

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования

САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ



УНИВЕРСИТЕТ ИТМО

Кафедра проектирования и безопасности компьютерных систем

УПРАВЛЕНИЕ МОБИЛЬНЫМИ УСТРОЙСТВАМИ

Лабораторная работа №2

По теме

«Обработка и тарификация трафика NetFlow»

Выполнил:
студент группы N3350
Нгуен В.К.

Проверил:
Федоров И.Р.

Санкт-Петербург,
2020

Цель работы

- Привести данный файл в читабельный вид
- Сформировать собственный файл для тарификации любого формата, с которым удобно работать
- Построить график зависимости объема трафика от времени
- Протарифицировать трафик

Описание работы

Вариант 11:

Протарифицировать абонента с IP-адресом 17.248.150.51
с коэффициентом k: 0.5 руб/Мб

1. Привести данный файл в читабельный вид

С помощью утилиты nfdump:

файл nfcapd.txt создан командой: touch nfcapd.txt

nfdump -r nfcapd.202002251200 -o "fmt:%sa,%da,%byt,%ts,%te"

```
quanglz997@ubuntu:~/Desktop/mobile_lab2$ touch nfcapd.txt
quanglz997@ubuntu:~/Desktop/mobile_lab2$ nfdump -r nfcapd.202002251200 -o "fmt:%sa,%da,%byt,%ts,%te" >> nfcapd.txt
quanglz997@ubuntu:~/Desktop/mobile_lab2$
```

quanglz997@ubuntu: ~/Desktop/mobile_lab2					
File	Edit	View	Search	Terminal	Help
192.168.250.50,	77.111.247.11,	12634,	2020-02-25	01:15:58.070,	2020-02-25 01
:16:04.650					
192.168.250.50,	77.111.247.11,	5493,	2020-02-25	01:16:02.400,	2020-02-25 01
:16:04.650					
192.168.250.50,	77.111.247.11,	5498,	2020-02-25	01:16:02.360,	2020-02-25 01
:16:04.650					
192.168.250.50,	77.111.247.11,	5478,	2020-02-25	01:16:02.360,	2020-02-25 01
:16:04.650					
192.168.250.50,	77.111.247.11,	4441,	2020-02-25	01:15:59.370,	2020-02-25 01
:16:04.650					
77.111.247.11,	217.15.20.194,	6320,	2020-02-25	01:15:59.450,	2020-02-25 01
:16:04.690					
77.111.247.11,	217.15.20.194,	7872,	2020-02-25	01:16:02.260,	2020-02-25 01
:16:04.690					
77.111.247.11,	217.15.20.194,	9360,	2020-02-25	01:15:59.410,	2020-02-25 01
:16:04.690					
185.26.182.106,	217.15.20.194,	4926,	2020-02-25	01:15:58.110,	2020-02-25 01
:16:04.690					
77.111.247.11,	217.15.20.194,	86188,	2020-02-25	01:15:58.100,	2020-02-25 01
:16:04.690					
77.111.247.11,	217.15.20.194,	3086,	2020-02-25	01:15:59.400,	2020-02-25 01
:16:04.690					
77.111.247.11,	217.15.20.194,	9119,	2020-02-25	01:16:02.390,	2020-02-25 01
:16:04.690					

