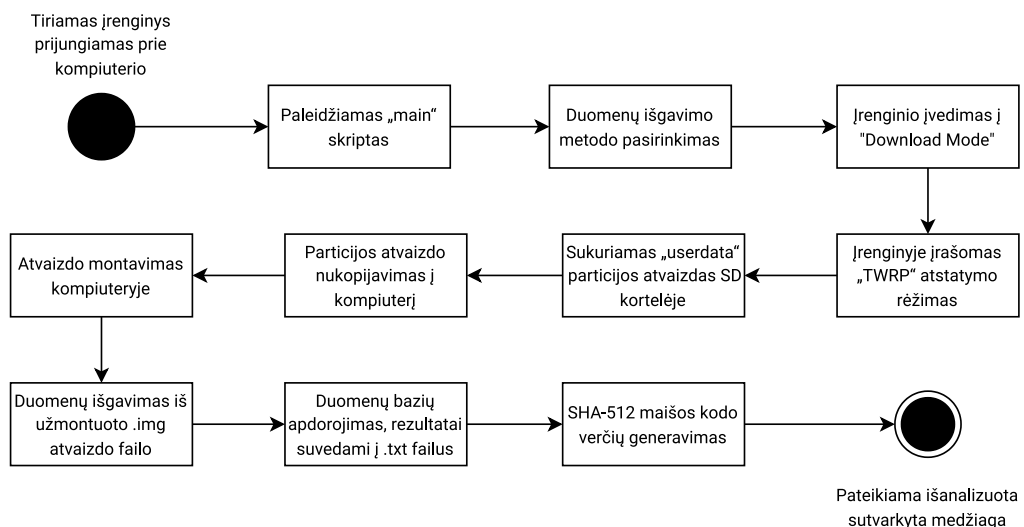
### 2.2. Versijos

„Android“ įrenginiuose, svarbu atkreipti dėmesį į operacinės sistemos versiją, nes priklausomai nuo jos, duomenų pasiekimas gali būti apsunkintas ar neįmanomas. „Android“ operacinės sistemos pirma versiją „1.0“ išleista 2008 m. [7] Šiais metais jau pasiekiamą „13“ versiją, ir sistema toliau tobulinama. Prieš pradėdant darbą, svarbu patikrinti sistemos versiją.

Norint sėkmingai panaudoti ekspertizei sukurtą įrankį, būtina susijungti su telefonu ir jam suteikti „root“ teises. Alternatyviai galime paleisti jį neoficialiame atstatymo režime, (angl. „custom recovery“), kuriame turime prieigą prie visos telefono atminties ir dirbame kaip „root“ vartotojas.

## 3. Įrankio veikimas

Žinant svarbiausius architektūros elementus, galime sukurti veikimo modelį (1 pav.):



1 pav. UML veiklos diagrama



Norint pradėti duomenų išgavimo procedūrą, reikia paleisti „main“ skriptą, pasirinkti norimą funkciją ir prijungti įrenginį prie kompiuterio naudojant USB laidą. Paleidus įrankį, vykdomi veiksmai, atitinkamai nuo pasirinktos įrankio funkcijos: disko atvaizdo automatinis išgavimas, disko atvaizdo rankinis išgavimas, duomenų išgavimas iš disko atvaizdo, išgautų duomenų bazių išvedimas į skaitomą .txt failą ar atvaizdo išgavimas TWRP režime. Atvaizdas kopijuojamas į kompiuterį. Atvaizdas montuojamas, ir iš jo išgaunami duomenys. Išgautos duomenų bazės yra analizuojamos, ir jų rezultatai, kartu su visais kitais reikiama failais, pateikiami viename aplanke.

## 4. Įranga bei jos paruošimas

Tyrimo praktinėje dalyje naudojau du mobiliuosius įrenginius - „Samsung Galaxy S3 Neo“ („Android“ versija 4.4.2) ir „Samsung Galaxy S5“ („Android“ versija 6.0.1). Abu įrenginiai buvo sėkmingai panaudoti numatytiems praktinės dalies veiksmams. Testams buvo planuojama naudoti dar tris modelius: „Google Nexus 5“ („Android“ versiją 6.0.1), „Oneplus 2“ („Android“ versija 6.0.1) bei „Samsung Galaxy S20 FE“ („Android“ versija 13), tačiau jie neatitiko šiam įrankiui. „Google Nexus 5“ kaip ir „Oneplus 2“ neturi galimybės prijungti microSD kortelės, tad atvaizdo išgavimas būtų buvęs sunkus. Pagrindinė problema yra panaudotas paleidimo įkroviklis (angl. „bootloader“). Šie įrenginiai naudoja „fastboot“ paleidimo įkroviklį. Norint panaudoti „custom recovery“ metodą, reikėtų atrakinti paleidimo įkroviklį, tuo pačiu ištrinant visus duomenis. Įrenginiams buvo galimybė suteikti „root“ teises naudojant programėlę „KingRoot“, bet šiam procesui telefonas turi būti be ekrano užrakto.

Programėlė „Kingroot“ suteikianti „root“ teises vienu paspaudimu jau neveikia [8]. „Kingroot“ serveriai bei tinklalapis „www.kingroot.net“ neveikia, be to programėlė nėra pilnai saugi, nes jungiasi prie kiniškų serverių[9], bei naudoja saugumo CVE spragas, norint suteikti „root“ teises, todėl būtina naudoti alternatyvius metodus. [10]

„Samsung Galaxy S20 FE“ yra originaliai šifruojamas su „force encrypt“ funkcija. Šiai dienai, nėra galimybės išgauti duomenų iš šifruoto įrenginio, o net jeigu pavyktų duomenis išgauti, jų iššifravimas gali trukti ilgai, ar reikalauti superkompiuterio.

Dėl šių priežasčių darbą atlikau su „Samsung Galaxy S3 NEO“ įrenginiu. Jis neatitiko „KingRoot“ reikalavimų, todėl įrenginiui sukūriau skriptą, kuris įrašo neoficialų „TWRP“ (Team Win Recovery Project) [11] atstatymo režimą. Dirbant atstatymo režime, galime išgauti duomenis iš įrenginio net ir su ekrano užraktu. Duomenų išgavimas su ekrano užraktu reikalauja rankiniu būdu įvesti įrenginį į „Download mode“ įrašymo būseną.

