

# Diskų kopijų teisminės ekspertizės „Android“ įrenginiuose

IV semestro projektinis darbas

Vadovas:

Lekt. Virgilijus Krinickij

Atliko:

Matas Niewulis

# Tikslas

- Sukurti automatizuotą įrankį, kuris ištirtų „Android“ įrenginį ir palengvintų jo ekspertizės procesą.

# Uždaviniai

- Apžvelgti Android įrenginio architektūrą
- Sukurti veikiantį įrankio prototipą
- Ištestuoti įrankį su keliais „Android“ įrenginiais
- Išanalizuoti ir pateikti rezultatus

# „Android“ įrenginio architektūra

- Operacinė sistema „Android“ yra sukurta ant „Linux“ branduolio (angl. kernel), kuris teikia pagrindinį sistemos funkcionalumą, toki kaip procesų valdymas, atminties valdymas, įrenginio tvarkyklės (angl. device driver) ir sauga.
- Android įrenginiai naudoja grafinę vartotojo sąsają (GUI). Vartotojo sąsaja gali būti pritaikoma ir gali skirtis priklausomai nuo skirtingų įrenginių gamintojų.
- Įrenginiai gali veikti su įvairiais sistemos variantais (pvz. „Samsung OneUI“, „Xiaomi MIUI“) kurie savo veikimu, funkcionalumu ar saugumu žymiai skiriasi nuo bazinio AOSP „Android Open Source Project“.
- „Android“ įrenginiai palaiko skirtingus paleidimo režimus, įskaitant:
