

**Министерство образования и науки Российской Федерации
Федерально государственное автономное образовательное
учреждение высшего образования
«Санкт-Петербургский национальный исследовательский
университет информационных технологий, механики и оптики»**



Мегафакультет: Компьютерных технологий и управления
Факультет: Безопасности информационных технологий
Кафедра: Проектирования и безопасности компьютерных систем
Направление (специальность): 10.03.01 «Информационная безопасность»

**Лабораторная работа №2
на тему
«Обработка и тарификация трафика NetFlow»
ВАРИАНТ № 3**

Выполнил:

Студент гр.N3352

/Распутина А.А.

Проверил:

Федоров Иван Романович

Санкт-Петербург

2020 г.

Цель работы:

Изучить и программно реализовать правило тарификации для услуг типа “Интернет” по размеру трафика.

Задание:

Вариант № 3 Протарифицировать абонента с IP-адресом 192.168.250.27 с коэффициентом k: 1руб/Мб.

В данной работе предполагается обработка трафика NetFlow v5 из файла nfcapd.202002251200:

В рамках работы требуется:

1. Привести данный файл в читабельный вид (проще всего это сделать с помощью утилиты nfdump)
nfdump -r nfcapd.202002251200
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 задания

Теоретическая часть

NetFlow — это протокол, разработанный компанией Cisco и предназначенный для сбора информации об IP-трафике внутри сети. Маршрутизаторы Cisco анализируют проходящий через интерфейс трафик, суммируют данные и отправляют статистику в формате NetFlow на специальный узел, называемый NetFlow Collector. NetFlow часто используется для ведения биллинга или для анализа трафика сети. Протокол существует в нескольких версиях, последняя версия 9 предназначена для учёта трафика между АС (Автономная Система) и в импортируемых данных имеет несколько дополнительных полей таких как АС источника, АС назначения и пр., но обычно, для биллинга в несложной сети внутри одной АС достаточно информации, содержащейся в данных NetFlow версии 5.

Правила тарификации услуг “Интернет”:

$$X = Q * k,$$

где X - итоговая стоимость, Q - общий объем трафика NetFlow за отчетный период, k - множитель тарифного плана (у каждого варианта свой).

В качестве результата работы необходимо представить программный модуль для обработки, просмотра статистики (график) и тарификации трафика NetFlow. Средства реализации выбираются студентом самостоятельно.

Практическая часть

Чтение файла nfcapd.202002251200 утилитой nfdump:

(если утилита отсутствует – предварительная установка - `sudo apt-get install nfdump`)

`nfdump -r nfcapd.202002251200:`

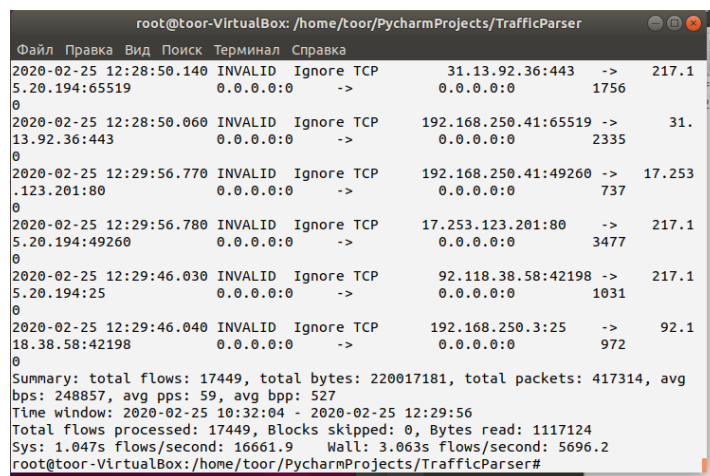


Рис. 1 – Чтение файла nfcapd.202002251200 при помощи nfdump -r nfcapd.202002251200

Перенос данных трафика в текстовый или csv файл производится командой:

