Slovenská technická univerzita v Bratislave

Fakulta informatiky a informačných technológií

Počítačové a komunikačné siete

**Zadanie č.2**

**Analyzátor sieťovej komunikácie**

Akademický rok 2022/2023

**Meno:** Ján Ágh **Dátum:** 19.10.2022

**Cvičiaci:** Ing. Lukáš Mastiľak **Počet strán:** 9

**Obsah**

[**1 Stručný opis problematiky a zadania** 1](#_Toc119789487)

[**2 Navrhnuté riešenie** 2](#_Toc119789488)

[**2.1 Použité programové prostriedky** 2](#_Toc119789489)

[**2.2 Organizácia projektu** 2](#_Toc119789490)

# **1 Stručný opis problematiky a zadania**

Cieľom zadania bolo navrhnúť analyzátor sieťovej komunikácie, ktorý mal byť schopný spracovať obsah súborov typu *.pcap* a zistiť požadované informácie o rámcoch obsiahnutých v nich. Program podporuje spracovanie, analýzu a výpis všetkých rámcov zaznamenaných vo vstupnom súbore, analýzu vybraných protokolov s komunikáciou so spojením (spadajúcich pod TCP), konkrétne *HTTP, HTTPS, TELNET, SSH, FTP-DATA a FTP-CONTROL*, a taktiež spracovanie komunikácie pre protokol ARP a zhodnotenie, či sa jedná o kompletnú komunikáciu alebo nie.

# **2 Navrhnuté riešenie**

## **2.1 Použité programové prostriedky**

Na riešenie úlohy bol použitý programovací jazyk Python verzie 3.10.8. Riešenie bolo vyvíjané v prostredí Visual Studio Code verzie 1.72.1 a pri jeho vývoji boli využité základné objektovo orientované princípy.

## **2.2 Organizácia projektu**

Implementácia sa nachádza v adresári s názvom “*network\_traffic\_analyzer*”. Spolu ju tvorí 9 súborov typu *.py*, adresár *Protocols* obsahujúci *.txt* súbory s dvojicami číslo protokolu v hexadecimálnom tvare – názov protokolu, adresár *pcaps*, ktorý obsahuje vstupné *.pcap* súbory na spracovanie, a po vykonaní analýzy aj adresár *yamls* naplnený výstupnými súbormi formátu *.yaml.*

Súbor *main.py* je hlavným vstupom do programu a obsahuje jedinú inštanciu triedy *UserInterface*, pomocou ktorej používateľ dokáže zadať všetky potrebné informácie na úspešné vykonanie analýzy vstupného súboru.

Súbor *user\_interface.py* obsahuje základné metódy na prvotnú analýzu rámca a taktiež rozhodovanie, aké ďalšie spracovanie má nasledovať, pričom toto rozhodovanie sa riadi vstupom používateľa.

Najdôležitejšou súčasťou programu je súbor *frame\_analyzer.py*, ktorý slúži na podrobnú analýzu a extrakciu všetkých dôležitých informácií z daného rámca, ako napríklad zdrojová a cieľová MAC adresa, použitý komunikačný protokol a mnoho ďalších.

V súbore *comm\_analyzer.py* sa nachádzajú metódy umožňujúce analýzu a filtrovanie rámcov podľa protokolov ARP alebo TCP.

Zvyšné súbory zohrávajú iba doplnkovú úlohu (*constanty.py* obsahuje konštanty, *converters.py* metódy na úpravu tvaru MAC adries, IP adries a výpisu rámca, *dict\_loader.py* slúži na uchovávanie načítaných protokolov zo súborov v adresári *Protocols*, *yaml\_creator.py* umožňuje výpis analyzovaných údajov do súboru formátu *.yaml* a *senders.py* uchováva štatistiku rámcov typu IPv4 pri rozšírenej analýze).

Text

Description automatically generated with medium confidence

*Obr. 2.1 Adresárová štruktúra implementácie*