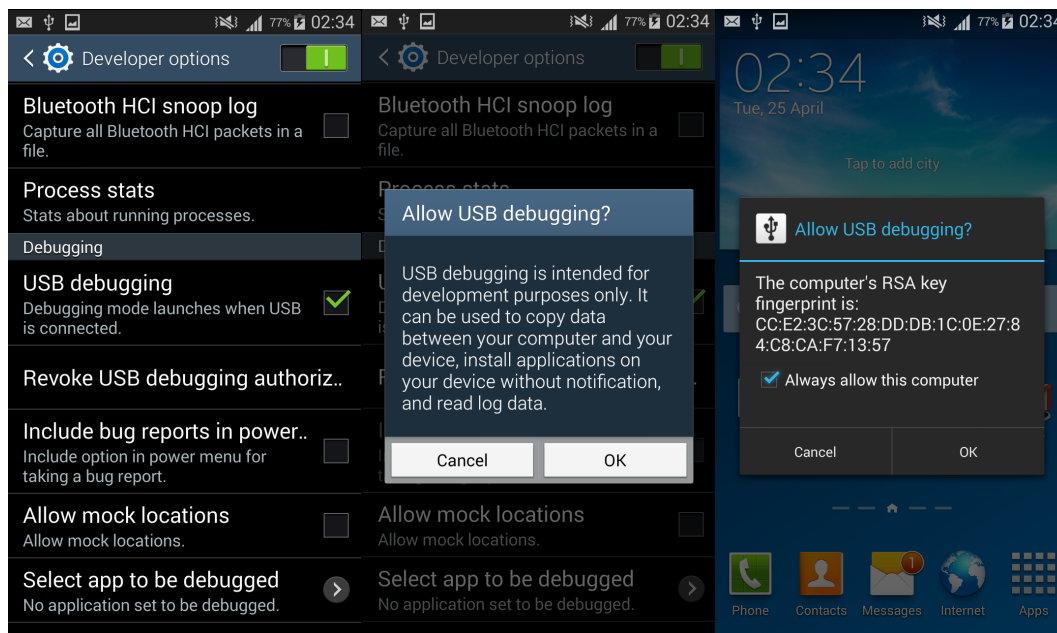
Atvaizdo sukūrimui reikalinga microSD kortelė kurios talpa didesne negu vidinės telefono atminties talpa. Yra galimybė atvaizdą gauti naudojant TCP/IP sujungimą, jeigu dirbame su root teisėmis operacinėje sistemoje. Deja, atstatymo režime nėra galimybės prijungti prie tinklo.

Įrenginio analizei reikalingas kompiuteris. Duomenų ištraukimas gali vykti „Windows“ bei „Linux“ operacinėse sistemose. Rekomenduojama naudoti Linux, bet įrankis gali būti panaudotas ir Windows operacinėje sistemoje, su „Windows Subsystem for Linux“ [12], kuriame yra galimybė įdiegti reikiamus įrankius bei paleisti „Bash“ skriptą. Tokiu atveju reikia papildomai įdiegti reikiamas tvarkykles (angl. device driver)

Norint įrašyti į įrenginį neoficialų atstatymo režimą ir jį paleisti, galime naudoti atviro kodo „Heimdall“ įrankį [13]. Naudojamas taip pat „ADB“ (angl. „Android Debug Bridge“) įrankis, kuris leidžia sujungti kompiuterį su mobiliu įrenginiu. Duomenų analizei reikalingas „sqlite3“ paketas, kuris padės apdoroti duomenis iš atvaizde esančių duomenų bazių.

## 5. Įrankio paleidimas bei duomenų išgavimas

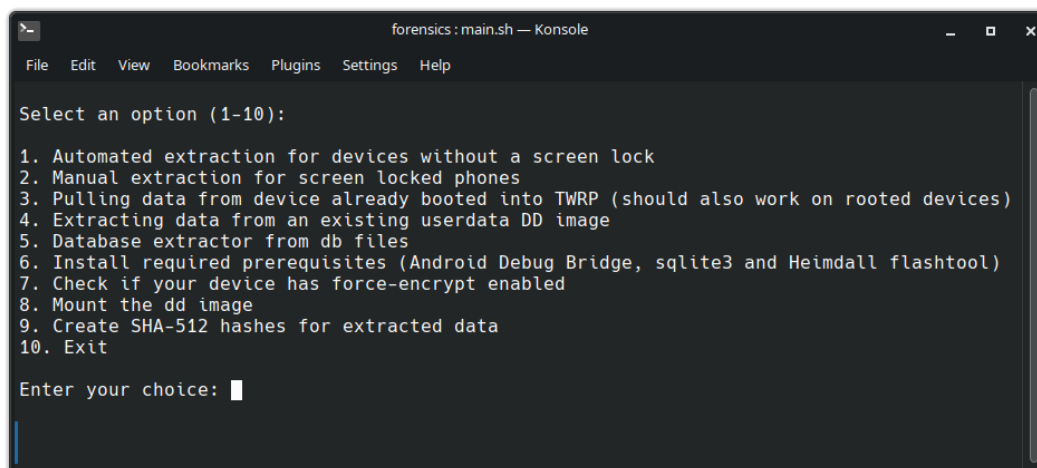
Priklausomai nuo pasirinkto metodo, norint išgauti duomenis automatinio būdu arba patikrinti „force-encrypt“ būseną, būtina įrenginyje įjungti USB derinimą (angl. „USB Debugging“). Tai galime padaryti menu „Kūrėjų parinktys“ (angl. Developer options) (2 pav.):



2 pav. USB derinimas

Esant įrankio darbo aplanke, atveriamės konsolės langą ir su komanda „./main.sh“ paleidžiame pagrindinį skriptą (skriptas paleidžia vieną iš devynių galimų skriptų esančių „bash“ aplanke). Kad įrankis sklandžiai veiktų, leidžiamam skriptui reikia suteikti aukštesnes teises. Tam naudojame „sudo“ komandą. „Sudo“ yra Linux operacinės sistemos komanda, kuri leidžia vartotojams vykdyti komandas su aukščiausiomis „root“ teisėmis. Tai reiškia, kad naudotojas gali turėti aukštesnį leidimų lygį ir atlikti daugiau operacijų. Veikimo principas panašus kaip administratoriaus teisės „Windows“ operacinėje sistemoje.