`nfdump -r nfcapd.202002251200 > file.txt`

`nfdump -r nfcapd.202002251200 > file.csv`

Date first seen	In Byte	Out Byte	Event	XEvent	Proto	Src IP	Addr:Port	Dst IP	Addr:Port	X-Src IP	Addr:Port	X-Dst IP
2020-02-25 11:21:06.190	572	0	INVALID	Ignore	TCP	192.168.250.3:80	->	23.226.231.226:3682		0.0.0.0	->	
2020-02-25 11:28:30.860	2241	0	INVALID	Ignore	TCP	192.168.250.50:61137	->	40.114.211.99:443		0.0.0.0	->	
2020-02-25 11:29:30.210	308	0	INVALID	Ignore	TCP	192.168.250.3:80	->	23.226.231.226:28857		0.0.0.0	->	
2020-02-25 11:30:01.860	152	0	INVALID	Ignore	UDP	192.168.250.62:58474	->	192.168.250.1:123		0.0.0.0	->	
2020-02-25 11:30:01.860	152	0	INVALID	Ignore	UDP	192.168.250.1:123	->	192.168.250.62:58474		0.0.0.0	->	
2020-02-25 11:30:02.530	132	0	INVALID	Ignore	UDP	192.168.250.50:62595	->	192.168.250.1:53		0.0.0.0	->	
2020-02-25 11:30:02.540	450	0	INVALID	Ignore	UDP	192.168.250.1:53	->	192.168.250.50:62595		0.0.0.0	->	
2020-02-25 11:30:02.540	5023	0	INVALID	Ignore	UDP	192.168.250.50:62596	->	173.194.73.95:443		0.0.0.0	->	
2020-02-25 11:30:02.550	6248	0	INVALID	Ignore	UDP	173.194.73.95:443	->	217.15.20.194:62596		0.0.0.0	->	
2020-02-25 11:30:02.700	126	0	INVALID	Ignore	UDP	192.168.250.50:60512	->	192.168.250.1:53		0.0.0.0	->	
2020-02-25 11:30:02.700	112	0	INVALID	Ignore	UDP	192.168.250.50:56363	->	192.168.250.1:53		0.0.0.0	->	
2020-02-25 11:30:02.700	616	0	INVALID	Ignore	UDP	192.168.250.1:53	->	192.168.250.50:56363		0.0.0.0	->	
2020-02-25 11:30:02.700	502	0	INVALID	Ignore	UDP	192.168.250.1:53	->	192.168.250.50:60512		0.0.0.0	->	
2020-02-25 11:30:02.710	4313	0	INVALID	Ignore	UDP	192.168.250.50:56364	->	108.177.14.94:443		0.0.0.0	->	
2020-02-25 11:30:02.730	4185	0	INVALID	Ignore	UDP	108.177.14.94:443	->	217.15.20.194:56364		0.0.0.0	->	

