

KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

NUSIKALTIMAI ELEKTRONINĖJE ERDVĖJE IR JŲ TYRIMŲ METODIKOS

T120M152

Laboratorinio darbo Nr. 2 ataskaita

INFORMACIJOS IŠTYRIMAS MOBILIUOSE ĮRENGINIUOSE

Atliko: IFM-1/3 gr.

Stud. Eligijus Kiudys

Patikrino:

Kaunas, 2022

---

..... gr. Stud.....

## Laboratorinis darbas Nr. 2.

### Įkalčių mobiliam įrenginyje ištyrimas ir bylos sudarymas

#### Darbo priemonės

1. Du mobiliųjų telefonų su Android OS atvaizdai - įkalčiai;
2. AutoPSY (<http://www.sleuthkit.org/autopsy/>)
3. FTP prieiga (įkalčių Android atvaizdai – NEE kataloge, ANDROID) <ftp://IP>  
Prisijungimo vardas: anonymous; Naudoti KTU VPN (Klases) prisijungimą atliekant darbą namuose;
4. Galima naudoti ir šiame sąraše nepateiktą programinę įrangą.

#### Darbo scenarijus:

Kompiuterio vartotojas Almantas Karvelis, buvo nužudytas, dėl galimo bendradarbiavimo su Valstybinėmis institucijomis arba, dėl kibernetinių išpuolių prieš "KTU TELEKOM" organizaciją. Policijos skyrius aptiko du mobiliuosius įrenginius ir pateikė informacijos apdorojimui dvi kopijas (telefoninius atvaizdus), uždavė klausimus į kuriuos prašo atsakymų ir paaiškinimų.

#### Darbo tikslas

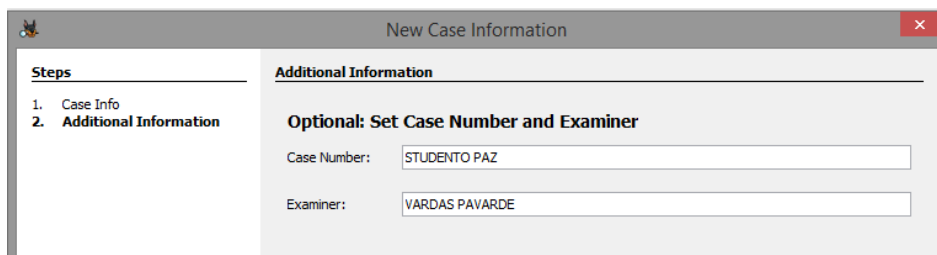
Atlikti mobiliųjų telefonų atvaizdų kopijų analizę ir atsakyti į tyrėjų pateiktus klausimus. Parengti tyrimo ataskaitą naudojantis AutoPSY programinę įrangą.

#### Darbo uždaviniai

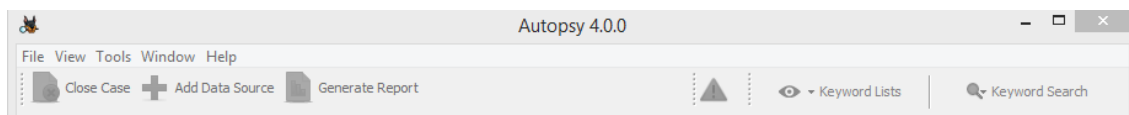
1. Naudojant AutoPSY surinkti informaciją iš mobiliųjų įrenginių atvaizdų.
2. Pateikti darbo rezultatų išvadas suformuojant ataskaitą.

#### Darbo planas

1. Naudojant AutoPSY susikurti savo tyrimo ataskaitos bylą. Bylos numeris: STUDENTO PAŽYMĖJIMO NR. Atlikėjas: VARDAS PAVARDE



2. Į programą importuoti (įrenginių eiliškumo tvarka) gautą informaciją iš policijos skyriaus.
3. Pridėti (**Attach to..**) tik tuos įkalčius kurie siejasi su pareigūnų pateiktais **UŽDUOTIES** klausimais.
4. Suformuoti ataskaitą (**Generate Report -> HTML**), suarchyvuoti (Pavarde.zip)



5. Įkelti ataskaitą į *MOODLE* aplinką.

