Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное
учреждение высшего образования
«Национальный исследовательский университет ИТМО»

Мегафакультет: Компьютерных технологий и управления
Факультет: Безопасности информационных технологий
Направление (специальность): 10.03.01 «Информационная безопасность»

Лабораторная работа №2

на тему

«Обработка и тарификация трафика NetFlow»

Вариант №3

Выполнил:
студент группы N3353
Вишняков М.Д.
Проверил:
Федоров Иван Романович

Санкт-Петербург
2020 г.

Цели работы:

1. Привести данный файл в читабельный вид, сформировать собственный файл для тарификации любого формата, с которым удобно работать (в соответствии с вариантом работы)
2. Построить график зависимости объема трафика от времени (любым удобным образом)
3. Протарифицировать абонента с IP-адресом 192.168.250.27 с коэффициентом k: 1руб/Мб

Описание выбранных средств реализации и обоснования выбора

Python - высокоуровневый язык программирования общего назначения, ориентированный на повышение производительности разработчика и читаемости кода. Стандартная библиотека включает большой объём полезных функций.

Причины, по которым выбран Python:

- кроссплатформенность
- обширная стандартная библиотека
- простота написания кода

Microsoft Excel для построения графика.

Выполнение работы

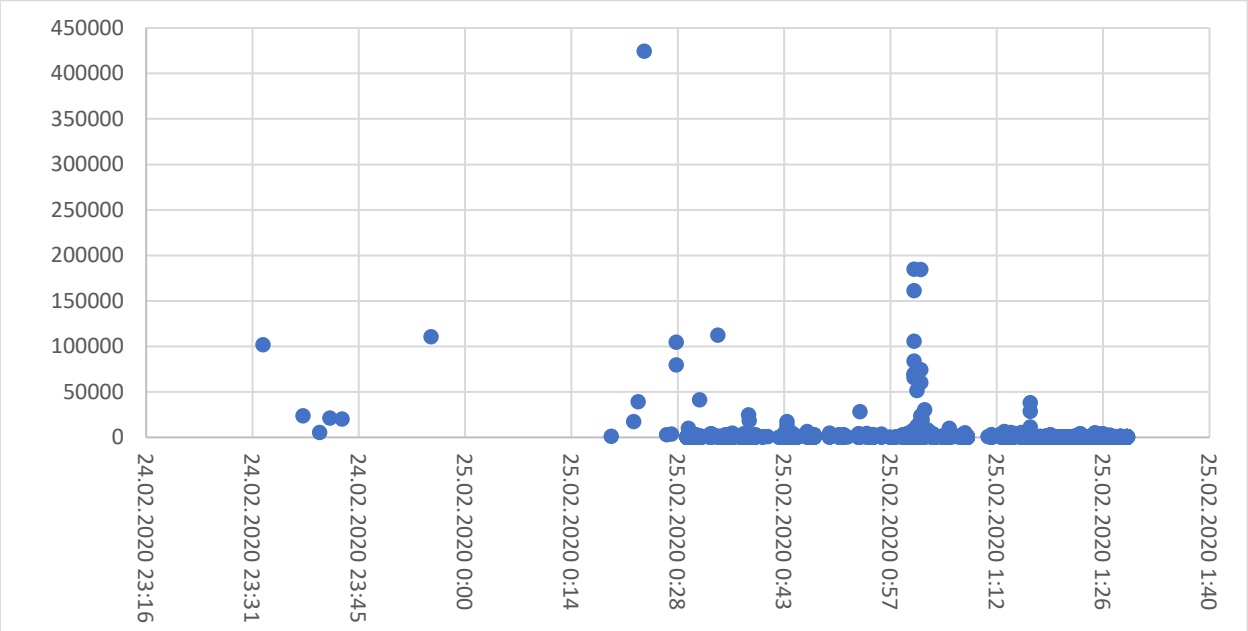
1. Выгружаю данные при помощи утилиты nfdump:

```
max@ubuntu:~/Documents/lab2$ nfdump -r nfcapd.202002251200 -o 'fmt:%ts,%sap,%dap,%ibyt,%obyt'
'src ip 192.168.250.27 or dst ip 192.168.250.27' > traffic.csv
```