  - Įprastinis režimas (Normal boot)
  - Atstatymo režimas (Recovery mode)
  - Įrašymo režimas (Flashing mode)

# Tipinis „Android“ įrenginio disko skaidymas

Tiriamas „Samsung Galaxy S3 Neo“ įrenginio disko skaidymas:

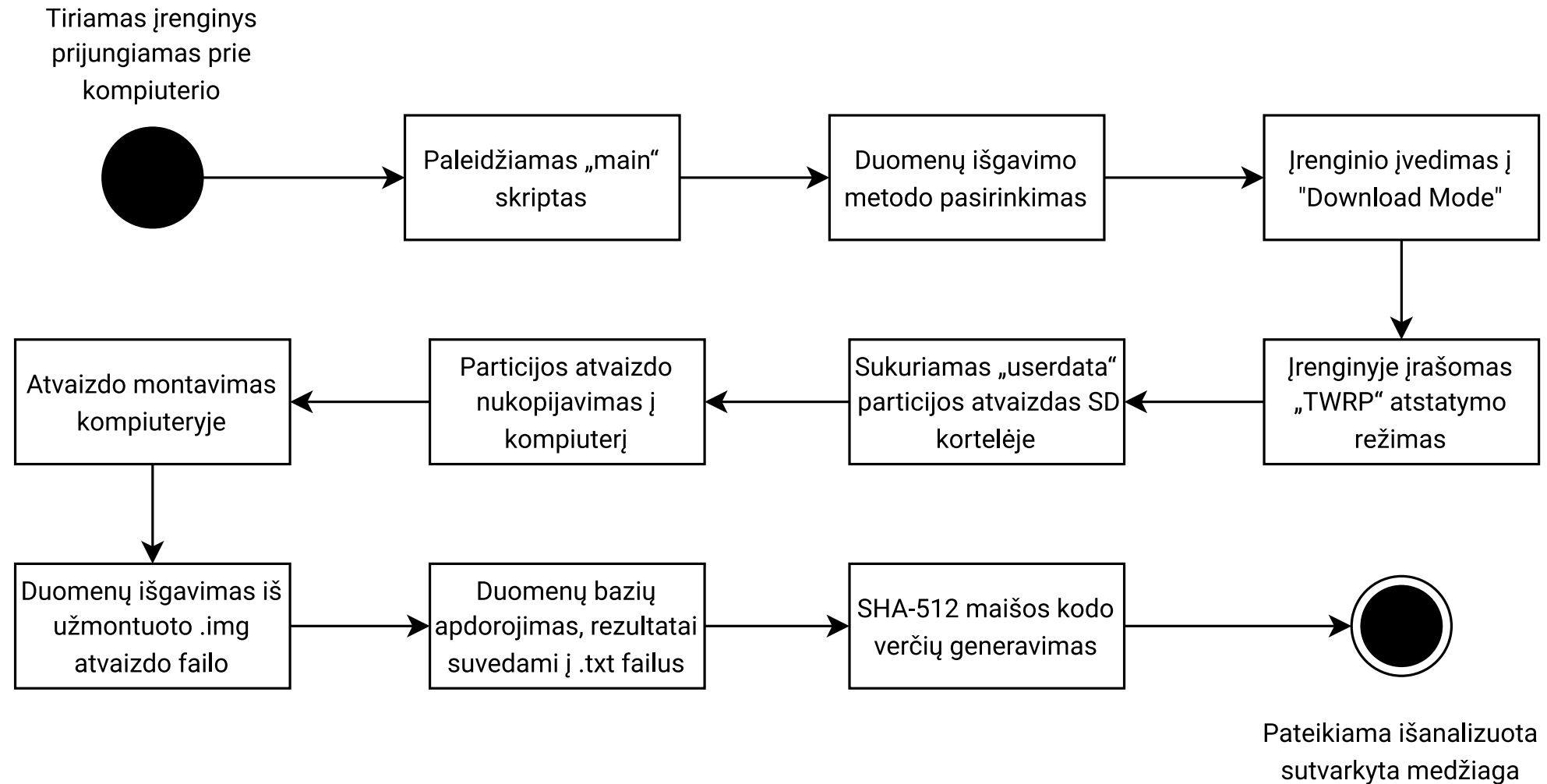
Number	Start (sector)	End (sector)	Size	Code	Name
1	8192	36863	14.0M	0700	apnhlos
2	36864	138751	49.7M	0700	modem
3	138752	139775	512K	0700	sbl1
4	139776	139839	32768	0700	dbi
5	139840	139903	32768	0700	ddr
6	139904	143999	2048K	0700	aboot
7	144000	145023	512K	0700	rpm
8	145024	146047	512K	0700	tz
9	146048	148095	1024K	0700	pad
10	148096	168575	10.0M	0700	param
11	168576	197247	14.0M	0700	efs
12	197248	203391	3072K	0700	modemst1
13	203392	209535	3072K	0700	modemst2
14	209536	230015	10.0M	0700	boot
15	230016	250495	10.0M	0700	recovery
16	250496	270975	10.0M	0700	fota
17	270976	285293	7159K	0700	backup
18	285294	291437	3072K	0700	fsg
19	291438	291439	1024	0700	fsc
20	291440	291455	8192	0700	ssd
21	291456	307839	8192K	0700	persist
22	307840	326271	9216K	0700	persdata
23	326272	4422271	2000M	0700	system
24	4422272	5831295	688M	0700	cache
25	5831296	6240895	200M	0700	hidden
26	6240896	30777310	11.6G	0700	userdata