## UŽDUOTYS

### Pirmas įrenginys (HTC)

1. Kiek ir kur telefone radote kontaktų?
2. Kokio stiliaus muzika patinka šio įrenginio naudotojui. Išvardinkite bent 2 atlikėjus. Nurodykite iš kur konkrečiai gauna informacija.
3. Kiek viso siųstą ir gautą trumpųjų (SMS) žinučių?
4. Ar šiame telefone naudojama Skype programinė įranga. Jei taip, tai koks yra Skype vartotojo prisijungimo adresas? Kur ir kaip radote šia informaciją?
5. Įvardinkite du Zynga kūrėjų kompanijos žaidimo WordsWithFriends, aponentus. Kur čia informaciją radote?
6. Ar galite nustatyti iš kokio galimai miesto yra šio įrenginio naudotojas? Jei taip, paaiškinti, kaip nustatėt (padarėt prielaidą).

### Antras įrenginys (sony)

1. Kiek ir kur telefone radote kontaktų?
2. Kiek viso atlikta telefoninių skambučių? Kiek iš jų yra įeinantys?
3. Kiek viso siųstą ir gautą trumpųjų (SMS) žinučių?
4. Ar galite nustatyti iš kokio galimai miesto yra šio įrenginio naudotojas? Jei taip, paaiškinti, kaip nustatėt (padarėt prielaidą).
5. Kokią programinę įrangą susirašinėjimui pasirinko šio įrenginio naudotojas?
6. Kokio operatoriaus paslaugomis naudojasi mobiliojo įrenginio naudotojas?
7. Telefono naudotojas buvo kaltinamas ginklo vagyste. Ar radote kažkokių įrodymų šiam faktui patvirtinti?

## IŠVADA

### Pirmas įrenginys

1. Buvo rasti 116 Kontaktai. Buvo rasta elektroninio pašto 11 kontaktų Jie buvo rasti tap žaidimų duomenų.

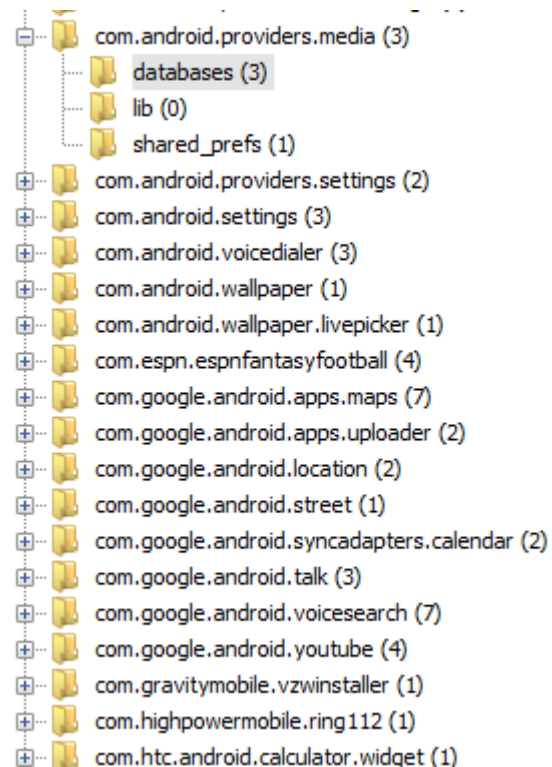
/LogicalFileSet1/HTC/com.zynga.words/databases/WordsFramework

/LogicalFileSet1/HTC/com.android.providers.calendar/databases/calendar.db

/LogicalFileSet1/HTC/com.android.providers.downloads/databases/downloads.db

/LogicalFileSet1/HTC/com.google.android.apps.maps/files/DATA\_Preferences

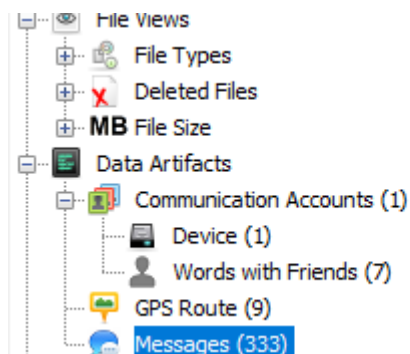
2.



A screenshot of a database viewer showing the 'audio\_genres' table with 6 entries. The table has two columns: '\_id' and 'name'.

