Slovenská technická univerzita v Bratislave

**Fakulta informatiky a informačných technológií**

Počítačové a komunikačné siete

**Analyzátor sieťovej komunikácie**Tibor Dulovec

**Meno cvičiaceho:** Ing. Miroslav Bahleda, PhD.

**Čas cvičení:** Štvrtok 18:00

**Dátum vytvorenia**: 19. 10. 2021

Obsah

[Zadanie úlohy 3](#_Toc85726526)

[Implementačné prostredie 3](#_Toc85726527)

[Externé súbory 3](#_Toc85726528)

[db.txt 3](#_Toc85726529)

[Icmp.txt 4](#_Toc85726530)

[Fungovanie programu 5](#_Toc85726531)

[Používateľské rozhranie 5](#_Toc85726532)

[Načítanie a spracovanie rámcov zo vzorky 6](#_Toc85726533)

[Výpis všetkých rámcov 6](#_Toc85726534)

[Výpis najviac použitých zdrojových IP adries 6](#_Toc85726535)

[Zobrazenie všetkých TFTP komunikácií 7](#_Toc85726536)

[Zobrazenie ARP komunikácií 7](#_Toc85726537)

[Zobrazenie ICMP rámcov 7](#_Toc85726538)

[Zobrazenie podľa TCP protokolu 7](#_Toc85726539)

[Nájdenie komunikácie podľa vybraného TCP protokolu 7](#_Toc85726540)

[Blokový návrh rozhodovania o určovania rámcu 8](#_Toc85726541)

[Príklady výpisu rámca 9](#_Toc85726542)

# Zadanie úlohy

Cieľom práce je navrhnutie a implementovanie programového analyzátora Ethernet siete, ktorý analyzuje komunikácie v sieti zaznamenané v načítanom .pcap súbore a poskytuje nasledujúce informácie o komunikáciách.

* Výpis všetkých rámcov v hexadecimálnom tvare postupne tak, ako boli zaznamenané v súbore.
  + Poradové číslo rámca v analyzovanom súbore.
  + Dĺžku rámca v bajtoch poskytnutú pcap API, ako aj dĺžku tohto rámca prenášaného po médiu
  + Typ rámca – Ethernet II, IEEE 802.3 (IEEE 802.3 s LLC, IEEE 802.3 s LLC a SNAP, IEEE 802.3 – Raw)
  + Zdrojovú a cieľovú fyzickú (MAC) adresu uzlov, medzi ktorými je rámec prenášaný.
  + Vo výpise jednotlivé bajty rámca usporiadajte po 16 alebo 32 v jednom riadku.
* Výpis vnorených protokolov pre rámce typu Ethernet a IEEE 802.3
* Analýza všetkých odosielajúcich uzlov a výpis najpoužívanejšieho
* Analýza komunikácií protokolov: HTTP, HTTPS, TELNET, SSH, FTP riadiace, FTP dátové, TFTP, ICMP, ARP

# Implementačné prostredie

Program je vytvorený v programovacom jazyku Python vo verzií 3.9. Pre správne fungovanie sa využíva knižnica Scrapy, ktorá slúži iba pre správne načítanie súboru.

# Externé súbory

## db.txt

Súbor slúži pre preklad číselných hodnôt protokolov do textových. Program sa v ňom orientuje podľa indexov, kde ma hladať.

Obrázok, na ktorom je text

Automaticky generovaný popis

## Icmp.txt

Súbor slúži pre rozlišovanie a priraďovanie mien k typom a kódom ICMP rámcov Obrázok, na ktorom je text

Automaticky generovaný popis

# Fungovanie programu

## Používateľské rozhranie

Obrázok, na ktorom je text

Automaticky generovaný popis

Pri spustení programu, program informuje používateľa o tom, ktorý súbor sa načítal.

Ďalej ma používateľ možnosť vyberať akcie podľa jeho rozhodnutia. Menu akcií a voľba si z neho vyberať je zobrazená vždy po vykonaní niektorej z akcií.

Po vykonaní akcií sa výstup vypíše do konzole. Zároveň sa všetky rámce vypíšu aj do externého súboru „frames-output.txt“. Ten sa premazáva každým novým spustením programu.

1. Prvá možnosť zobrazí všetky rámce a informácie o nich
2. Druhá možnosť zobrazí všetky zdrojové IP adresy a vypíše tu najpoužívanejšiu. Zároveň vypíše aj počet použití.
3. Tretia možnosť vypíše všetky TFTP komunikácie
4. Štvrtá možnosť vypíše všetky ARP komunikácie
5. Piata možnosť vypíše všetky ICMP rámce
6. Šiesta možnosť vypíše všetky TCP protokoly podľa voľby používateľa Obrázok, na ktorom je text, elektronika, obvod

   Automaticky generovaný popis
7. Siedma možnosť vypíše všetky TCP komunikácie daného protokolu. Používateľské rozhranie sa správa podobne ako pri možnosti 6.
8. Po stalčení klávesy q sa aplikácia ukončí

## Načítanie a spracovanie rámcov zo vzorky

Na začiatku programu sa zo vzorky načítajú všetky rámce. Tie sa spracujú vo funkcií *„calc\_all\_frames()“*

Všetky rámce sú objekty triedy **Frame,** ktoré majú v sebe všetky svoje vlastnosti.   
Vlastnosti a informácie, ktoré vyplývajú iba z daného rámca si vypočítava objekt sám. Ten iba dostane samotné dáta zo súboru, číslo, ktorý je v poradí a preloženú databázu protokolov z externého súboru db.txt.