Paleidus ./main skriptą, su „sudo“ teisėmis, pasirodys menu su daugeliu parinkčių (3 pav.):



3 pav. Įrankio pagrindinis menu

## 5.1. Įrankio atvaizdo gavimas automatiškai (1) atveju

1. Paleidus skriptą suteikiame „sudo“ teises.
2. Pirmą kartą paleidus įrankį, būtina įdiegti reikiamas bibliotekas bei programas - „ADB“, „heimdall-flash“ bei „sqlite3“. Pasirenkame parinktį, bei naudojamą operacinę sistemą. Kai įrankiai įsidięs, paspaudus bent kokį klavišą grįžtame į pagrindinį menu.
3. Parenkame pirmąjį skriptą, kuris skirtas automatiniam duomenų išgavimui.
4. Skriptas sukuria „extracted\_data“ bei „mounted\_dd“ aplankus. Pirmasis skirtas išgautų duomenų bei rezultatų saugojimui, o antrasis naudojamas kaip montavimo katalogas (angl. „mount point“) įrenginio disko atvaizdui.
5. Skriptas patikrins ar įrenginys prijungtas su USB derinimo režimu. Paprašys jį įjungti bei patvirtinti.
6. Paspaudus klavišą, įrankis įrašys (angl. flash) neoficialų atstatymo režimo atvaizdą. Šiam tikslui naudojamas atviro kodo įrankis „heimdall“, skirtas daugumai telefonų įrašinėti (angl. flash).
7. Įrankis reikalaus fiziškai nuspausti reikiamus mygtukus, kad mobilų įrenginį įvesti į atstatymo režimą.
8. Skriptas patikrins ar įrenginys atitinkamai atskaitomas „ADB“ aplinkoje.
9. Jeigu taip įvyks, įrankis išspausdins particijų lentelę, kurioje vartotojas turės įrašyti atitinkamą particijos pavadinimą, kurios etiketė „userdata“. Pavadinimas įrašomas mmcblk0pXX formatu rankiniu būdu, tam kad skriptą būtų galima pritaikyti kitiems mobiliems įrenginiams o ne tik šiam konkrečiam modeliui.
10. Parinkus particiją, įrankis reikalaus suformatuoti ankščiau užmontuotą microSD atminties kortelę į „exFAT“ arba „EXT4“ failų sistemą. Formatavimas būtinas, nes dauguma kortelių būna suformatuotos „FAT32“ failų sistema, kuri neleidžia sukurti didesnio nei 4GB failo.
11. Įrankis pradeda kurti bitinį „userdata“ particijos atvaizdą.
12. Naudojant „adb pull“ komandą, skriptas nukopijuoja atvaizdą į kompiuterio darbo aplanką.
13. Kai atvaizdas jau nukopijuotas, visi duomenys esantys įrenginyje yra išsaugoti kompiuteryje.
14. Įrankis gražina originalų „recovery“ atvaizdą, kad įrenginys išliktų originalioje būsenoje.
15. Įrankis užmontuoja „userdata“ particiją ir iš jos ištraukia duomenis.
16. Paspaudus bet kokį klavišą, grįžtama į pagrindinį menu.
17. Iš pagrindinio menu reikia pasirinkti duomenų bazių ekstrakcijos funkciją, kad „extracted\_db“ aplanke susikurtų tekstiniai failai su reikiama duomenimis.
18. Pasirinkus „Exit“ funkciją, įrankis užbaigia darbą. Visi duomenys tvarkingai apdoroti teisminei analizei yra sukaupiti „extracted\_data“ aplanke.

## **5.2. Įrenginio atvaizdo gavimas rankiniu (2) atveju**

Norint išgauti duomenis iš įrenginio, kuris užrakintas/apsaugotas ekrano užraktu, būtina naudoti antrą skriptą.

Skripto veikimui nebūtinai reikalingas USB derinimas, bet būtina rankiniu būdu įvesti įrenginį į „Download mode“ įrašymo (angl. flashing) režimą. Spaudžiame ir prilaikome „volume down + home + power“ klavišus, ir patvirtiname „volume up“ klavišu.

Veliau, visi veiksmai vyksta kaip aukščiau, nuo 5.1.6-5.1.13 bei 5.1.15-5.1.18

## **5.3. Įrenginio atvaizdo gavimas iš įrenginio jau paleisto „TWRP“ režime (3) atveju**

Naudojant kito gamintojo ar modelio įrenginį, kuriame jau radome būdą kaip įrašyti ir paleisti „TWRP“ atstatymo režimą, galime naudoti šią parinktį. Veliau, visi veiksmai vyksta kaip aukščiau, nuo 5.1.8-5.1.13 bei 5.1.15-5.1.18

## **5.4. Duomenų išgavimas iš jau turimo userdata.img dd atvaizdo (4) atveju**

Jeigu turime jau egzistuojantį įrenginio „dd“ atvaizdą, galime jį apdoroti. Pasirinkus šią funkciją, nurodome atvaizdo vietą (angl. path). Įrankis užmontuoja atvaizdą, bei išgauna iš jo reikiamus duomenis ir išsaugoja juos „extracted\_data“ aplanke. Iš pagrindinio menu reikia pasirinkti duomenų bazių ekstrakcijos funkciją, kad „extracted\_db“ aplanke susikurtų tekstiniai failai su reikiama duomenimis. Pasirinkus „Exit“ funkciją, įrankis užbaigia darbą

## **5.5. Duomenų bazių analizė ir duomenų išvedimas į skaitomus .txt failus (5) atveju**

Pasirinkus šią funkciją, įrankis apdoroja .db failus, esančius extracted\_data aplanke. Skriptas gali analizuoti:

- SMS/MMS duomenų bazes
- Kontaktų duomenų bazes
- Skambučių registro duomenų bazes
- Kalendoriaus įvykių duomenų bazes
- Naršyklės duomenų bazes
- Elektroninio pašto (e-Mail) duomenų bazes

Skriptas naudoja sqlite3 paketą, kad apdoroti duomenų bazes su SQL užklausomis. Po apdorojimo, rezultatai išvedami į tekstinius failus tokius kaip: messages.txt, contacts.txt, calendar.txt, login\_data.txt, cookies\_data.txt, call\_logs.txt, browsing\_history.txt.

Įrankis gali taip pat išgauti užrašytus naršyklėje slaptažodžius, kartu su prisijungimo vardu ir prisijungimo tinklalapio adresu. Šis funkcionalumas taip pat realizuojamas SQL užklausomis, nes slaptažodžiai „Google Chrome“ naršyklės duomenų bazėje yra saugojami paprastu tekstu (angl. plain text).