2. Формирование собственного файла для тарификации

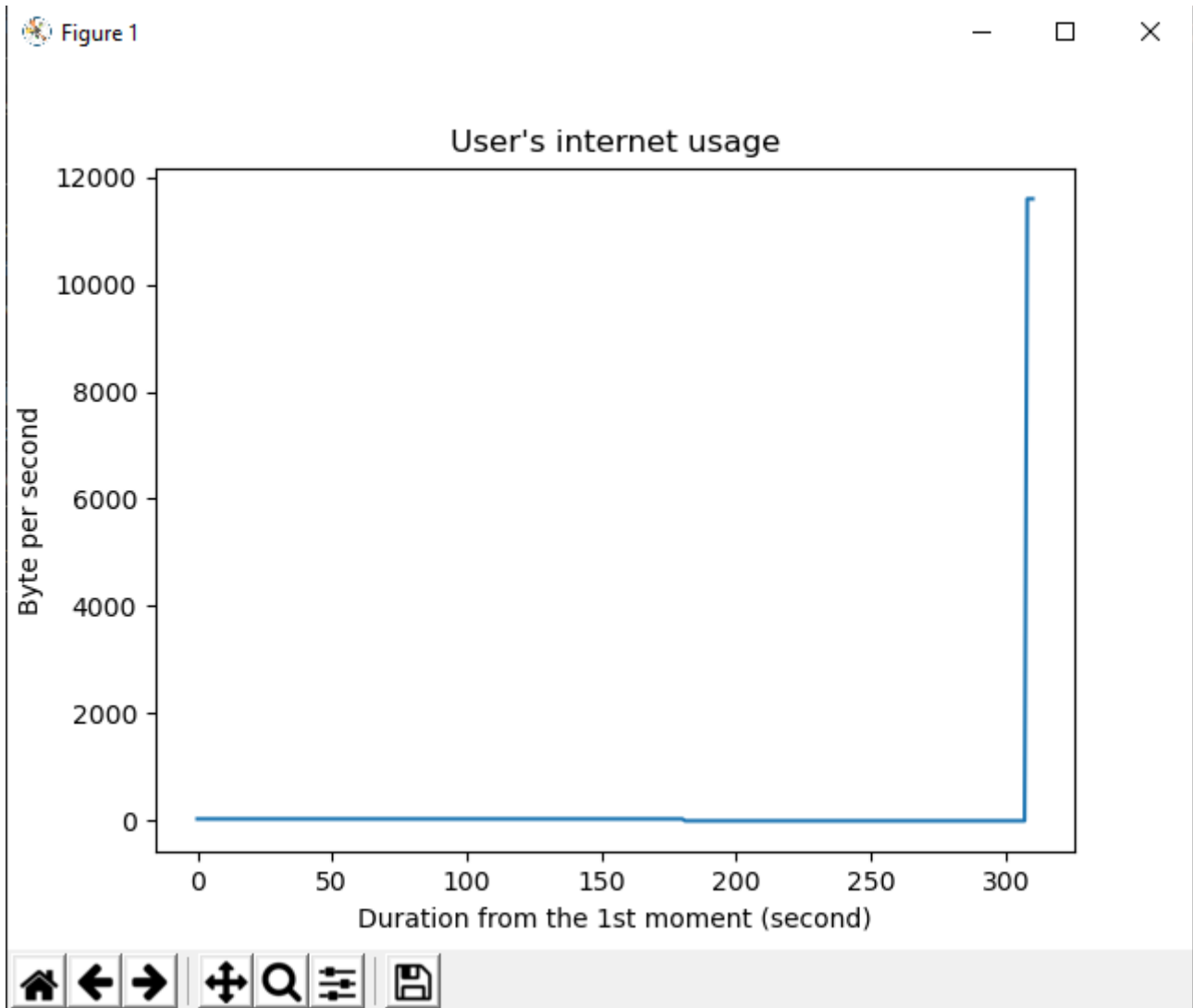
nfcpad.txt ~/Desktop/mobile_lab2							Save			
Src IP Addr	Dst IP Addr	Bytes	Date first seen	Date last seen						
192.168.250.3,	23.226.231.226,	572,	2020-02-25 00:21:06.190,	2020-02-25	00:29:59.190					
192.168.250.50,	40.114.211.99,	2241,	2020-02-25 00:28:30.860,	2020-02-25	00:30:01.130					
192.168.250.3,	23.226.231.226,	308,	2020-02-25 00:29:30.210,	2020-02-25	00:30:01.790					
192.168.250.62,	192.168.250.1,	152,	2020-02-25 00:30:01.860,	2020-02-25	00:30:01.860					
192.168.250.1,	192.168.250.62,	152,	2020-02-25 00:30:01.860,	2020-02-25	00:30:01.860					
192.168.250.50,	192.168.250.1,	132,	2020-02-25 00:30:02.530,	2020-02-25	00:30:02.530					
192.168.250.1,	192.168.250.50,	450,	2020-02-25 00:30:02.540,	2020-02-25	00:30:02.540					
192.168.250.50,	173.194.73.95,	5023,	2020-02-25 00:30:02.540,	2020-02-25	00:30:02.540					
173.194.73.95,	217.15.20.194,	6248,	2020-02-25 00:30:02.550,	2020-02-25	00:30:02.550					
192.168.250.50,	192.168.250.1,	126,	2020-02-25 00:30:02.700,	2020-02-25	00:30:02.700					
192.168.250.50,	192.168.250.1,	112,	2020-02-25 00:30:02.700,	2020-02-25	00:30:02.700					
192.168.250.1,	192.168.250.50,	616,	2020-02-25 00:30:02.700,	2020-02-25	00:30:02.700					
192.168.250.1,	192.168.250.50,	502,	2020-02-25 00:30:02.700,	2020-02-25	00:30:02.700					
192.168.250.50,	108.177.14.94,	4313,	2020-02-25 00:30:02.710,	2020-02-25	00:30:02.710					
108.177.14.94,	217.15.20.194,	4185,	2020-02-25 00:30:02.730,	2020-02-25	00:30:02.730					
192.168.250.27,	192.168.250.1,	156,	2020-02-25 00:30:03.680,	2020-02-25	00:30:03.680					
192.168.250.27,	192.168.250.1,	156,	2020-02-25 00:30:03.680,	2020-02-25	00:30:03.680					
192.168.250.1,	192.168.250.27,	508,	2020-02-25 00:30:03.680,	2020-02-25	00:30:03.680					
192.168.250.27,	192.168.250.1,	158,	2020-02-25 00:30:03.680,	2020-02-25	00:30:03.680					
192.168.250.27,	192.168.250.1,	158,	2020-02-25 00:30:03.680,	2020-02-25	00:30:03.680					
192.168.250.1,	192.168.250.27,	700,	2020-02-25 00:30:03.680,	2020-02-25	00:30:03.680					
192.168.250.27,	192.168.250.1,	156,	2020-02-25 00:30:03.690,	2020-02-25	00:30:03.690					
192.168.250.27,	192.168.250.1,	156,	2020-02-25 00:30:03.690,	2020-02-25	00:30:03.690					
192.168.250.1,	192.168.250.27,	768,	2020-02-25 00:30:03.690,	2020-02-25	00:30:03.690					
192.168.250.27,	192.168.250.1,	176,	2020-02-25 00:30:03.690,	2020-02-25	00:30:03.690					
192.168.250.27,	192.168.250.1,	176,	2020-02-25 00:30:03.690,	2020-02-25	00:30:03.690					
192.168.250.1,	192.168.250.27,	768,	2020-02-25 00:30:03.690,	2020-02-25	00:30:03.690					
192.168.250.27,	192.168.250.1,	154,	2020-02-25 00:30:03.690,	2020-02-25	00:30:03.690					
192.168.250.27,	192.168.250.1,	154,	2020-02-25 00:30:03.690,	2020-02-25	00:30:03.690					
192.168.250.1,	192.168.250.27,	764,	2020-02-25 00:30:03.700,	2020-02-25	00:30:03.700					
192.168.250.27,	192.168.250.1,	154,	2020-02-25 00:30:03.700,	2020-02-25	00:30:03.700					
192.168.250.27,	192.168.250.1,	154,	2020-02-25 00:30:03.700,	2020-02-25	00:30:03.700					
192.168.250.1,	192.168.250.27,	764,	2020-02-25 00:30:03.700,	2020-02-25	00:30:03.700					
192.168.250.1,	192.168.250.27,	676,	2020-02-25 00:30:03.700,	2020-02-25	00:30:03.700					
192.168.250.27,	192.168.250.1,	152,	2020-02-25 00:30:03.700,	2020-02-25	00:30:03.700					
192.168.250.27,	192.168.250.1,	152,	2020-02-25 00:30:03.700,	2020-02-25	00:30:03.700					
192.168.250.1,	192.168.250.27,	676,	2020-02-25 00:30:03.700,	2020-02-25	00:30:03.700					
Plain Text ▾ Tab Width: 8 ▾ Ln 1, Col 1 ▾							INS			

