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 №5

Выполнил:
студент группы N3354
Кутьков В.М.
Проверил:
Федоров Иван Романович

Санкт-Петербург
2020 г.

Цели работы:

1. Привести данный файл в читабельный вид
2. Сформировать собственный файл для тарификации любого формата, с которым удобно работать (в соответствии с вариантом работы)
3. Построить график зависимости объема трафика от времени (любым удобным образом)
4. Протарифицировать трафик в соответствии с вариантом.

Вариант 5

Протарифицировать абонента с IP-адресом 192.168.250.59 с коэффициентом k: 1руб/Мб, первые 1000Мб бесплатно.

Описание выбранных средств реализации и обоснования выбора.

Python - высокоуровневый язык программирования общего назначения.

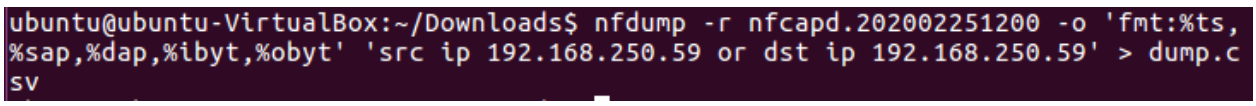
Отличительные особенности, по которым был выбран Python:

- простой в использовании синтаксис,
- наличие большого количества модулей и библиотек под разные задачи,
- универсальность, может применяться для решения задач в различных сферах
- кроссплатформенность

Для построения графика зависимости трафика от времени был использован Microsoft Excel, в силу простоты работы с ним.

Выполнение работы.

1. При помощи nfdump выгружаю необходимые данные:




```
nfdump -r nfcapd.202002251200 -o ‘fmt:%ts,%sap,%dap,%ibyt,%obyt’ ‘src ip
192.168.250.59 or dst ip 192.168.250.59’ > dump.csv
```

