МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

Сетевые средства мониторинга операционной системы Linux

Отчет по лабораторной работе 6

по дисциплине «**Системное программное обеспечение**»

студента 3 курса группы ИВТ-б-о-202

Шор Константина Александровича

Направления подготовки 09.03.01«Информатика и вычислительная техника»

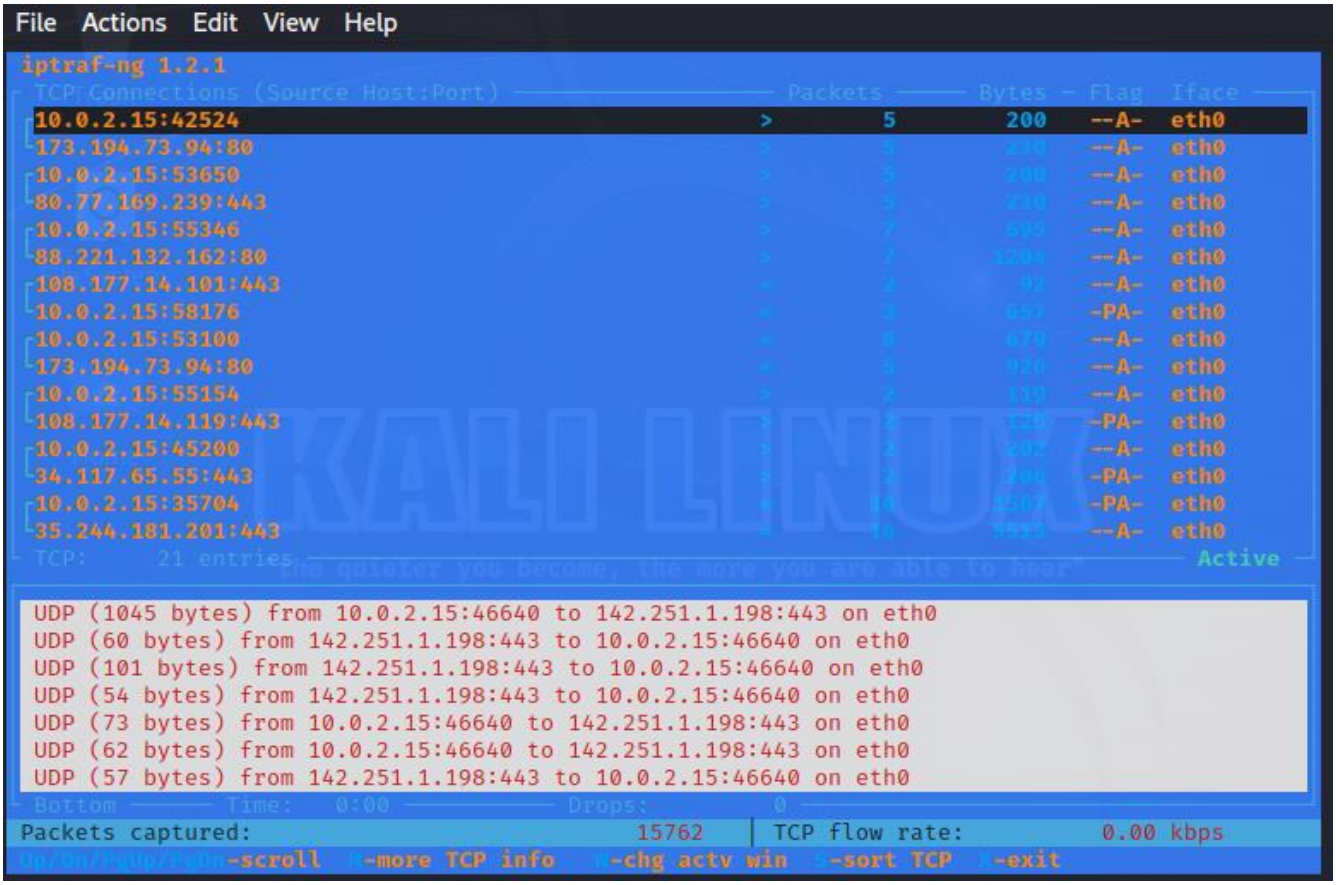
