KAUNO TECHNOLOGIJOS UNIVERSITETAS

KOMPIUTERIŲ KATEDRA

Virtualios infrastruktūros sauga

T120M144

Laboratorinio darbo Nr. 4 ataskaita

Hypervizoriaus disko failų analizė

Atliko: IFM-1/3 gr.

Stud. Eligijus Kiudys

Patikrino:

Kaunas, 2022

# Laboratorinis darbas Nr. 4.

**Hypervizoriais sukurtų virtualių diskuose esančių failų analizė**

## Darbo tikslas

Naudojant (iš praeitų laboratorinių darbų) WMware ESXi arba Hyper-V technologija sukurtomis virtualių mašinų diskais, parengti ataskaitą naudojant AutoPSY (<http://www.sleuthkit.org/autopsy/)> įrankį.

## Darbo priemonės

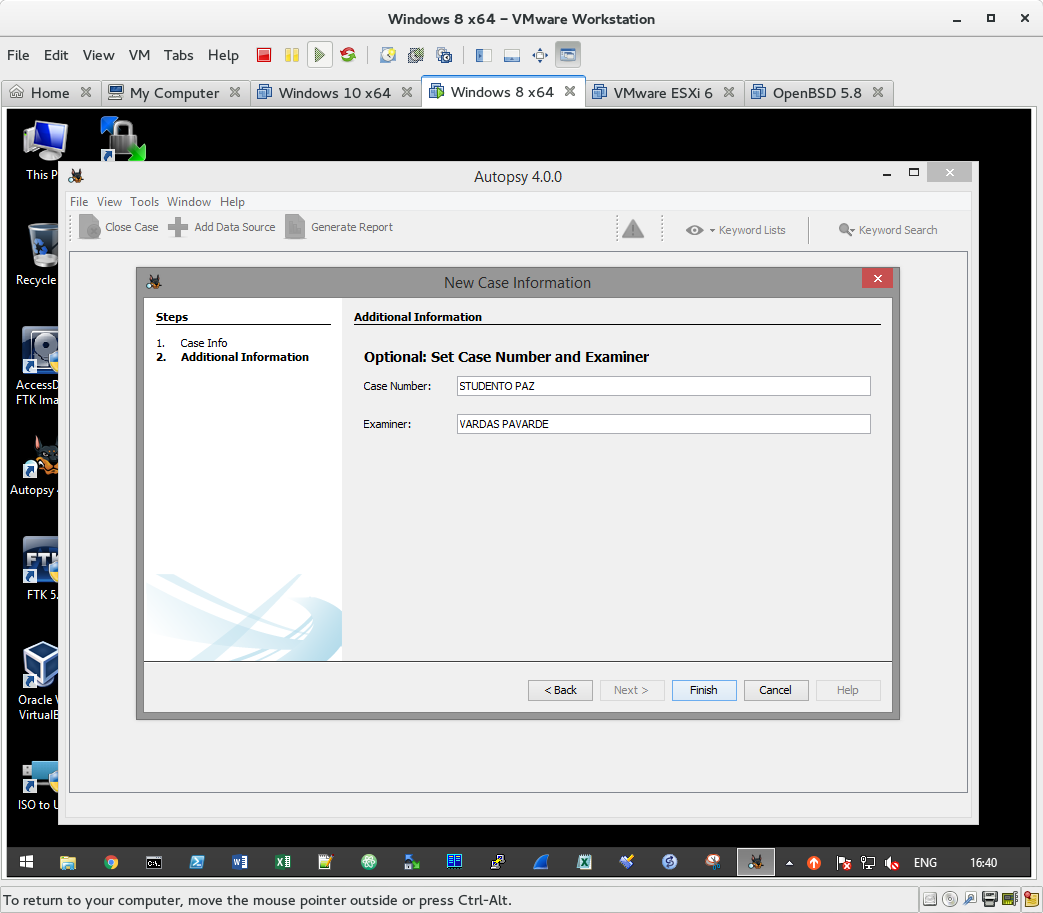
1. Diskų atvaizdų diskai
2. AutoPSY (<http://www.sleuthkit.org/autopsy/)>
3. Qemu-img (virtualių diskų formatų keitimo programinė įranga)
4. Putty (ssh prisijungimui), WinSCP (failų parsisiuntimui naudojant ssh protokolą).
5. FTP prieiga. Prisijungimo vardas: anonymous