## 6. Įrankio panaudojimo rezultatai su skirtingais įrenginiais

Sukurtas įrankis gan universalus, bet neveikia su visais modeliais. Atlikau testus su keliais Android įrenginiais:

- Samsung Galaxy S3 NEO (s3ve3gxx - GT-I9301I)
  - Android versija 4.4.2,
  - paleidimo įkroviklis - „Samsung S-boot“
- Samsung Galaxy 5 (klte - SM-G900F )
  - Android versija 6.0.1 (bandyta taip pat su 4.4.4 bei 5.1.1)
  - paleidimo įkroviklis „Samsung S-boot“
- Google Nexus 5 (D821 - hammerhead)
  - Android versija 6.0.1 (bandyta taip pat su 4.4.4, 5.0,2 bei 5.1.1)
  - paleidimo įkroviklis „fastboot“
- Oneplus 2 (a2003 - oneplus2)
  - Android versija 6.0.1
  - paleidimo įkroviklis „fastboot“

### 6.1. Rezultatai su Samsung Galaxy S3 NEO įrenginiu

Įrankis buvo pagrindinai kuriamas ir testuojamas su šiuo įrenginiu. Visas funkcionalumas su šiuo įrenginiu veikia. Yra galimybė išgauti duomenis automatinio būdu be ekrano užrakto, bei rankiniu būdu su ekrano užrakto. Visi duomenys pasiekiami. Įrenginys turi microSD kortelių skaitytuvą, todėl nebuvo jokių problemų su atvaizdo išgavimu bei talpinimu.

Iš šio įrenginio pavyko išgauti visus reikiamus duomenis, t.y. :

- SMS/MMS duomenų bazes
- Kontaktų duomenų bazes
- Skambučių registro duomenų bazes
- Kalendoriaus įvykių duomenų bazes
- Naršyklės duomenų bazes

Elektroninio pašto (e-mail) duomenų nepavyko išgauti, nes įrenginyje esanti programėlė yra per sena. Nepavyko prisijungti prie Gmail nei Outlook pašto paskyros, todėl ši informacija nebuvo analizuojama.

### 6.2. Rezultatai su Samsung Galaxy S5 įrenginiu

Šis įrenginys buvo sėkmingai panaudotas duomenų išgavimui bei jų analizei. Tinka ir automatinis ir rankinis duomenų išgavimo būdas. Įrenginys turi microSD kortelių skaitytuvą, todėl nebuvo problemų su atvaizdo talpinimu. Deja įrenginys veikiantis „TWRP“ režime dėl kažkokios priežasties praranda USB sujungimą. Tada būtina kelis kartus atjungti ir prijungti USB laidą. Galutinai atvaizdas išgaunamas korektiškai ir iš įrenginio pavyko išgauti tokius pačius duomenis kaip ir iš Samsung Galaxy S3 NEO įrenginio.

### 6.3. Rezultatai su Google Nexus 5 ir Oneplus 2 įrenginiais

Google Nexus 5 įrenginio atveju nepavyko sėkmingai išgauti duomenų dėl kelių priežasčių: panaudotas paleidimo įkroviklis bei microSD kortelių skaitytuvo trūkumas.

Šiam įrenginiui yra galimybė įrašyti „TWRP“ režimą bei suteikti jam root teises, bet tam padaryti reikia atrakinti „fastboot“ paleidimo įkroviklį komanda „fastboot oem unlock“. Tai darant, visa įrenginio atmintis yra išvaloma, o duomenys esantys įrenginyje yra negrįžtamai sunaikinami.

Jeigu „fastboot“ paleidimo įkroviklis buvo įrenginyje atrakintas (pvz. dėl to kad įrenginio savininkas turėjo įrašytą neoficialią sistemą (angl. custom rom), įrankis galėtų įrašyti „TWRP“ režimą. Deja tai neleistų sukurti atvaizdo, nes kaip minėjau, Nexus 5 neturi microSD kortelių skaitytuvo. Galima išgauti duomenis iš šio įrenginio, paprastai kopijuojant juos iš įrenginio paleisto „TWRP“ režime, bet teisėtai galime dirbti tik su diskų atvaizdais, kas ir yra šio tyrimo tikslas.

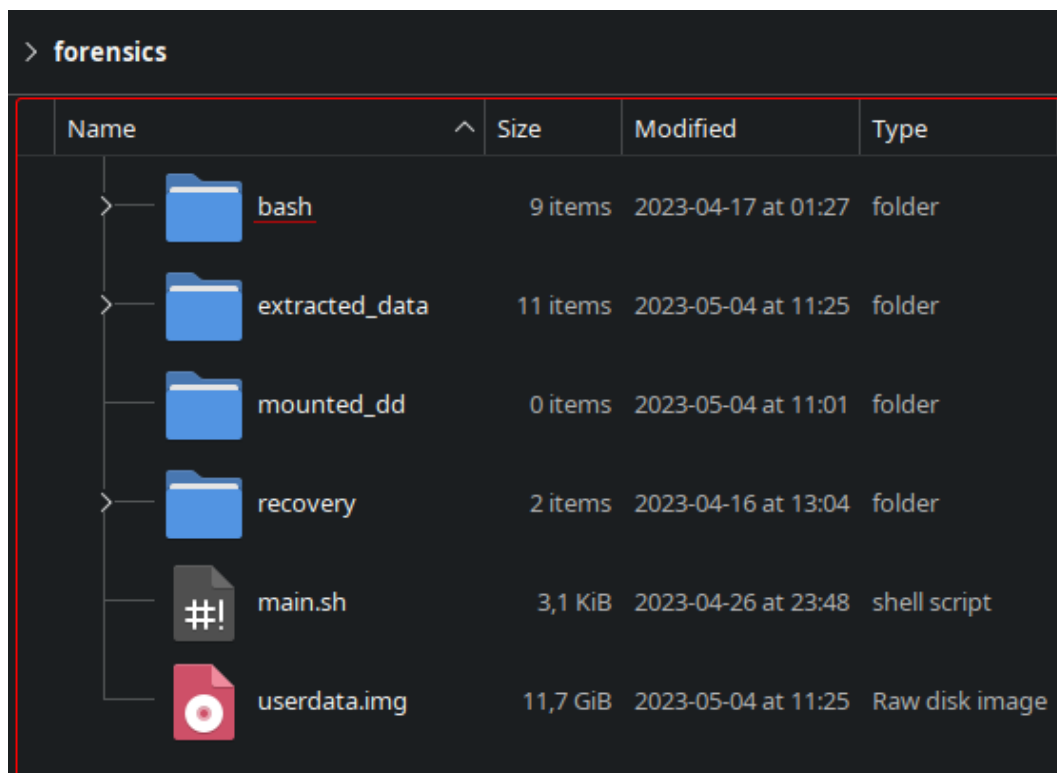
Lygiai toks pats atvejis yra ir su Oneplus 2 įrenginiu, naudojamas „fastboot“ paleidimo įkroviklis bei nėra microSD kortelių skaitytuvo. Šis įrankis netinka Nexus 5 bei Oneplus 2 įrenginiams.