Симферополь, 2023

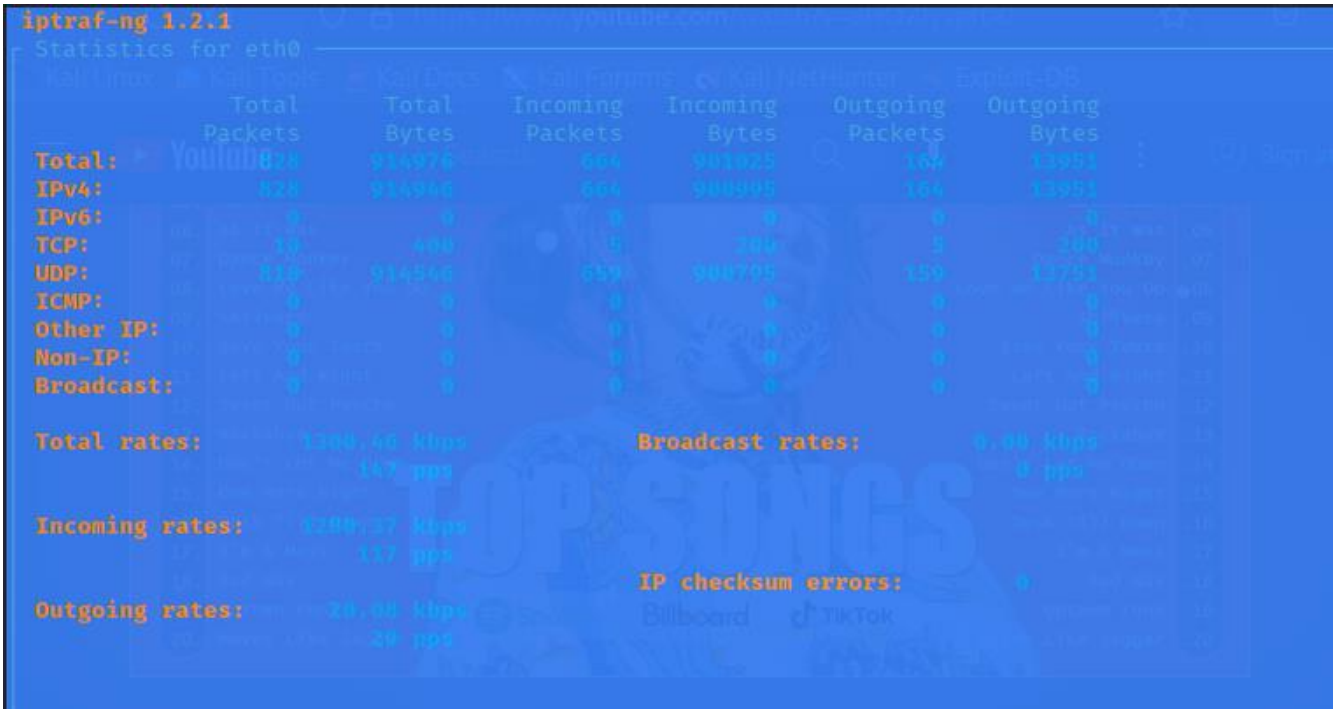
Лабораторная работа №6. Сетевые средства мониторинга операционной системы Linux

Цель работы: Получение навыков использования утилит мониторинга сети, сбор статической информации и представление её в графическом виде.

1. Написать скрипт для сбора статистики с интерфейса. Обеспечить его постоянной загрузкой активности

