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

# 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

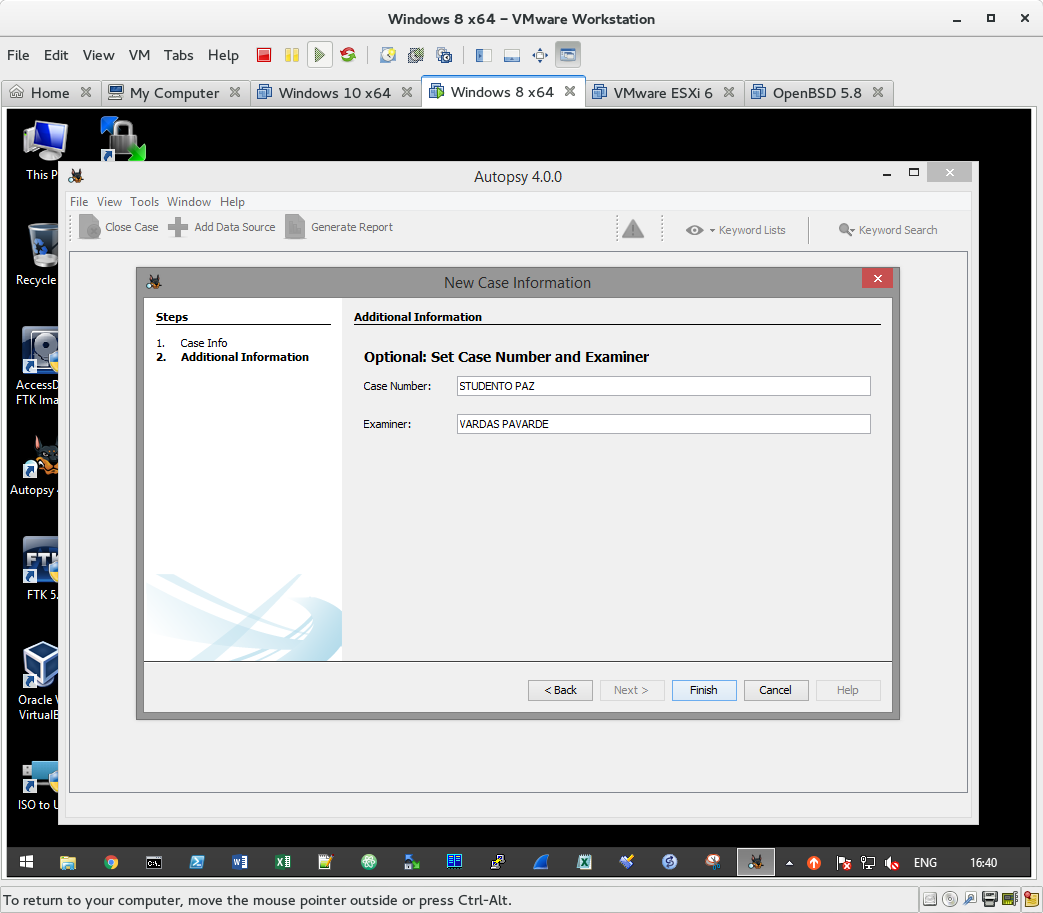
Atlikti mobiliųjų telefonų atvaizdų kopijų analizę ir atsakyti į tyrėjų pateiktus klausimus. Parengti tyrimo ataskaitą naudojantis AutoPSY programinę įrangą.