## 7. Ištrauktų duomenų failų struktūra

Šiame skyriuje aptariama pagrindinė failų bei katalogų struktūra. Visi ištrauktieji failai yra talpinami CWD/extracted\_data kataloge. (CWD - current working directory)

### 7.1. Katalogų struktūra

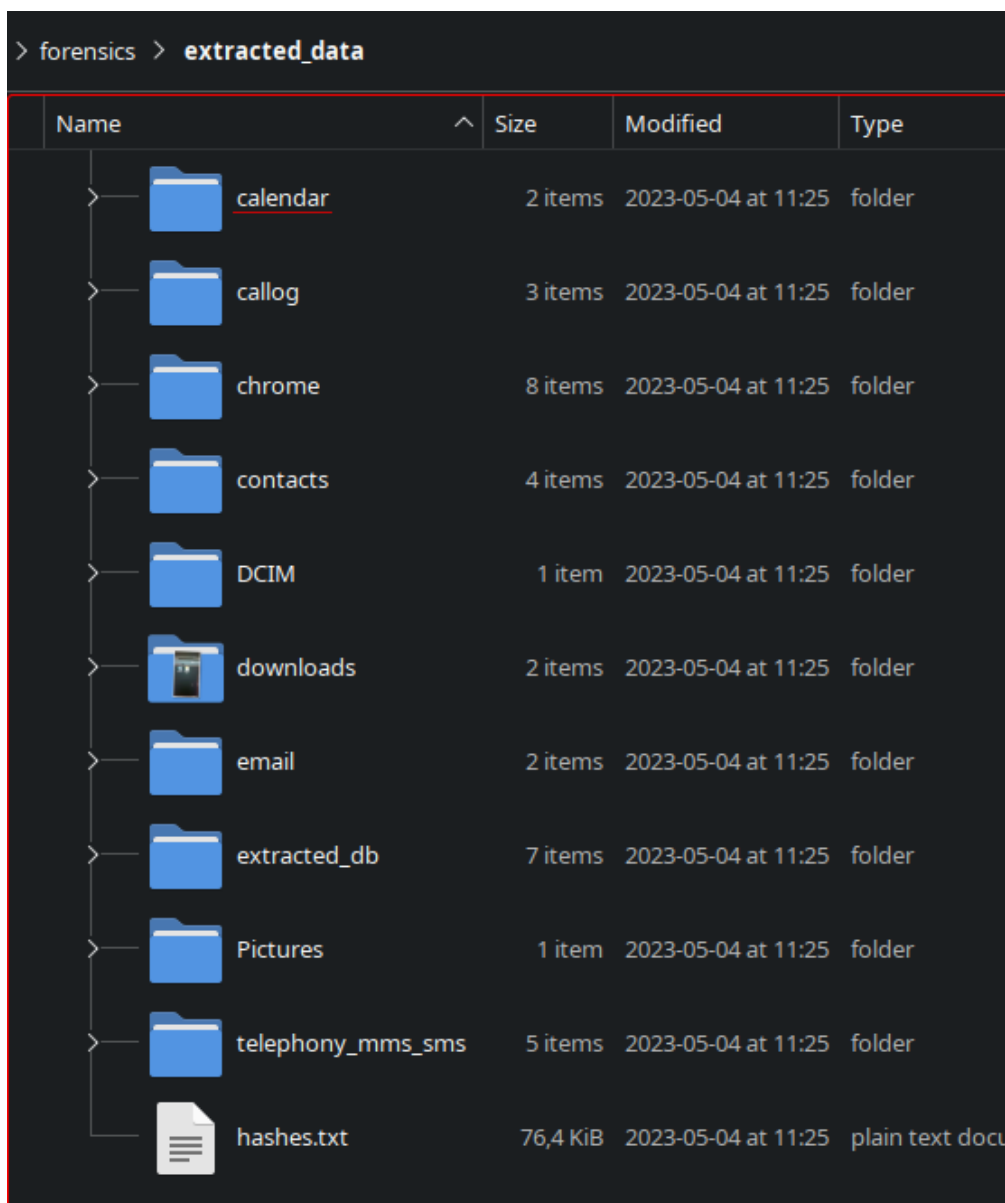
CWD darbo kataloge matome tokius failus bei katalogus (4 pav.):



> forensics					
	Name	Size	Modified	Type	
>	bash	9 items	2023-04-17 at 01:27	folder	
>	extracted_data	11 items	2023-05-04 at 11:25	folder	
	mounted_dd	0 items	2023-05-04 at 11:01	folder	
>	recovery	2 items	2023-04-16 at 13:04	folder	
	main.sh	3,1 KiB	2023-04-26 at 23:48	shell script	
	userdata.img	11,7 GiB	2023-05-04 at 11:25	Raw disk image	

4 pav. Darbo katalogo struktūra

Katalogas „bash“ talpina visus reikiamus skriptus. Katalogas „mounted\_dd“ yra skirtas „user-data“ atvaizdui užmontuoti. Katalogas „recovery“ saugo savyje du atstatymo režimo atvaizdus - vienas originalus išgautas iš „Samsung“ .tar.md5 originalios programinės įrangos atvaizdo, bei antras neoficialus „TWRP“ atvaizdas. Darbo kataloge taip pat talpinamas „main.sh“ failas bei „userdata.img“ ištrauktas atvaizdo failas. „extracted\_data“ kataloge talpinami visi išgauti bei išanalizuoti failai (5 pav.):



Name	Size	Modified	Type
calendar	2 items	2023-05-04 at 11:25	folder
callog	3 items	2023-05-04 at 11:25	folder
chrome	8 items	2023-05-04 at 11:25	folder
contacts	4 items	2023-05-04 at 11:25	folder
DCIM	1 item	2023-05-04 at 11:25	folder
downloads	2 items	2023-05-04 at 11:25	folder
email	2 items	2023-05-04 at 11:25	folder
extracted_db	7 items	2023-05-04 at 11:25	folder
Pictures	1 item	2023-05-04 at 11:25	folder
telephony_mms_sms	5 items	2023-05-04 at 11:25	folder
hashes.txt	76,4 KiB	2023-05-04 at 11:25	plain text docu

5 pav. Ištrauktų duomenų katalogo struktūra

Katalogai: calendar, callog, chrome, contacts, email, telephony\_mms\_sms saugo duomenų bazes ištrauktas iš userdata.img atvaizdo. Katalogai DCIM, Pictures, Downloads saugo failus, kurie buvo patalpinti įrenginio vidinėje atmintyje. Katalogas extracted\_db talpina išanalizuotų duomenų bazių rezultatus. Failas hashes.txt talpina SHA-512 maišos kodą visiems failams, kad būtų galima lengvai palyginti ar failai nebuvo modifikuoti tarp jų išgavimo ir perkėlimo į kitą kompiuterį.