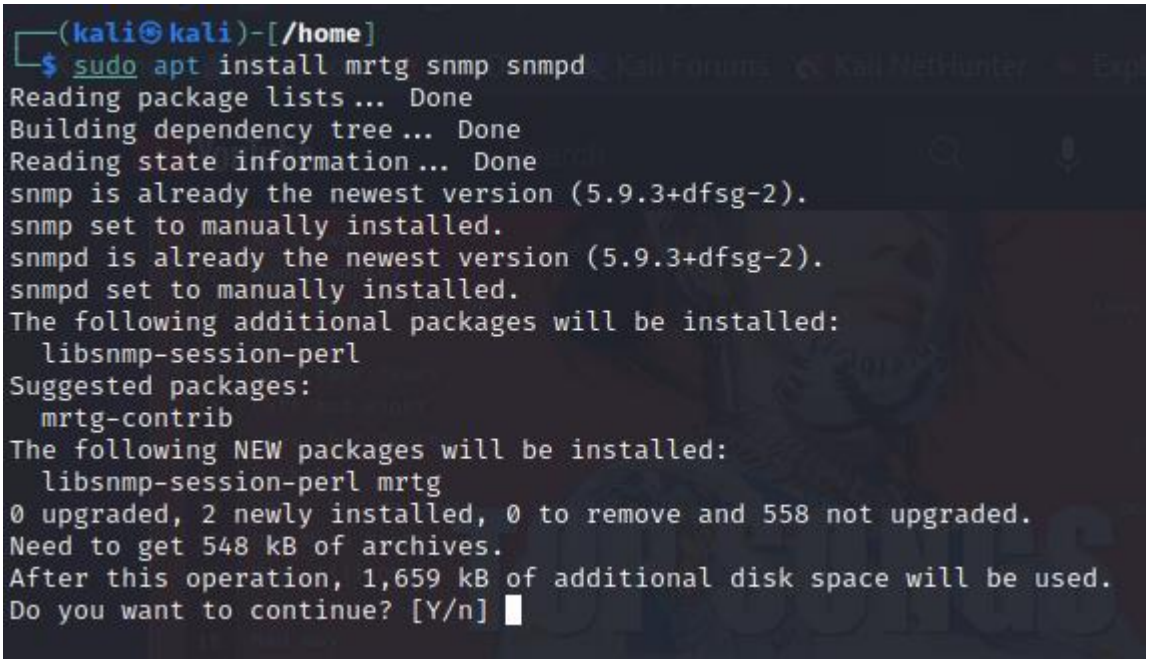
Общая статистика iptraf



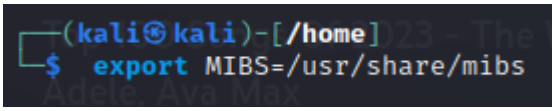

iptraf-ng 1.2.1
Statistics for eth0
Total Packets
Total Bytes
Incoming Packets
Incoming Bytes
Outgoing Packets
Outgoing Bytes
Total:
IPv4:
IPv6:
TCP:
UDP:
ICMP:
Other IP:
Non-IP:
Broadcast:
Total rates:
Broadcast rates:
Incoming rates:
IP checksum errors:
Outgoing rates:

2. Обеспечить сбор данных для формирования графика активности с использованием утилиты mrtg