- Susijungus su įrenginiu per ADB komunikaciją, ir surinkus komandą „fdisk /dev/block/mmcblk0“, gauname particijų skaidymo lentelę, kartu su jų dydžiu, pradiniais ir baigtiniais sektoriais, kodu bei pavadinimu.
- Įrenginio teisminei ekspertizei reikalingas skaidinys vardu „userdata“. Jame sukaupti visi vartotojo failai, programėlių duomenys bei duomenų bazės.
- „Android“ įrenginiuose įprastai naudojama „EXT4“ failų sistema.

# Komunikacija su „Android“ įrenginiu

- Norint pasiekti duomenis, galima naudoti paprastą USB sujungimą.
- „Android“ įrenginiai įprastai naudoja MTP režimą prijungiant juos prie kompiuterio.
- Norint analizuoti įrenginį plačiau, galime naudoti „ADB“ (Android Debug Bridge) režimą, kuris leidžia išsamiau valdyti įrenginį.
- Norint įrašyti particijos atvaizdą, galime naudoti „fastboot“ ar „Download mode“ režimą. Šiam tyrimui naudotas „Download mode“ režimas „Samsung“ įrenginyje.

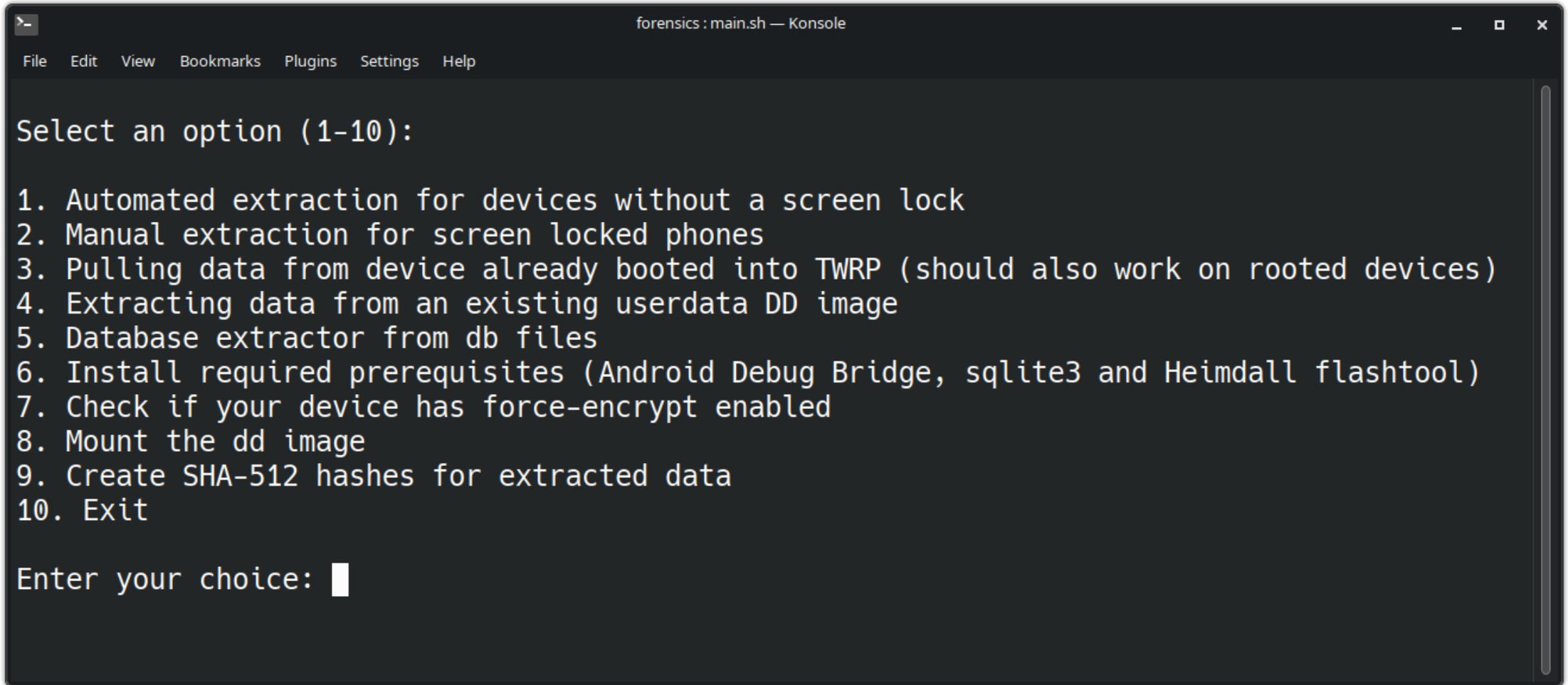
# Sukurto įrankio veikimo modelis



# Techniniai reikalavimai ir savybės

- Kompiuteris (rekomenduojama su „Linux“ operacinės sistemos distribucija)
- Tinkantis „Android“ įrenginys (be priverstinio šifravimo (angl. Force encrypt))
- USB laidas
- MicroSD atminties kortelė, sumontuota tiriamame įrenginyje (kortelės talpa turi būti didesne už įrenginio vidinės atminties talpą)
- Įrankis sukurtas „Shell script“/„Bash script“ kalba.
- Numatomai įrankis sukurtas „Linux“ operacinėms sistemoms, bet yra galimybė naudoti taip pat ir „Windows“ operacinėse sistemose (su WSL „Windows Subsystem for Linux“ komponentu).
- Pirmą kartą paleidžiant įrankį, būtina įdiegti reikalingus komponentus:
  - android-sdk-platform-tools (naudojamas adb komunikacijai)
  - heimdall-flash (naudojamas įrenginio įrašymui (angl. Flashing))
  - sqlite3 (naudojamas duomenų bazių apdorojimui)

# Jrankio pagrindinis menu



```
forensics : main.sh — Konsole
File Edit View Bookmarks Plugins Settings Help

Select an option (1-10):

1. Automated extraction for devices without a screen lock
2. Manual extraction for screen locked phones
3. Pulling data from device already booted into TWRP (should also work on rooted devices)
4. Extracting data from an existing userdata DD image
5. Database extractor from db files
6. Install required prerequisites (Android Debug Bridge, sqlite3 and Heimdall flashtool)
7. Check if your device has force-encrypt enabled
8. Mount the dd image
9. Create SHA-512 hashes for extracted data
10. Exit

Enter your choice: █
```