Полученный dump.csv

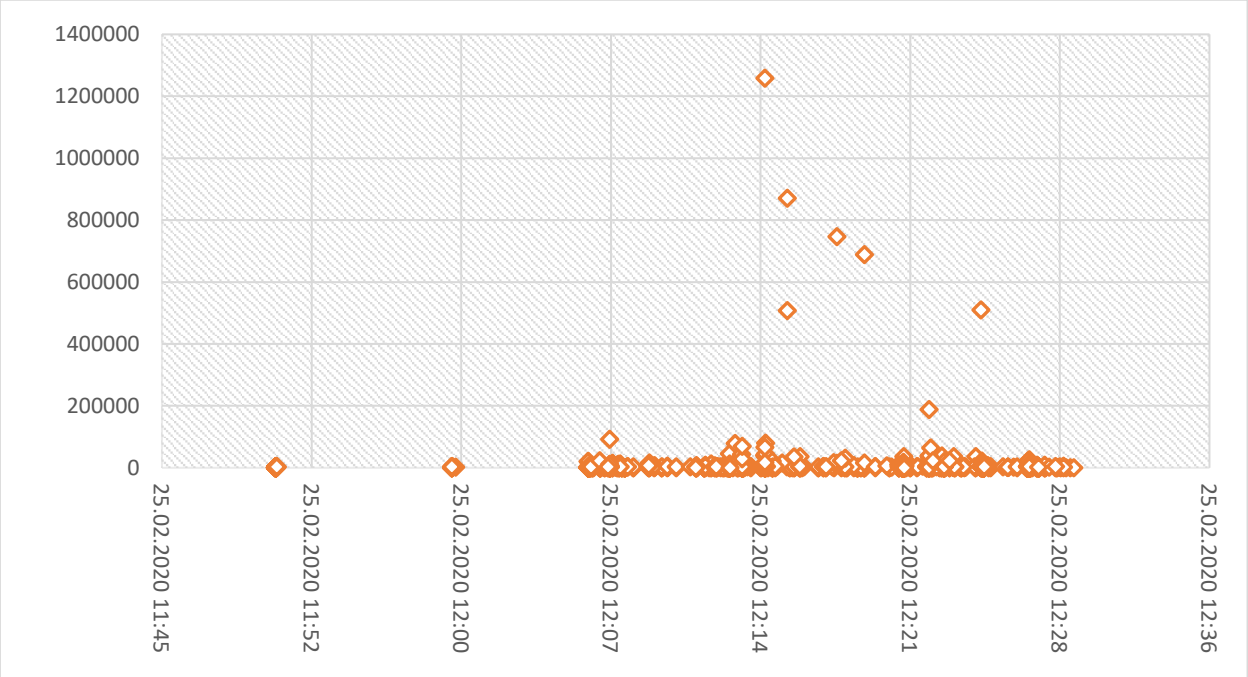
README.md | lab2.py | dump.csv

```
2020-02-25 11:51:04.070,  192.168.250.59:50360,   192.168.250.1:53   ,     126,        0
2020-02-25 11:51:04.070,   192.168.250.1:53   ,  192.168.250.59:50360,     676,        0
2020-02-25 11:51:04.080,  192.168.250.59:50024,  17.253.123.204:80    ,     519,        0
2020-02-25 11:51:04.160,  192.168.250.59:53646,   192.168.250.1:53   ,     146,        0
2020-02-25 11:51:04.170,   192.168.250.1:53   ,  192.168.250.59:53646,     146,        0
2020-02-25 11:51:04.300,  192.168.250.59:64789,   192.168.250.1:53   ,     128,        0
2020-02-25 11:51:04.350,   192.168.250.1:53   ,  192.168.250.59:64789,    1054,        0
2020-02-25 11:51:04.360,  192.168.250.59:50025,   192.168.250.1:53   ,     168,        0
2020-02-25 11:51:04.360,   192.168.250.1:53   ,  192.168.250.59:50025,     120,        0
2020-02-25 11:51:04.360,  192.168.250.59:50026,     54.76.9.103:443  ,    2779,        0
2020-02-25 11:51:04.420,  192.168.250.59:60330,   192.168.250.1:53   ,     132,        0
2020-02-25 11:51:04.430,   192.168.250.1:53   ,  192.168.250.59:60330,     660,        0
2020-02-25 11:51:04.430,  192.168.250.59:50027,   52.50.170.249:443  ,    4238,        0
2020-02-25 11:51:04.560,  192.168.250.59:58122,   192.168.250.1:53   ,     118,        0
2020-02-25 11:51:04.560,  192.168.250.59:55941,   192.168.250.1:53   ,     156,        0
2020-02-25 11:51:04.570,  192.168.250.59:64067,   192.168.250.1:53   ,     132,        0
2020-02-25 11:51:04.570,  192.168.250.59:63028,   192.168.250.1:53   ,     140,        0
2020-02-25 11:51:04.570,   192.168.250.1:53   ,  192.168.250.59:58122,     682,        0
2020-02-25 11:51:04.570,   192.168.250.1:53   ,  192.168.250.59:55941,     658,        0
2020-02-25 11:51:04.570,   192.168.250.1:53   ,  192.168.250.59:64067,     620,        0
2020-02-25 11:51:04.580,   192.168.250.1:53   ,  192.168.250.59:63028,     844,        0
2020-02-25 11:51:04.590,  192.168.250.59:58828,   192.168.250.1:53   ,     130,        0
2020-02-25 11:51:04.600,  192.168.250.59:51992,   192.168.250.1:53   ,     124,        0
2020-02-25 11:51:04.650,   192.168.250.1:53   ,  192.168.250.59:58828,     736,        0
2020-02-25 11:51:04.660,  192.168.250.59:50028,   17.188.133.34:443   ,    1634,        0
2020-02-25 11:51:04.680,   192.168.250.1:53   ,  192.168.250.59:51992,    1078,        0
2020-02-25 11:51:04.690,  192.168.250.59:50029,   192.168.250.1:53   ,     168,        0
2020-02-25 11:51:04.690,   192.168.250.1:53   ,  192.168.250.59:50029,     120,        0
2020-02-25 11:51:04.690,  192.168.250.59:50030,  34.248.175.248:443   ,    2737,        0
2020-02-25 11:51:04.760,  192.168.250.59:50031,   17.188.129.19:443   ,     168,        0
2020-02-25 11:51:04.770,  192.168.250.59:50032,   52.50.170.249:443   ,    3947,        0
2020-02-25 11:51:05.130,  192.168.250.59:50419,   192.168.250.1:53   ,     130,        0
2020-02-25 11:51:05.150,   192.168.250.1:53   ,  192.168.250.59:50419,     658,        0
2020-02-25 11:51:05.310,  192.168.250.59:50034,   3.113.123.149:443   ,     168,        0
2020-02-25 11:51:05.330,  192.168.250.59:58621,   192.168.250.1:53   ,     122,        0
2020-02-25 11:51:05.350,   192.168.250.1:53   ,  192.168.250.59:58621,     650,        0
2020-02-25 11:51:05.460,  192.168.250.59:59494,   192.168.250.1:53   ,     142,        0
2020-02-25 11:51:05.470,   192.168.250.1:53   ,  192.168.250.59:59494,     848,        0
2020-02-25 11:51:05.970,  192.168.250.59:56470,   192.168.250.1:53   ,     128,        0
2020-02-25 11:51:05.980,   192.168.250.1:53   ,  192.168.250.59:56470,    1062,        0
2020-02-25 11:51:05.980,  192.168.250.59:50037,   192.168.250.1:53   ,     168,        0
2020-02-25 11:51:05.980,   192.168.250.1:53   ,  192.168.250.59:50037,     120,        0
2020-02-25 11:51:05.150,  192.168.250.59:50033,  52.197.127.212:443   ,    2838,        0
2020-02-25 11:51:07.040,  192.168.250.59:50040,  34.248.175.248:443   ,    2538,        0
2020-02-25 11:51:07.050,  192.168.250.59:50041,  52.209.165.128:443   ,    2527,        0
2020-02-25 11:51:08.230,  192.168.250.59:50043,  52.209.165.128:443   ,    2175,        0
```