_id	name
1	\uefc0
2	Electronica
3	Electronic
4	Electronica/Dance
5	electronica
6	Hip Hop/Rap

3. Buvo surasta 333 žinučių.



4. Buvo surasti ištrinti skype failai, juose galima matyti telefono numerį, savininko vardą – lee.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<boolean name="-32" value="true" />
<string name="3">U0uSU1TI2VjchJWS5J64LjFyWK/P4lbyysgrDJEbIbIOqx4Ug/RovrswrjWGCOarr4XAgdtWQYLTf/Xkg8t
GgukYvkmmbkNlIO5OjsiDEz/BIJ1QJTMg==</string>
<string name="2">213.146.167.34:10509</string>
<string name="1">+17174212953</string>
<int name="10" value="0" />
<string name="0">lee</string>
<string name="7">AIB0EwAAoQI=</string>
<boolean name="-2" value="true" />
<string name="-28"></string>
<boolean name="-27" value="true" />
<boolean name="-26" value="true" />
<boolean name="-3" value="false" />
<string name="4">ALxUJQF0c/YnN3ealZEW0HxBsVQuyO6d5Y31gXFOSdAF9w3wLkMbJy0v5KuCRyHOQ==</string>
<int name="-26_2" value="1" />
</map>
```

5. 2 70268016 zyngawf\_24685519 zyngawf\_24685519 2012-01-24T23:52:31Z 20

Visi rasti žaidėjai kurie žaidė su sukurtu žaidėju

Table games 81 entries Page 1 of 1 Export to CSV							
pk	game_id	opponen...	△ creat...	created_at	updated_at	display_s...	opponent_name
2	1484147528	66258871	70268016	2012-01-24T23:53:48Z	2012-01-28T20:09:33Z	9	Hmahalik11
12	1552714680	66258871	70268016	2012-02-01T19:41:24Z	2012-02-01T19:44:04Z	9	Hmahalik11
19	1588788397	70999702	70268016	2012-02-05T22:18:02Z	2012-02-06T03:01:29Z	9	VictoriaCrognale
21	1591662646	4	70268016	2012-02-06T03:01:10Z	2012-02-08T23:06:53Z	9	Player 2
23	1615551491	70999702	70268016	2012-02-08T23:07:30Z	2012-02-12T03:09:51Z	9	VictoriaCrognale
28	1661851148	70999702	70268016	2012-02-14T01:26:47Z	2012-02-24T03:28:53Z	9	VictoriaCrognale
34	1744274908	66258871	70268016	2012-02-23T02:44:53Z	2012-02-25T18:27:19Z	9	Hmahalik11
50	2042831167	82943694	70268016	2012-03-28T23:34:31Z	2012-04-02T10:31:32Z	9	donnietindall9876
51	2042817899	4784222	70268016	2012-03-28T23:33:00Z	2012-03-28T23:36:54Z	9	Dtindall
55	2128659478	227170	70268016	2012-04-07T14:01:14Z	2012-04-18T00:08:07Z	4	Kachup57

6. Vašingtonas, Arlington. Taip pat žiūrint pagal žemėlapiu kordinates galima matyti, kad ten dažniausiai žmogus lankėsi.

Lee you live down in VA right?

Headers

Text

HTML

RTF

Attachments (0)

Accounts

Yep, Arlington

Headers

Text

HTML

RTF

Attachments (0)

Accounts

to live? Arlington is a good area. very dc accessible.

Headers

Text

HTML

RTF

Attachments (0)

Accounts

Ok. Eventually making my way down there but need to be somewhat close to DC

Antras įrenginys (Sony)

..... gr. Stud.....

5

1. Buvo rasti 54 kontaktai su telefono numeriais, 13 elektroninių paštų, 11 whatsapp adresų.

/LogicalFileSet1/Sony (SonyEricsson)\_Xperia X10

mini/Dump/data/data/com.android.providers.contacts/databases/contacts2.db

/LogicalFileSet1/Sony (SonyEricsson)\_Xperia X10

mini/Dump/data/data/com.android.providers.telephony/databases/mmssms.db

/LogicalFileSet1/Sony (SonyEricsson)\_Xperia X10

mini/Dump/data/data/com.whatsapp/databases/wa.db

/LogicalFileSet1/Sony (SonyEricsson)\_Xperia X10

mini/Dump/data/data/com.viber.voip/databases/viber\_data

2. Atlikta 130 skambučių, iš jų 5 yra įeinantys.
3. Gauta 16 SMS, išsiųsta – 19.
4. Žiūrint GPS koordinates, aktyviausias ir daugiausiai pasikartojančios koordinatės yra Orlando miestas, JAV, Floridos valstija
5. Naudojo WhatsApp, Viber bei SMS žinučių siuntimo programinę įrangą.
6. T-Mobile
7. Įrenginio savininkas du kartus lankėsi prie ginklų parduotuvės, esančios adresu 7253 Centreville Rd, Manassas, VA 20111 po jos darbo valandų. Taip pat interneto naršyklės DB rasta išsaugotų žymų „gunbroker“, „Guns for sale“. Papildomai rasta netikrų žinučių siuntimo PĮ, netikrų darbo skelbimų kūrimo PĮ, taigi manoma, kad naudotojas užsiiminėjo neteisėta veikla.