Visi reikalingi analizei failai yra sukaupti šiame kataloge, ir šį katalogą reikėtų pateikti teismui kaip įrodymus.

## 7.2. Išanalizuotų .db failų apžvalga

Šiame poskyryje matomos iliustracijos, rodo tyrimo metu išgautus iš „Samsung Galaxy S3 NEO“ įrenginio duomenis. Visi šie duomenys buvo sukurti ir parengti šiam darbui - žinutes, skambučiai, kontaktai, kalendoriaus įrašai bei naršyklės duomenys buvo specialiai parengti šiam tyrimui. Visi vardai, telefono numeriai bei žinučių turinys yra fiktyvus.

6 pav. matome dalį išanalizuoto messages.txt failo. Faile duomenys grupuojami pagal telefono numerius ir surašomi pagal datą.

```
1 | Conversation with +3706554582 |
2 | 2023-03-27 21:01:49 | sent: | Labas, skambinu del siuntinio. Susitiksime rytoj 12val prie Didlaukio stoteles
3 | 2023-03-27 21:03:19 | sent: | Kai galesi atskambink ar atrasyk, Tomas jau zino apie kroviniu perdavima
4 |
5 | Conversation with +37061912217 |
6 | 2023-03-27 21:57:45 | received: | Viskas okei, tikslus perdavimo adresas: didlaukio stoteles apylinkėje rasi juoda kuprine. Su kuo ir
7 | kiek pats zinai
8 | 2023-03-27 21:58:19 | sent: | Busiu su Tomu ir Paulium
9 | 2023-03-27 21:59:51 | received: | Buk pats, nebereikia tiek daug zmonių, dar kazkas uzkalbins.
10 | 2023-03-27 22:06:31 | sent: | Taip kaip kalbejom, busiu pats, Tomo nebus o Pauliui negaliu prisiskambint. Tikiuosi nebus isdavikas
11 | 2023-03-27 22:06:59 | received: | iki rytojaus
12 |
13 | Conversation with +37062545425 |
14 | 2023-03-27 04:18:40 | sent: | Labas
```

6 pav. Žinučių .txt failas

7 pav. matome dalį išanalizuoto login\_data.txt failo. Matome prisijungimo URL adresą, prisijungimo vartotojo vardą bei slaptažodį.

```
1 | URL: https://accounts.google.com/v3/signin/challenge/pwd
2 | Username: matascriminal@gmail.com
3 | Password: Ma1922noCriminal
4 |
5 |
```

7 pav. Prisijungimo duomenų .txt failas

8 pav. matome dalį išanalizuoto cookies\_data.txt failo. Matome slapukų kilmę, bei jų vertes.

```
1 | Host: .google.com
2 | Name: CONSENT
3 | Value: PENDING+627
4 | Encrypted Value: |13325597197998264|13388669197998264
```

8 pav. Cookies slapukų .txt failas

9 pav. matome dalį išanalizuoto browsing\_history.txt failo. Matome puslapio pavadinimą, URL adresą bei jo atidarymo datą ir valandą.

```
1 | {
2 |
3 | "Title": "https://consent.google.com/ml?continue=https://www.google.com/
4 | search%3Fq%3Dsketchy%2Bwebsite%26oq%3Dsketchy%2Bwebsite%26client%3Dms-android-samsung%26sourceid%3Dchrome-
5 | mobile%26espv%3D1%26ie%3DUTF-8%26gws_rd%3Dssl&gl=PL&m=1&pc=srp&uxe=none&hl=pl&src=1 is not available",
6 |
7 | "URL": "http://www.google.com/search?q=sketchy+website&oq=sketchy+website&client=ms-android-
8 | samsung&sourceid=chrome-mobile&espv=1&ie=UTF-8",
9 |
10 | "Last Visit Time": "2023-04-10 10:46:38"
11 | }
```

9 pav. Naršyklės istorijos .txt failas



10 pav. matome dalį išanalizuoto call\_logs.txt failo. Matome skambučio datą, telefono numerį, skambučio trukmę sekundėmis bei tipą: 1- išeinantis skambutis, 2 - įeinantis skambutis.

```
1 SDate: 2023-03-27 22:03:31
2 Duration: 84
3 Number: +37061912217
4 Name: Martin
5 Type: 2
6
```

10 pav. Skambučių istorijos .txt failas

11 pav. matome dalį išanalizuoto contacts.txt failo. Matome užrašytus adresų knygėlėje kontaktus su jų pavadinimais bei telefono numeriais.

```
1 Paulius | +37060554582
2 Telekonferencija | +37061900999
3 Martin | +37061912217
4 Tomas | +37062545425
5 SOS 112 | 112
6 Infolinija | 117
7 Konsultacijos | 1533
8 Telefono saskaita | 1544
9 Paslaugu valdymas | 1566
10 Aldona | 625487348
11 Povilas | 652437634
12
```

11 pav. Kontaktų .txt failas

12 pav. matome dalį išanalizuoto calendar.txt failo. Matome užrašytą įvykį su jo data, pavadinimu, bei komentarais.

```
1 Didkaukio st juoda kuprine. | Nueiti butinai | 2023-03-28 12:00:00 | 2023-03-28 13:00:00
2
```

12 pav. Kalendoriaus.txt failas

Visi failai yra talpinami viename kataloge, bei yra užrašyti .txt formatu, kad būtų galima juos atidaryti ir peržiūrėti kiekvienoje operacinėje sistemoje. Šie failai yra itin svarbūs analizei, nes juose galime rasti daug vertingos informacijos. Dėl to kad su testuojamu įrenginiu nukeliavau į kitą valstybę, galime gauti konkrečią datą ir valandą kada buvo peržengta valstybės sieną (13 pav.):

```
25 |
26 Conversation with Telia |
27 2023-04-10 13:40:15 | received: | EŽYS sveikina tave Lenkijoje! Klientų aptarnavimo tel. +37064181817. Nemokamas
  pagalbos telefonas 112 . Nelaimės atveju konsulinės pagalbos tel.+37052362444 (visą parą). Jei turi planą ar
  akciją su minučių, SMS ir interneto naudomis, galiojanti ir ES/EEE šalyse, šios naudos galios ir Lenkijoje. Jei
  naudojiesi standartiniais tarifais Lietuvoje, Lenkijoje tau galios tie patys tarifai, kaip ir Lietuvoje, t.y.
  išeinantiems skambučiams ES/EEE viduje - 0.22 €/min., SMS - 0.07 €. Primename, kad ES/EEE šalyse taikomas
  mobiliųjų duomenų limitas pagal turimą planą. Tau galiojančias planų naudas ir standartinius tarifus sužinosi
  nemokamu tel. +37069851000 arba www.ezys.lt. Atkreipk dėmesį, kad skambučiai / SMS į tam tikrus numerius (pvz.
  800 serija) yra apmokestinami padidintu tarifu. ES pasienio teritorijose gali netyčia prisijungti prie brangesnio
  tinklo - kad to išvengtum pasirink ES tinklą rankiniu būdu. Latvijoje ir orlaiviuose gali būti taikomi aukštesni
  tarifai dėl palydovinio ryšio - norėdami to išvengti, įjunkite skrydžio režimą. Daugiau informacijos: https://
  ezys.lt/planai/tarptautiniai-tarifai. Geros kelionės!
28
```