## Darbo uždaviniai

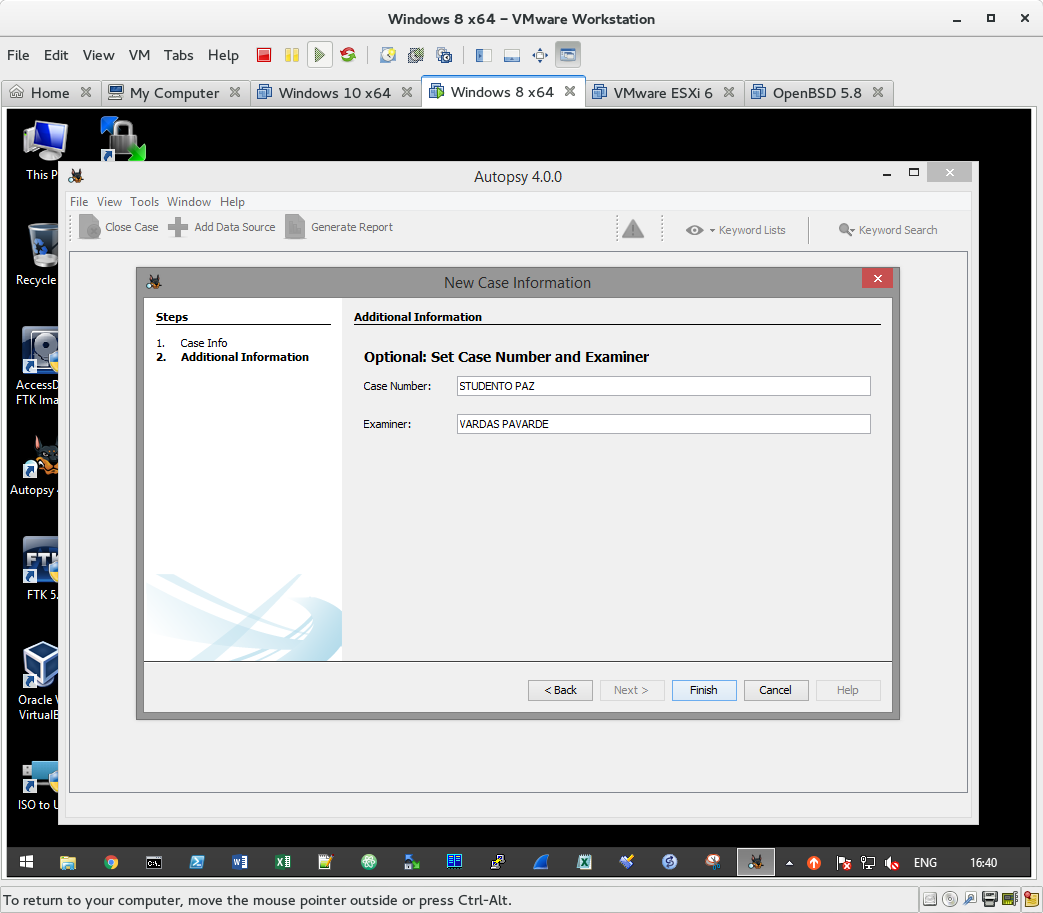
1. Naudojant AutoPSY surinkti informaciją iš hypervizoriaus suformuotų virtualių diskų.
2. Pateikti darbo rezultatų išvadas suformuojant ataskaitą.

## Darbo planas

1. Naudojant AutoPSY susikurti savo bylą (pav. Nr. 1). Bylos numeris: STUDENTO PAŽYMĖJIMO NR. Atlikėjas: VARDAS PAVARDĖ
2. Gauti \*.vmdk, \*.vhd disko atvaizdus
3. Virtualius hypervizoriaus diskus pakeisti į RAW formatą (jei tokio formato nesupranta AutoPSY).
4. Suformuoti ataskaitą (pav. Nr. 2) (***Generate Report -> HTML***), suarchyvuoti (Pavarde.zip)
5. Įkelti ataskaitą į *MOODLE* aplinką



1 Pav. Bylos formavimo reikalavimai



2 Pav. Ataskaita