Рис. 2 – Перенос данных nfcapd.202002251200 в текстовый файл

Date first seen	Event	XEvent	Proto	Src IP	Addr:Port	Dst IP	Addr:Port	X-Src IP	Addr:Port	X-Dst IP	Addr:Port	In Byte	Out Byte
2020-02-25 11:21:06.190	INVALID	Ignore	TCP	192.168.250.3	80	23.226.231.226	3682	0.0.0.0	->	0.0.0.0	->	572	0
2020-02-25 11:28:30.860	INVALID	Ignore	TCP	192.168.250.50	61137	40.114.211.99	443	0.0.0.0	->	0.0.0.0	->	2241	0
2020-02-25 11:29:30.210	INVALID	Ignore	TCP	192.168.250.3	80	23.226.231.226	28857	0.0.0.0	->	0.0.0.0	->	308	0
2020-02-25 11:30:01.860	INVALID	Ignore	UDP	192.168.250.62	58474	192.168.250.1	123	0.0.0.0	->	0.0.0.0	->	152	0
2020-02-25 11:30:01.860	INVALID	Ignore	UDP	192.168.250.1	123	192.168.250.62	58474	0.0.0.0	->	0.0.0.0	->	152	0
2020-02-25 11:30:02.530	INVALID	Ignore	UDP	192.168.250.50	62595	192.168.250.1	53	0.0.0.0	->	0.0.0.0	->	132	0
2020-02-25 11:30:02.540	INVALID	Ignore	UDP	192.168.250.1	53	192.168.250.50	62595	0.0.0.0	->	0.0.0.0	->	450	0
2020-02-25 11:30:02.540	INVALID	Ignore	UDP	192.168.250.50	62596	173.194.73.95	443	0.0.0.0	->	0.0.0.0	->	5023	0
2020-02-25 11:30:02.550	INVALID	Ignore	UDP	173.194.73.95	443	217.15.20.194	62596	0.0.0.0	->	0.0.0.0	->	6248	0
2020-02-25 11:30:02.700	INVALID	Ignore	UDP	192.168.250.50	60512	192.168.250.1	53	0.0.0.0	->	0.0.0.0	->	126	0
2020-02-25 11:30:02.700	INVALID	Ignore	UDP	192.168.250.50	56363	192.168.250.1	53	0.0.0.0	->	0.0.0.0	->	112	0
2020-02-25 11:30:02.700	INVALID	Ignore	UDP	192.168.250.1	53	192.168.250.50	60512	0.0.0.0	->	0.0.0.0	->	616	0
2020-02-25 11:30:02.710	INVALID	Ignore	UDP	192.168.250.50	56364	108.177.14.94	443	0.0.0.0	->	0.0.0.0	->	4313	0
2020-02-25 11:30:02.730	INVALID	Ignore	UDP	108.177.14.94	443	217.15.20.194	56364	0.0.0.0	->	0.0.0.0	->	4185	0

Рис. 3 - Перенос данных nfcapd.202002251200 в CSV файл

Команда для формирования файла, пригодного для парсинга:

`nfdump -r nfcapd.202002251200 -o csv > file.csv`

Результат вычисления для абонента с IP-адресом 192.168.250.27 с коэффициентом k: 1руб/Мб:

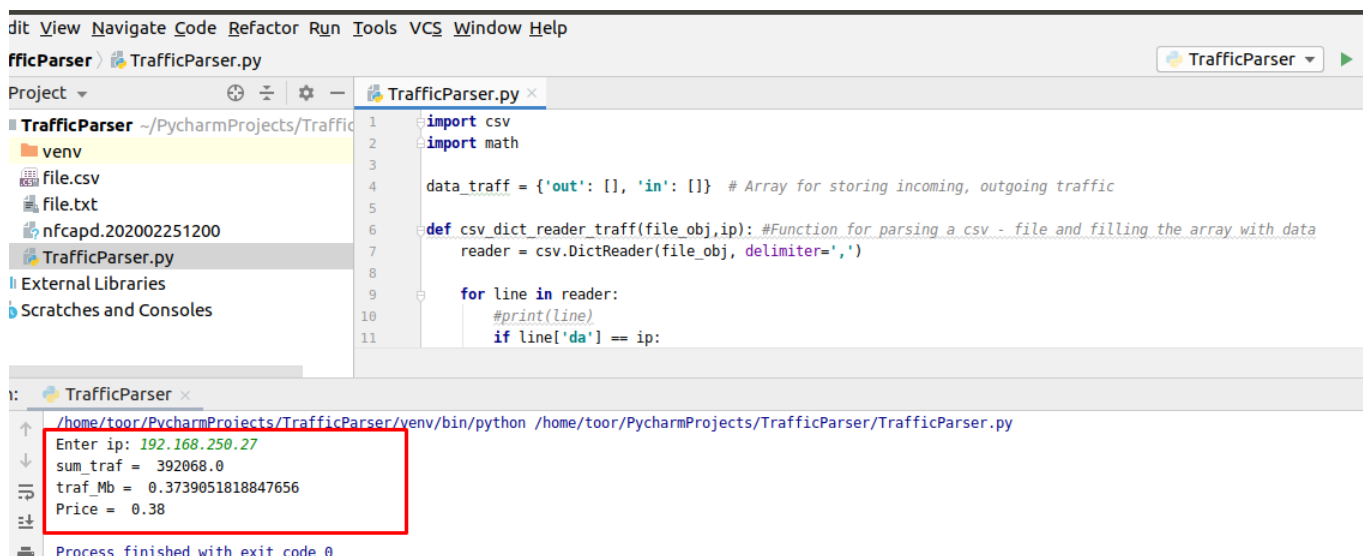


Рис. 4 – Расчет тарифа, отладка приложения в PyCharm

Результат работы программы:

Enter ip: 192.168.250.27

sum_traf = 392068.0 байт

traf_Mb = 0.3739051818847656 Мб

Price = 0.38 руб

Проверка:

Для проверки работы программы были проведены расчеты в Excel с фильтрами по ip из варианта и расчетом суммы к оплате за трафик по тарифу:

Файл

Главная

Вставка

Разметка страницы

Формулы

Данные

Рецензирование

Вид

Справка

Поделиться

Примечания

Вставить

Буфер обмена

Шрифт

Выравнивание

Число

Стили

Ячейки

Редактирование

Конфиденциальность

S38

✕

✓

fx

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
1	Date first seen	Event	XEvent	Proto	Src IP Addr:Port	Dst IP Addr:Port	X-Src IP Addr:Port	X-Dst IP Addr:Port	In Byte	Out Byte						#ЗНАЧ!	Строка	БА	Число	
4	2020-02-25 11:30:03.680	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61617	0.0.0.0:0	-> 0.0.0.0:0	508	0						75	508		508	
7	2020-02-25 11:30:03.680	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61618	0.0.0.0:0	-> 0.0.0.0:0	700	0						75	700		700	СУММА БАЙТ
10	2020-02-25 11:30:03.690	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61620	0.0.0.0:0	-> 0.0.0.0:0	768	0						75	768		768	392068
13	2020-02-25 11:30:03.690	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61619	0.0.0.0:0	-> 0.0.0.0:0	768	0						75	768		768	
16	2020-02-25 11:30:03.700	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61622	0.0.0.0:0	-> 0.0.0.0:0	764	0						75	764		764	СУММА МБ
19	2020-02-25 11:30:03.700	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61621	0.0.0.0:0	-> 0.0.0.0:0	764	0						75	764		764	0,373905182
20	2020-02-25 11:30:03.700	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61624	0.0.0.0:0	-> 0.0.0.0:0	676	0						75	676		676	
23	2020-02-25 11:30:03.700	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61623	0.0.0.0:0	-> 0.0.0.0:0	676	0						75	676		676	Сумма к оплате
24	2020-02-25 11:30:03.710	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61626	0.0.0.0:0	-> 0.0.0.0:0	888	0						75	888		888	0,37390518
27	2020-02-25 11:30:03.710	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61625	0.0.0.0:0	-> 0.0.0.0:0	888	0						75	888		888	0,38
28	2020-02-25 11:30:03.710	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61628	0.0.0.0:0	-> 0.0.0.0:0	760	0						75	760		760	руб
31	2020-02-25 11:30:03.720	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61627	0.0.0.0:0	-> 0.0.0.0:0	760	0						75	760		760	
32	2020-02-25 11:30:03.720	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61630	0.0.0.0:0	-> 0.0.0.0:0	596	0						75	596		596	
35	2020-02-25 11:30:03.720	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61629	0.0.0.0:0	-> 0.0.0.0:0	596	0						75	596		596	
36	2020-02-25 11:30:03.730	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61632	0.0.0.0:0	-> 0.0.0.0:0	700	0						75	700		700	
37	2020-02-25 11:30:03.730	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61631	0.0.0.0:0	-> 0.0.0.0:0	700	0						75	700		700	
38	2020-02-25 11:30:03.730	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61634	0.0.0.0:0	-> 0.0.0.0:0	884	0						75	884		884	
39	2020-02-25 11:30:03.730	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61633	0.0.0.0:0	-> 0.0.0.0:0	884	0						75	884		884	
40	2020-02-25 11:30:03.740	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61636	0.0.0.0:0	-> 0.0.0.0:0	772	0						75	772		772	
41	2020-02-25 11:30:03.740	INVALID	Ignore	UDP	192.168.250.1:53	-> 192.168.250.27:61635	0.0.0.0:0	-> 0.0.0.0:0	772	0						75	772		772	

file

Лист1

+

Рис. 5 – Расчет суммы по абоненту в MS Excel

Итого к оплате: 0,38 руб, следовательно, процедура расчета отрабатывает корректно.