3. Построение графика зависимости объема трафика от времени

input: файл netflow с и IP-адресом (17.248.150.51)

output: график зависимости объема трафика от времени

```
PS C:\Users\QuangLz\Desktop\lab2_--master> py
Python 3.8.2 (tags/v3.8.2:7b3ab59, Feb 25 2020, 22:45:29) [MSC v.1916 32 bit (Intel)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import graphic
>>> graphic.design('17.248.150.51')
>>>
```



4. Тарификация Интернет

input: файл netflow с и IP-адресом (17.248.150.51)

output: тарификации услуг "Интернет tariff"

```
>>> import tariff
>>> tariff.total('17.248.150.51')
0.01961374282836914
>>>
```

Вывод

NetFlow — сетевой протокол, предназначенный для учёта сетевого трафика, разработанный компанией Cisco Systems. Является фактическим промышленным стандартом и поддерживается не только оборудованием Cisco, но и многими другими устройствами (в частности, Juniper, ZTE и Enterasys). Также существуют свободные реализации для UNIX-подобных систем. NetFlow часто используется для ведения биллинга или для анализа трафика сети.

Анализаторы и коллекторы NetFlow — это очень полезный инструментарий для мониторинга и анализа данных сетевого трафика, который поможет вам обнаружить возможные проблемы еще до того, как они станут реальной угрозой. Анализаторы NetFlow позволят вам определить те машины и устройства, которые негативно влияют на пропускную способность вашей сети, найти узкие места в вашей системе, а также, в конечном счете, повысить общую эффективность функционирования вашей 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.