13 pav. SMS žinutė nuo tinklo operatoriaus apie valstybės sienos peržengimą

## Išvados ir rekomendacijos

Sukurtas įrankis, turi daug funkcionalumų. Gali automatiškai arba rankiniu būdu išgauti duomenis iš daugelio mobiliųjų įrenginių. Įrankis tinkamas telefonams su ekrano užraktu bei be ekrano užrakto. Įrankis gali ištraukti duomenis iš „Android“ įrenginio „userdata“ partitijos atvaizdo, bei gauti juos iš įrenginio, kuris jau paleistas „TWRP“ režime. Darbo eigoje sukurtas įrankis gali taip pat ištraukti ir apdoroti SMS, kontaktų, skambučių, bei naršyklės duomenų bazes. Taip apdorota medžiaga gali būti panaudota teisminei ekspertizei. Skriptas turi daug informacinių dialogų, kurie leidžia vartotojui lengvai suprasti kas vyksta ir kokius žingsnius reikia įvykdyti, kad duomenų išgavimas vyktų sklandžiai.

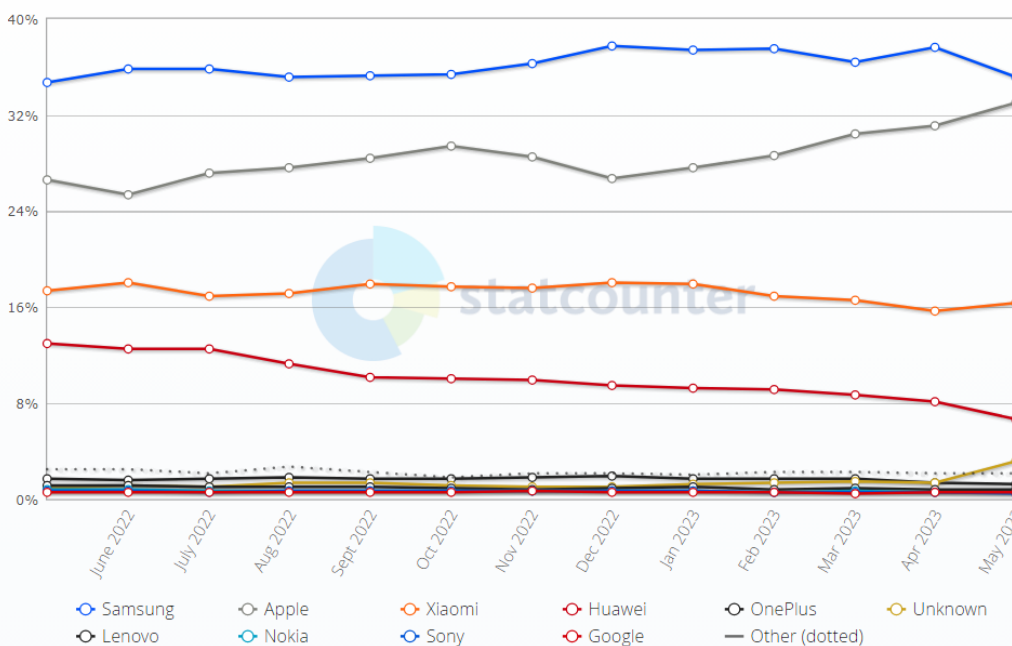
Įrankis veikia su daugeliu Samsung įrenginių, bei su kitais įrenginiais, kuriems turime galimybę suteikti „root“ teises arba įrašyti neoficialų atstatymo režimą.

Darbo metu atliktame tyrime panaudotas įrankis sėkmingai ištraukia duomenis iš „Samsung Galaxy S5“ (veikiančio su naujausia jam prieinama „Android 6.0.1“ versija) bei „Samsung Galaxy S3 NEO“ (veikiančiu su naujausia jam prieinama „Android 4.4.4“ versija). Iš šių mobiliųjų įrenginių pavyko išgauti visus analizei vertingus failus, o prireikus, tolimesnei analizei, įrankis suteikia galimybę sumontuoti atvaizdą ir atlikti analizę rankiniu būdu, analizuojant kitų programėlių duomenų bazes.

Įrankis ne tik išgauna duomenis, bet ir juos tinkamai suformatuoja, į lengvai skaitomus tekstinius failus. Šis funkcionalumas leidžia žmonėms kurie niekada nederbo su duomenų bazių analize lengvai peržiūrėti duomenis, tokius kaip SMS žinutes sudėliotas chronologiškai pagal gavėją, naršomų internetinių puslapių istoriją su naršymo datomis, bei URL adresais.

Kadangi tai tik pirmą pabaigta įrankio versija, jo automatinė duomenų išgavimo procedūra ribota veikti su Samsung įrenginiais. Atsižvelgiant į tai jog Lietuvoje pirmąja Samsung gamybos įrenginiai, sukurtas įrankis gali būti vertingas teisminėms analizėms. Remiantis Statcounter statistika [14] (14 pav.), virš trečdalis Lietuvoje naudojamų įrenginių yra Samsung gamybos.