График зависимости объема трафика от времени (любым удобным образом)

При анализе данных необходимо также учитывать, что объем данных может быть указан в разных единицах измерения:

[illegible]

Рис. 6 – Обработка и анализ данных с другими единицами измерения в MS Excel

При построении графика по данным таблицы получаем результат:

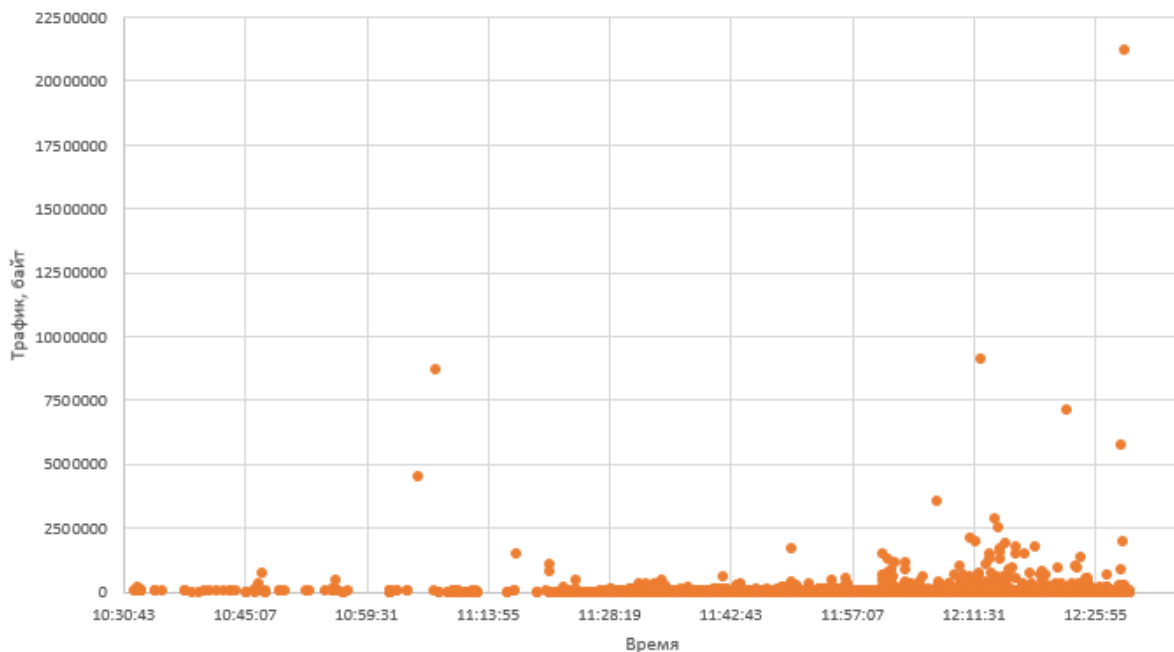


Рис. 7 – График зависимости объема трафика от времени

Анализ трафика:

В течение времени анализа трафика были замечены несколько значительных «пики» трафика» - в 11:06:39, 12:12:18 и в 12:29:18 – максимальное значение - **20.2 Мб**

