**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

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

**Факультет безопасности информационных технологий**

**Дисциплина:**

**«*Управление мобильными устройствами*»**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2**

**«Обработка и тарификация трафика NetFlow»**

**Выполнил:**

студент гр. N3354, Захаров Е.А.



\_\_\_\_\_\_\_\_\_\_\_\_\_/ Захаров Е.А./

**Проверил:**

аспирант, Федоров И.Р.

\_\_\_\_\_\_\_\_\_\_\_\_\_/ Федоров И.Р. /

Отметка о выполнении: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Цель работы:

Сконвертировать дамп NetFlow Collector’a в читабельный вид, реализовать в виде программного модуля обработчик данных сконвертированных дампов, построить график зависимости объема трафика от времени.

Задание (вариант #4):

Протарифицировать абонента с IP-адресом 192.168.250.59 с коэффициентом k: 0,5руб/Мб до достижения 500Мб, далее 1руб/Мб

Описание работы:

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 Сollector. 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.

Для реализации программного модуля был использован язык программирования Python, из-за его удобства в обработке и анализе табличных данных. Промежуточный csv файл был получен при помощи утилиты nfdump, после чего скорректирован применением регулярных выражений в Notepad++.

Исходный код и все сопутствующие материалы представлены в удаленном репозитории, размещенном по адресу

https://github.com/egozak31/itmo.UMU/tree/master/lab\_2

Пример работы программы:

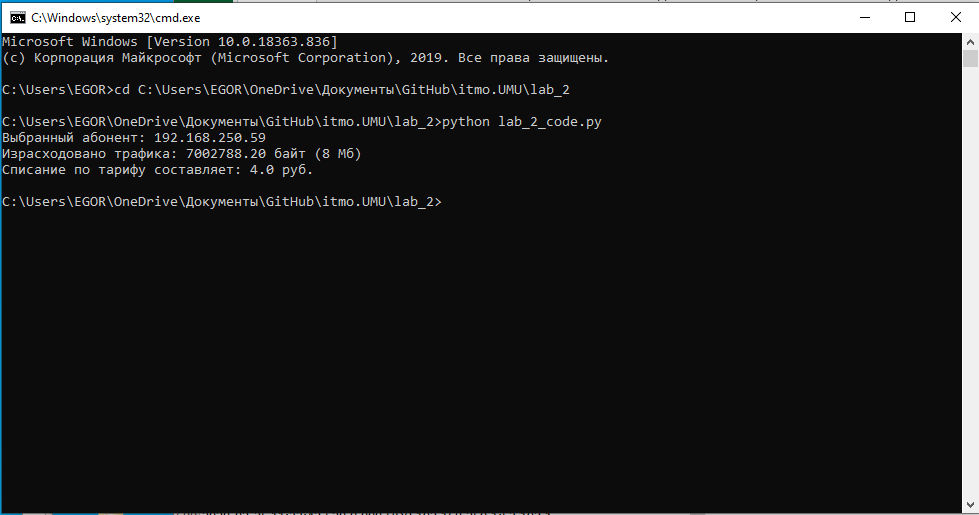


График зависимости объема трафика от времени для 192.168.250.59:



Вывод:

В ходе выполнения работы, я реализовал в виде программного модуля обработчик данных сконвертированных дампов, а также построил график зависимости объема трафика от времени.