# Įrankio privalumai, apribojimai bei savybės

- Kiekvienas skirtingo gamintojo įrenginys skiriasi keliais aspektais. Pagrindinė problema yra „root“ teisių suteikimas. „Root“ teisės „Android“ įrenginyje, veikia panašiai kaip administratoriaus teisės „Windows“ operacinėse sistemose. Suteikiamas aukščiausias leidimų lygis.
- „Root“ teisių suteikimas yra būtinas norint naudotis išsamiomis „ADB shell“ komandomis. Šiuo atveju naudojamas „dd“ įrankis (disk/data duplicator) reikalauja „root“ teisių norint pasiekti atmintį ir sudaryti jos disko atvaizdą.
- „Kingroot“ programėlė, kuri buvo ilgai naudojama norint suteikti „root“ teises vienu paspaudimu jau neveikia. „Root“ teisių suteikimas tapo sunkesnis ir reikėjo ieškoti naujų sprendimų, kas sumotyvavo mane sukurti savo įrankį.
- Sukurtas įrankis nereikalauja „root“ teisių įprastiniame režime. Vietoj to paleidžia įrenginį atstatymo režime, kuris iškart veikia su aukščiausiomis teisėmis. Naudojamas atstatymo režimo variantas tai „TWRP“ (Team Win Recovery Project) kuris yra atviro kodo.
- Įrankis veikia su nešifruotais „Android“ įrenginiais, turinčiais microSD kortelių skaitytuvą.
- Įrankis neveikia su šifruotais įrenginiais, kurių paleidimo įkroviklis yra užrakintas.

Tiriama sritis	.db failas	Lentelė	Laukai
SMS žinutės	mmssms.db	sms	date, (siuntimo data) address, (gavėjas) body, (žinutės tekstas) Type (žiutes tipas)
Kontaktai	contacts2.db	raw_contacts	display_name, (kontakto pavadinimas) data1 (įrašo duomenys)
Skambučių istorija	logs.db	logs	date, (skambučio data) duration, (skambučio trukmė) number, (skambinamas numeris) name, (kontakto pavadinimas) Type (skambučio tipas)
Kalendorius	calendar.db	events	title, (įvykio pavadinimas) description, (įvykio aprašymas) dtstart, (įvykio pradžia) Dtend (įvykio pabaiga)
Naršyklės istorija	history.db	urls	title, (tinklalapio pavadinimas) url, (tinklalapio URL adresas) last_visit_time (vizito data)
Naršyklės slaptažodžiai	login_data.db	logins	origin_url, (prisijungimo URL adresas) username_value, (prisijungimo vardas) password_value (prisijungimo slaptažodis)
Slapukai	cookies.db	cookies	host_key, (slapuko raktas) name, (slapuko pavadinimas) value, (slapuko duomenys) encrypted_value, (šifruoti duomenys) creation_utc, (slapuko sudarymo data) expires_utc (slapuko svarbos data)

# Praktinio panaudojimo rezultatai

- Įrankis buvo pagrindinai testuojamas su „Samsung Galaxy S3 NEO“ ir „Samsung Galaxy S5“ įrenginiais. Abu įrenginiai buvo sėkmingai išanalizuoti. Iš šių įrenginių pavyko išgauti:
  - SMS/MMS duomenis
  - Kontaktų duomenis
  - Skambučių registro duomenis
  - Kalendoriaus įvykių duomenis
  - Naršyklės duomenis
  - Nuotraukas bei kitus failus iš pagrindinės atminties
- Įrankio testavimas su „Oneplus 2“ bei „Google Nexus 5“ įrenginiais buvo nesėkmingas. Šių įrenginių paleidimo įkroviklis (angl. bootloader) numatomai užrakintas. Paleidimo įkroviklį būtina atrakinti norint įrašyti atstatymo režimo atvaizdą. Jo atrakinimas, dėl saugumo priežasčių sunaikina visus įrenginiuose kaupiamus duomenis.
- Įrankio testavimas su „Samsung Galaxy S20 FE 5G“ buvo nesėkmingas, nes įrenginys yra šifruotas su „force-encrypt“ funkcija.