Ďalšie vlastnosti a priradenie do komunikácií (ako napríklad TFTP), ktoré vyplývajú aj zo vzťahu k iným rámcom následne vypočítava samotná funkcia *„calc\_all\_frames()“*.

Jediné komunikácie, ktoré sa počítajú mimo tejto funkcie sú komunikácie podľa TCP protokolu.

## Výpis všetkých rámcov

Obrázok, na ktorom je text

Automaticky generovaný popis

Táto funkcia iba prechádza všetky rámce, ktoré dostane ako parameter a vypisuje ich podľa toho, ako to ma rámec definované v triede.

Zároveň táto funkcia robí zálohu do externého súboru.

Funkcia sa využíva aj v iných častiach kódu, stará sa vždy o výpis množiny rámcov.

## Výpis najviac použitých zdrojových IP adries

Samotné adresy a počet ich použití sú zozbierané už v *„calc\_all\_frames()“* funkcií. Táto funkcia ich prehľadáva, vypisuje a zároveň vzájomným porovnávaním hľadá tu najviac používanú.

Potom vypíše tu najpoužívanejšiuObrázok, na ktorom je text

Automaticky generovaný popis

## Zobrazenie všetkých TFTP komunikácií

Vďaka tomu, že všetky komunikácie sú už vypísané. V kóde stačí jedným cyklom ich všetky prejsť a vypísať podľa potrebyObrázok, na ktorom je text

Automaticky generovaný popis

V kóde sa využíva rozšírena funckia výpisu rámcov: *„print\_frames\_limits“*Táto funkcia sa stará o to, aby v prípade veľkého počtu rámcov boli vypísané iba prvých a posledných 10.

## Zobrazenie ARP komunikácií

Táto funkcia tak isto z predom zozbieraných rámcov vypíše všetky rámce. Zároveň informuje aj o tom, či ma komunikácia pár, zdrojovú MAC adresu, cieľovú MAC adresu, zdrojovú IP adresu a cieľovú IP adresu.

## Zobrazenie ICMP rámcov

Funkcia iba prejde všetky rámce a odfiltruje tie, ktoré nie sú ICMP

## Zobrazenie podľa TCP protokolu

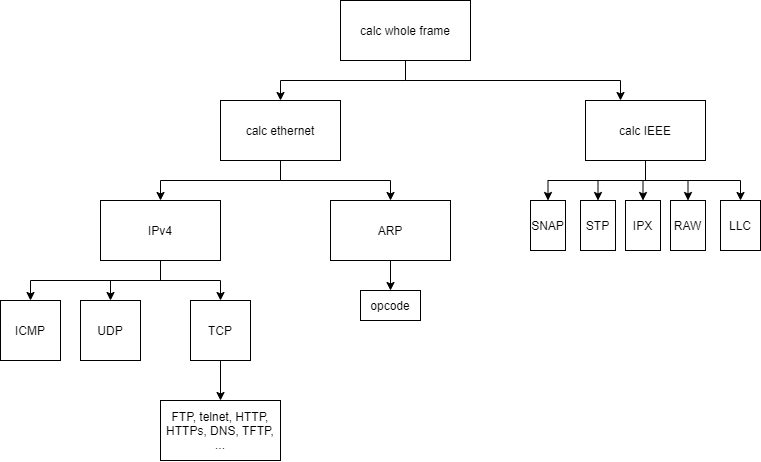
Pre túto funkciu funguje vyhľadávanie všetkých protokolov, ktoré sú v db.txt externom súbore.

## Nájdenie komunikácie podľa vybraného TCP protokolu

Táto funkcia prehľadáva všetky komunikácie a hľadá značky. Podľa nich sa rozhoduje, či vytvorí novú komunikáciu alebo ju priradí k už vytvorenej.

Každá nová vytvorená komunikácia je od začiatku vnímaná ako uzavretá. Po tom ako sa nájde koniec. (reset alebo FIN z oboch strán), sa označí ako uzatvorenú

# Blokový návrh rozhodovania o určovania rámcu



# Príklady výpisu rámca

Obrázok, na ktorom je text

Automaticky generovaný popis

Obrázok, na ktorom je text, elektronika

Automaticky generovaný popis