traffic.csv

	Date first seen	Src IP Addr:Port	Dst IP Addr:Port	In Byte	Out Byte
2	2020-02-25 00:30:03.680	192.168.250.27:61617	192.168.250.1:53	156	0
3	2020-02-25 00:30:03.680	192.168.250.27:61618	192.168.250.1:53	156	0
4	2020-02-25 00:30:03.680	192.168.250.1:53	192.168.250.27:61617	508	0
5	2020-02-25 00:30:03.680	192.168.250.27:61619	192.168.250.1:53	158	0
6	2020-02-25 00:30:03.680	192.168.250.27:61620	192.168.250.1:53	158	0
7	2020-02-25 00:30:03.680	192.168.250.1:53	192.168.250.27:61618	700	0
8	2020-02-25 00:30:03.690	192.168.250.27:61621	192.168.250.1:53	156	0
9	2020-02-25 00:30:03.690	192.168.250.27:61622	192.168.250.1:53	156	0
10	2020-02-25 00:30:03.690	192.168.250.1:53	192.168.250.27:61620	768	0
11	2020-02-25 00:30:03.690	192.168.250.27:61623	192.168.250.1:53	176	0
12	2020-02-25 00:30:03.690	192.168.250.27:61624	192.168.250.1:53	176	0
13	2020-02-25 00:30:03.690	192.168.250.1:53	192.168.250.27:61619	768	0
14	2020-02-25 00:30:03.690	192.168.250.27:61625	192.168.250.1:53	154	0
15	2020-02-25 00:30:03.690	192.168.250.27:61626	192.168.250.1:53	154	0
16	2020-02-25 00:30:03.700	192.168.250.1:53	192.168.250.27:61622	764	0
17	2020-02-25 00:30:03.700	192.168.250.27:61627	192.168.250.1:53	154	0
18	2020-02-25 00:30:03.700	192.168.250.27:61628	192.168.250.1:53	154	0
19	2020-02-25 00:30:03.700	192.168.250.1:53	192.168.250.27:61621	764	0
20	2020-02-25 00:30:03.700	192.168.250.1:53	192.168.250.27:61624	676	0
21	2020-02-25 00:30:03.700	192.168.250.27:61629	192.168.250.1:53	152	0
22	2020-02-25 00:30:03.700	192.168.250.27:61630	192.168.250.1:53	152	0
23	2020-02-25 00:30:03.700	192.168.250.1:53	192.168.250.27:61623	676	0
24	2020-02-25 00:30:03.710	192.168.250.1:53	192.168.250.27:61626	888	0
25	2020-02-25 00:30:03.710	192.168.250.27:61631	192.168.250.1:53	156	0
26	2020-02-25 00:30:03.710	192.168.250.27:61632	192.168.250.1:53	156	0
27	2020-02-25 00:30:03.710	192.168.250.1:53	192.168.250.27:61625	888	0
28	2020-02-25 00:30:03.710	192.168.250.1:53	192.168.250.27:61628	760	0

2. Построю график зависимости объема трафика от времени для абонента по выгруженным данным:



3. Протарифицирую абонента с IP-адресом 192.168.250.27 при помощи написанной программы.

IP-адрес абонента передаётся как аргумент командной строки.

```
max@ubuntu:~/Documents/lab2$ python3 lab2.py 192.168.250.27
3.25
max@ubuntu:~/Documents/lab2$
```

Таким образом, за заданный промежуток времени абонент должен 3 рубля 25 копеек.

Вывод: в ходе выполнения работы был построен график зависимости объема трафика от времени и написана программа для тарификации абонента.

Листинг

lab2.py

```
import csv
import sys

def calculateCost(stats,ip):
    traffic = 0
    for item in stats:
        if len(item) == 5:
            if item[1].find(ip) != -1:
                trafficString = item[3]
            elif item[2].find(ip) != -1:
                trafficString = item[4]
            if trafficString.find('M') == -1:
                traffic += int(trafficString)
            else:
                traffic += float(piceOfTraffic[:piceOfTraffic.find('M')]) * 1024
* 1024
    return '%.2f' % (traffic / 1024 / 1024)

def main():
    with open('traffic.csv','r') as csvTrafic:
        cost = calculateCost(csv.reader(csvTrafic),sys.argv[1])
        print(cost)

if __name__ == '__main__':
    main()
```