## Darbo uždaviniai

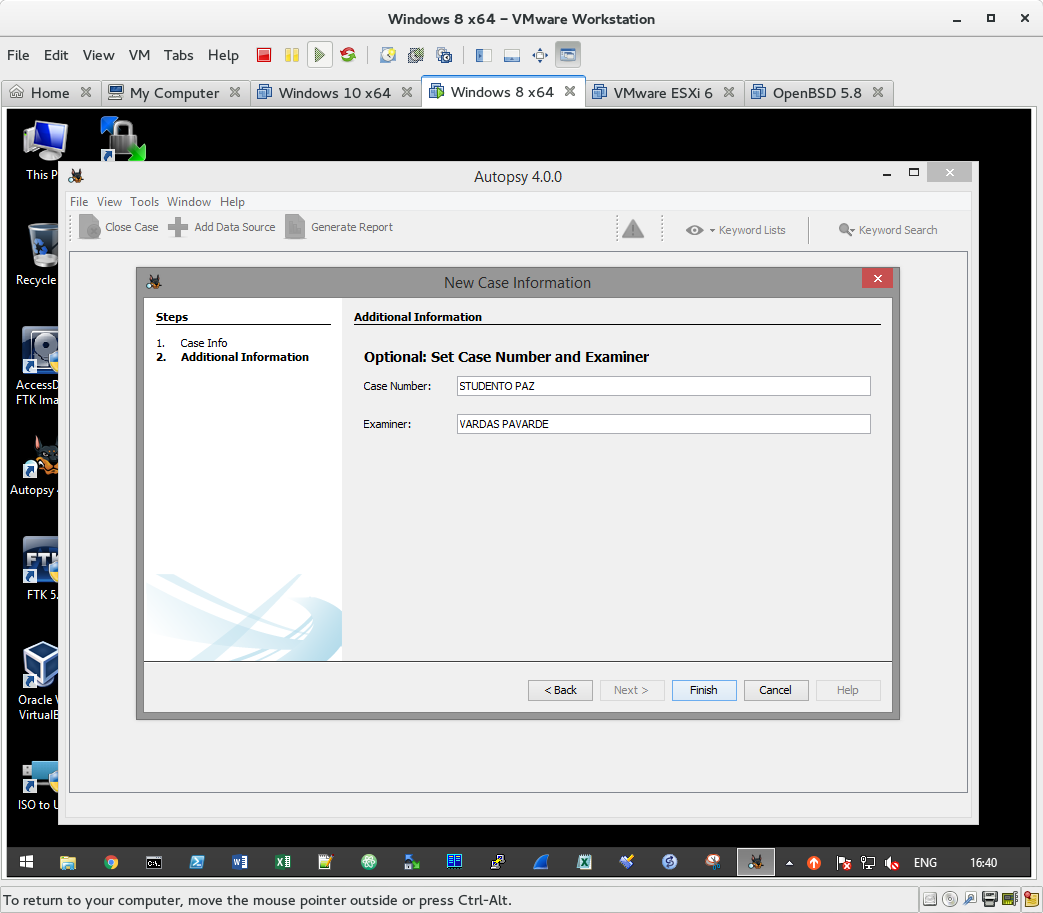
1. Naudojant AutoPSY surinkti informaciją iš mobiliųjų įrenginių atvaizdų.
2. Pateikti darbo rezultatų išvadas suformuojant ataskaitą.

## Darbo planas

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



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



1. 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

Graphical user interface, table

Description automatically generated

1. Buvo surasta 333 žinučių.

Graphical user interface, text, application, chat or text message

Description automatically generated

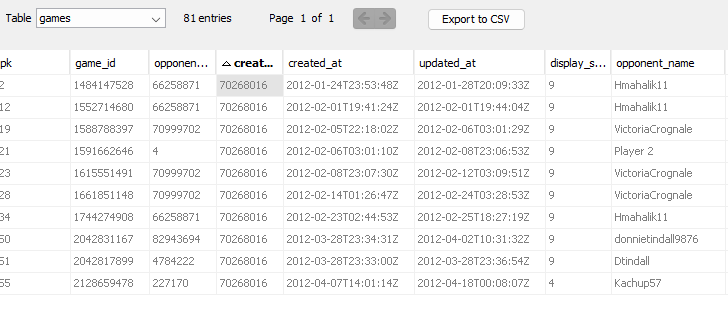
1. Buvo surasti ištrinti skype failai, juose galima matyti telefono numerį, savininko vardą – lee.

Text, letter

Description automatically generated

1. 

Visi rasti žaidėjai kurie žaidė su sukurtu žaidėju



1. Wašingtonas, Arlington. Taip pat žiūrint pagal žemėlapio kordinates galima matyti, kad ten dažniausiai žmogus lankėsi.

Graphical user interface, text, application

Description automatically generated

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

**Antras įrenginys (Sony)**

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

1. Atlikta 130 skambučių, iš jų 5 yra įeinantys.
2. Gauta 16 SMS, išsiųsta – 19.
3. Žiūrint GPS kordinates, aktyviausias ir daugiausiai pasikartojančios kordinatės yra Orlando miestas, JAV, Floridos valstija
4. Naudojo WhatsApp, Viber bei SMS žinučių siuntimo programinę įrangą.
5. T-Mobile
6. 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.