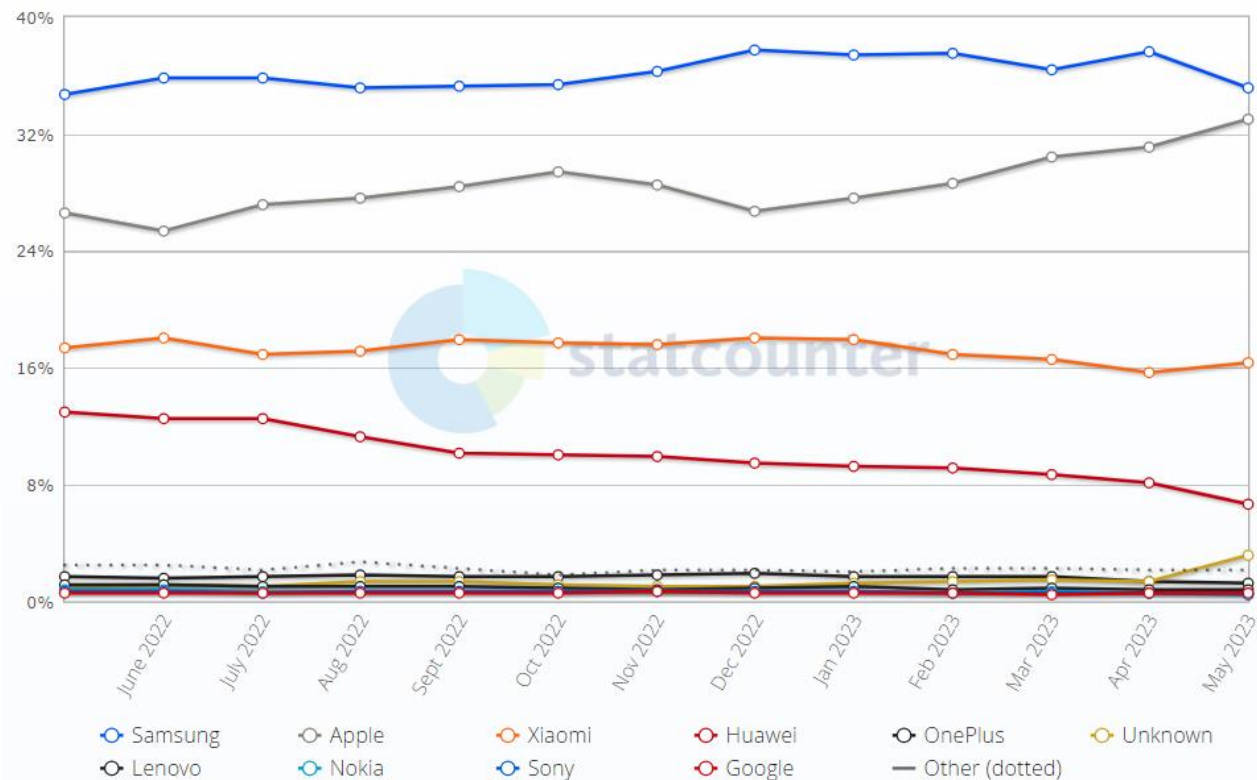
# Išvados (1)

- Kuriant įrankį paaiškėjo kad sukurti universalų įrankį, kuris veiktų su visais įrenginiais, itin sunku.
- Kadangi tai tik pirma pabaigta įrankio versija, jo **automatinė** duomenų išgavimo procedūra ribota veikti su „Samsung“ įrenginiais.
- Įrankis gali ištraukti ir apdoroti SMS, kontaktų, skambučių, kalendoriaus bei naršyklės duomenų bazes. Išgauna taip pat nuotraukas ir kitus asmeninius failus, kas yra esminė informacija teisminėms ekspertizėms
- Sukurtas įrankis, turi daug funkcionalumų. Gali išgauti duomenis iš nešifruotų mobiliųjų įrenginių. Yra tinkamas įrenginiams su ekrano užraktu bei be ekrano užrakto. Įrankis turi daug informacinių dialogų, kurie leidžia vartotojui lengvai suprasti kas vyksta ir kokius žingsnius reikia įvykdyti, kad duomenų išgavimas vyktų sklandžiai ir paprastai.

# Išvados (2)

- Remiantis „Statcounter“ statistika, apie 77% Lietuvoje naudojamų įrenginių veikia su „Android“ operacine sistema. „Samsung“ gamybos įrenginiai sudaro apie 50% naudojamų Lietuvoje „Android“ įrenginių. Atsižvelgiant į tai jog „Samsung“ gamybos įrenginiai pirmauja, sukurtas įrankis gali būti vertingas teisminėms analizėms.

Mobile Vendor Market Share Lithuania  
May 2022 - May 2023



Statcounter. Vendor Market Share - Mobile - Lithuania, 2023. <https://gs.statcounter.com/vendor-market-share/mobile/lithuania> (Accessed on June 6, 2023)

# Praktinė demonstracija

<https://www.youtube.com/watch?v=BpO70yDgHno>

# Ačiū už dėmesį.

Diskų kopijų teisminės ekspertizės Android įrenginiuose

Vadovas:

Lekt. Virgilijus Krinickij

Atliko:

Matas Niewulis