Установка

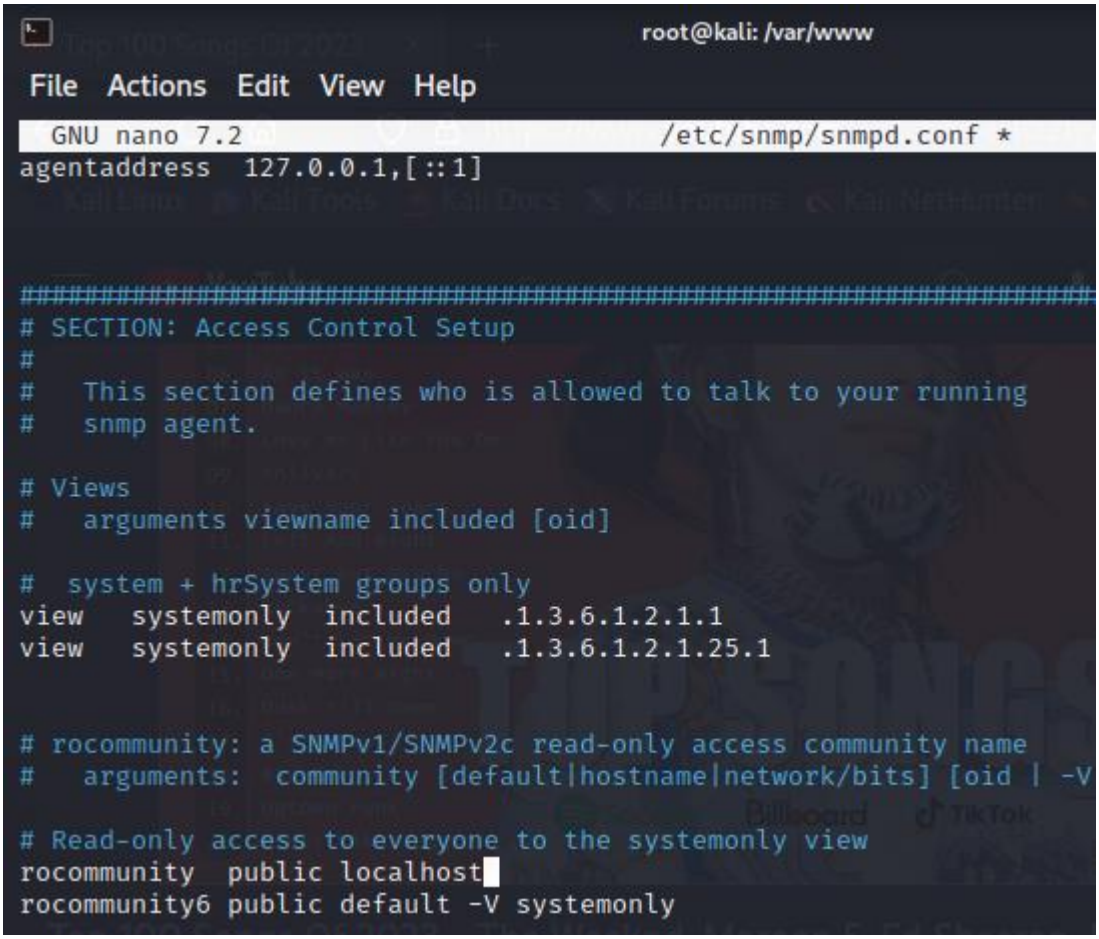


Экспорт



Создание папки и настройка прав доступа

Конфигурация snmpd



Установка рабочей папки и mrtg

```
┌──(root㉿kali)-[/var/www]
└─# systemctl restart snmpd.service

┌──(root㉿kali)-[/var/www]
└─# cfgmaker public@localhost > /etc/mrtg/mrtg.cfg
--base: Get Device Info on public@localhost:
--base: Vendor Id: Unknown Vendor - 1.3.6.1.4.1.8072.3.2.10
--base: Populating confcache
--base: Get Interface Info
--base: Walking ifIndex
--snpd:   public@localhost: → 1 → ifIndex = 1
--snpd:   public@localhost: → 2 → ifIndex = 2
--base: Walking ifType
--snpd:   public@localhost: → 1 → ifType = 24
--snpd:   public@localhost: → 2 → ifType = 6
--base: Walking ifAdminStatus
--snpd:   public@localhost: → 1 → ifAdminStatus = 1
--snpd:   public@localhost: → 2 → ifAdminStatus = 1
--base: Walking ifOperStatus
--snpd:   public@localhost: → 1 → ifOperStatus = 1
--snpd:   public@localhost: → 2 → ifOperStatus = 1
--base: Walking ifMtu
--snpd:   public@localhost: → 1 → ifMtu = 65536
--snpd:   public@localhost: → 2 → ifMtu = 1500
--base: Walking ifSpeed
--snpd:   public@localhost: → 1 → ifSpeed = 10000000
--snpd:   public@localhost: → 2 → ifSpeed = 1000000000
```

Создание индексного файла для веб сервера

```
┌──(root㉿kali)-[/var/www]
└─# indexmaker /etc/mrtg/mrtg.cfg > /var/www/mrtg/index.html
```

Создал файл VirtualHost для сервера

```
 GNU nano 7.2                    /etc/apache2/sites-available/mrtg.conf
Alias /mrtg "/var/www/mrtg/"
<Directory "/var/www/mrtg/">
 Options None
 AllowOverride None
 Require all granted
</Directory>
ServerName firs_server
<Directory "/var/www/mrtg/">
 Order allow,deny
 Allow from all
</Directory>
```

Срипт обновления

```
#!/bin/bash
LANG=C
export $LANG
/usr/bin/mrtg /etc/mrtg/mrtg.cfg --logging /var/log/mrtg.log
```