Mobile Vendor Market Share Lithuania  
May 2022 - May 2023



14 pav. Mobiliųjų įrenginių pasiskirstymas pagal gamintojus Lietuvoje

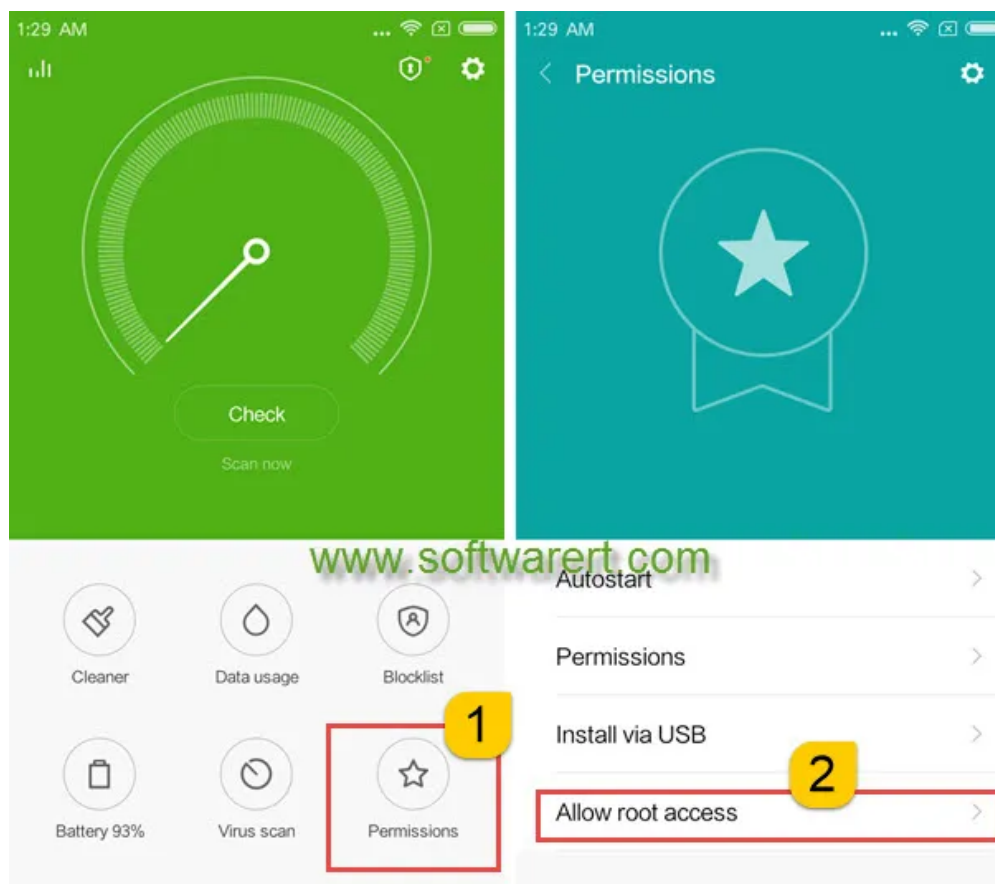
## Ateities tyrimų planas

Ateityje būtų vertinga tiksliau išanalizuoti įrenginius su „force-encrypt“ šifravimu įjungtu pagal gamintojo numatymus. Dauguma mobiliųjų įrenginių naudoja „fastboot“ paleidimo įkroviklį, kurį būtina atrakinti, kad būtų galimybė suteikti root teises arba įrašyti „TWRP“ atstatymo režimą. Be aukštesnių root teisių, duomenų particijos atvaizdo išgavimas nėra įmanomas.

Reikėtų taip pat atsižvelgti į SQL užklausas, nes kai kurios iš jų ar failo keliai yra betarpiškai parengti veikti su „Samsung“ mobiliais įrenginiais. Ši modifikacija nereikalauja daugelio pakeitimų kode, tad nebūtų sunku sukurti dar viena pasirinkimų meniu, duomenų bazių analizės skripte, kuriame galėtume nurodyti įrenginio gamintoją, ir atitinkamai pagal tai apdoroti failus atitinkamuose aplankuose bei su atitinkamomis užklausomis

Jeigu betarpiška analizė būtų teisėta, įranki būtų galima patobulinti papildomu funkcionalumu, kuris leistų apdoroti įrenginius be microSD kortelių skaitytuvo. Būtų galima sukurti skriptą kuris betarpiškai ištrauktų reikiamus analizei failus, praleidus atvaizdo kūrimą.

Galiausiai, būtų galima tyrinėti dar kelis atvejus, pavyzdžiui kitiškus įrenginius, nes jų saugumo lygis yra žymiai žemesnis nei kitų. Kai kurie „Xiaomi“ gamintojo įrenginiai, priklausomai nuo programinės įrangos versijos, buvo parduodami su galimybe įjungti „root“ teises betarpiškai „Kūrėjo parinkčių“ meniu, nereikalaudant jokių modifikacijų įrenginio particijose ar įkroviklyje. Šią parinktį matome šioje iliustracijoje (15 pav.):



15 pav. „Xiaomi“ įrenginių nustatymas leidžiantis įjungti root teises

Toks skriptas taip pat suveiktų su visais įrenginiais kuriems vietoj įrašinėti neoficialų atstatymo režimą, suteiksime „root“ teises sistemos lygyje.

## Literatūros šaltiniai

- [1] Hashim Shaikh. Practical android phone forensics. *Digital forensics*, 2017. <https://resources.infosecinstitute.com/topic/practical-android-phone-forensics/>.
- [2] Xiaodong Lin, Ting Chen, Tong Zhu, Kun Yang, and Fengguo Wei. Automated forensic analysis of mobile applications on android devices. *Digital Investigation*, 26:S59--S66, 2018. <https://www.sciencedirect.com/science/article/pii/S1742287618301889>.
- [3] Asif Iqbal; Hanan Al Obaidli; Andrew Marrington; Andy Jones. Windows surface rt tablet forensics. *Digital Investigation*, 11:S87--S93, 2014. <https://www.sciencedirect.com/science/article/pii/S1742287614000164>.
- [4] Hadeel Tariq Al-Rayes. Studying main differences between android & linux operating systems. *International Journal of Electrical & Computer Sciences IJECS-IJENS*, 12(05):46--49, 2012.
- [5] Darren Quick and Kim-Kwang Raymond Choo. Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, 11(4):273--294, 2014.
- [6] Emmanuel Lessieur, Olivier Martinot, Yanick Fratantonio, and Arnaud Francillon. Demystifying android bootloaders: Reversing and attacking the huawei bootloader. *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2017.
- [7] Android. A Brief History of Android, 2021. <https://www.android.com/history/> (Accessed on April 24, 2023).
- [8] Kingroot. Kingroot - One Click Root, 2022. <https://www.kingroot.net/>.
- [9] XDA Forum. A warning about kingroot for 24-12-2016, 2016.
- [10] KingRoot. Kingroot. Official website. <https://kingroot.net>.
- [11] TeamWin. Twrp. Official website. <https://twrp.me>.
- [12] Wikipedia. Windows subsystem for linux, 2023.
- [13] Benjamin Dobell. Heimdall, 2023.
- [14] Statcounter. Vendor Market Share - Mobile - Lithuania, 2023. <https://gs.statcounter.com/vendor-market-share/mobile/lithuania> (Accessed on June 6, 2023).