17327	2020-02-25 12:29:47.250	INVALID	Ignore TCP	192.168.250.41:49254	->	192.168.250.1:53	0.0.0.0	->	0.0.0.0	168	0	#3HA4!	168
17328	2020-02-25 12:29:47.250	INVALID	Ignore TCP	192.168.250.1:53	->	192.168.250.41:49254	0.0.0.0	->	0.0.0.0	120	0	#3HA4!	120
17329	2020-02-25 12:29:18.360	INVALID	Ignore TCP	192.168.250.41:49241	->	17.253.123.202:443	0.0.0.0	->	0.0.0.0	251667	0	#3HA4!	251667
17330	2020-02-25 12:29:18.420	INVALID	Ignore TCP	17.253.123.202:443	->	217.15.20.194:49241	0.0.0.0	->	0.0.0.0	20.2 M	0	#3HA4!	20.2 M
17331	2020-02-25 12:28:46.760	INVALID	Ignore TCP	93.184.220.29:80	->	217.15.20.194:55506	0.0.0.0	->	0.0.0.0	498	0	#3HA4!	498
17332	2020-02-25 12:29:49.180	INVALID	Ignore TCP	192.168.250.41:49256	->	17.253.123.201:80	0.0.0.0	->	0.0.0.0	732	0	#3HA4!	732

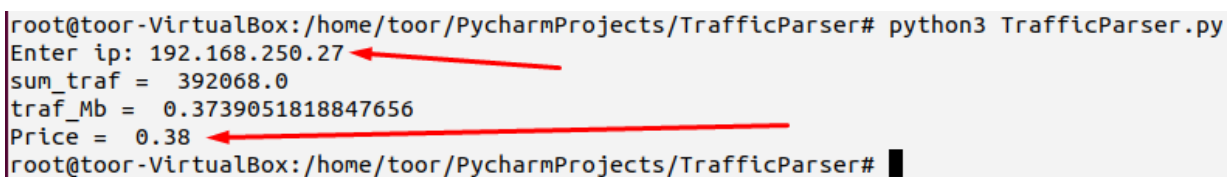
Рис. 8 – Максимальное значение объема трафика от времени

Запуск программы на исполнение производится при помощи команды из директории **TrafficParser** с файлом **TrafficParser.py** (файл с данными file.csv необходим для корректной работы программы):

python3 TrafficParser.py (либо python TrafficParser.py)

После запуска программы необходимо ввести ip-адрес.

В результате работы программы будет выведена сумма к оплате (если ip-адрес отсутствует в файле, будет выведена цена 0 руб):



```
root@toor-VirtualBox:/home/toor/PycharmProjects/TrafficParser# python3 TrafficParser.py
Enter ip: 192.168.250.27
sum_traf = 392068.0
traf_Mb = 0.3739051818847656
Price = 0.38
root@toor-VirtualBox:/home/toor/PycharmProjects/TrafficParser#
```

Рис. 9 – Запуск программы на исполнение и результат работы

Выводы

В результате проделанной работы были изучены и программно реализованы на Python правила тарификации для услуг типа “Интернет” объема трафика”.

Протарифицирован абонент с IP-адресом 192.168.250.27 с коэффициентом к: 1руб/Мб. Также построен и проанализирован график зависимости объема трафика от времени.

Приложение TrafficParser.py:

```
import csv
import math

data_traff = {'out': [], 'in': []} # Array for storing incoming, outgoing traffic

def csv_dict_reader_traff(file_obj, ip): #Function for parsing a csv - file and
filling the array with data
    reader = csv.DictReader(file_obj, delimiter=',')

    for line in reader:
        #print(line)
        if line['da'] == ip:
            data_traff['in'].append(line['ibyt'])
        if line['sa'] == ip:
            data_traff['out'].append(line['obyt'])

def traffic(data): # Payment calculation
    price = 0
    traf_Mb = 0
    sum_traf = 0

    for traf_out in data['out']:
        sum_traf += float(traf_out)
    for traf_in in data['in']:
        sum_traf += float(traf_in)
    traf_Mb = sum_traf / (2**20) # From bytes to Mb

    print('sum_traf = ' , sum_traf )
    print('traf_Mb = ' , traf_Mb )

    price += round(math.ceil(traf_Mb*100)/100, 2)*1 # - 1 rub / Mb
    return price

with open("file.csv") as f_obj:
    ip = input("Enter ip: ")
    csv_dict_reader_traff(f_obj, ip)
    print('Price = ', traffic(data_traff))
```