2. Выгрузим данные только для нашего абонента, и используя Microsoft Excel и полученные данные (dump_src_only.csv) строим график зависимости объема трафика от времени

```
ubuntu@ubuntu-VirtualBox:~/Downloads$ nfdump -r nfcapd.202002251200 -o 'fmt:%ts,
%sap,%dap,%ibyt,%obyt' 'src ip 192.168.250.59' > dump_src_only.csv
```

```
nfdump -r nfcapd.202002251200 -o ‘fmt:%ts,%sap,%dap,%ibyt,%obyt’ ‘src ip
192.168.250.59’ > dump_src_only.csv
```



3. Протарифицируем абонента

```
>Lab2.py 192.168.250.59

7.88
```

Вывод: в ходе выполнения работы был сформирован файл для тарификации, построен график зависимости объема трафика от времени, написана программа тарификации, протарифицирован абонент `192.168.250.59`.

Приложение

Lab2.py

```
import csv
import sys

def calculate(dump, ip):
    traffic = 0
    for elem in dump:
        if elem[1].find(ip) != -1: traffic_str = elem[3]
        elif elem[2].find(ip) != -1: traffic_str = elem[4]
        if traffic_str.find('M') == -1: traffic += int(traffic_str)
        else: traffic += float(traffic_str[:traffic_str.find('M')]) * 1024 * 1024
    traffic -= 1000 if traffic >= 1000 else 0
    return '%.2f' % (traffic / 1024 / 1024)

def main():
    with open('dump.csv','r') as csv_dump:
        print(calculate(csv.reader(csv_dump),sys.argv[1]))

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