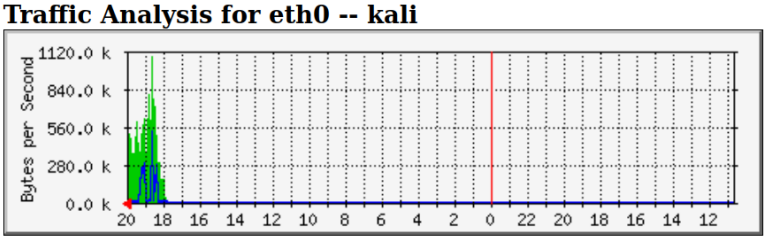
Настройка cron

```
*/4 * * * * /etc/mrtg/mrtg.sh
```

3. Сформировать график сетевой активности

MRTG Index Page

Traffic Analysis for eth0 -- kali



MRTG MULTI ROUTER TRAFFIC GRAPHER

version 2.17.10

Tobias Oetiker <tobi@oetiker.ch>
and Dave Rand <dlr@bungi.com>

4. Создать кольцевую БД rrd и обеспечить её постоянное обновление данными сетевой активности

Создание колцевой БД

```
┌──(root㉿kali)-[/var/local]
└─# rrdtool create eth0.rrd --step 300 DS:input:COUNTER:600:U:U\
DS:output:COUNTER:600:U:U RRA:AVERAGE:0.5:1:576 RRA:MAX:0.5:1:576\
RRA:AVERAGE:0.5:6:672 RRA:MAX:0.5:6:672 RRA:AVERAGE:0.5:24:732\
RRA:MAX:0.5:24:732 RRA:AVERAGE:0.5:144:1460 RRA:MAX:0.5:144:1460
```

Создание скрипта обновления

```
  GNU nano 7.2                                  /home/kali/rrd_cron.sh
#!/bin/bash
INPUT=`/sbin/ifconfig $1 |grep bytes | cut -d ' ' -f 14 | head -n1`
OUTPUT=`/sbin/ifconfig $1 |grep bytes | cut -d ' ' -f 14 | head -n2|tail -n1`
rrdtool update /var/local/eth0.rrd -t "input:output" N:$INPUT:$OUTPUT
```

Настройка cron

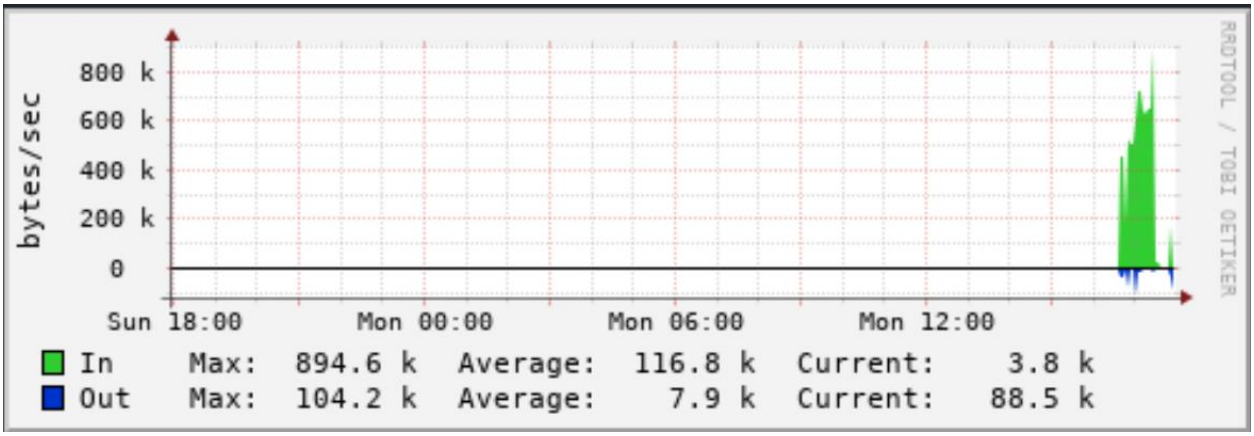
```
*/5 * * * * /var/local/eth1_update.sh
```

5. Сгенерировать график сетевой активности за заданный промежуток времени

Генерация графика

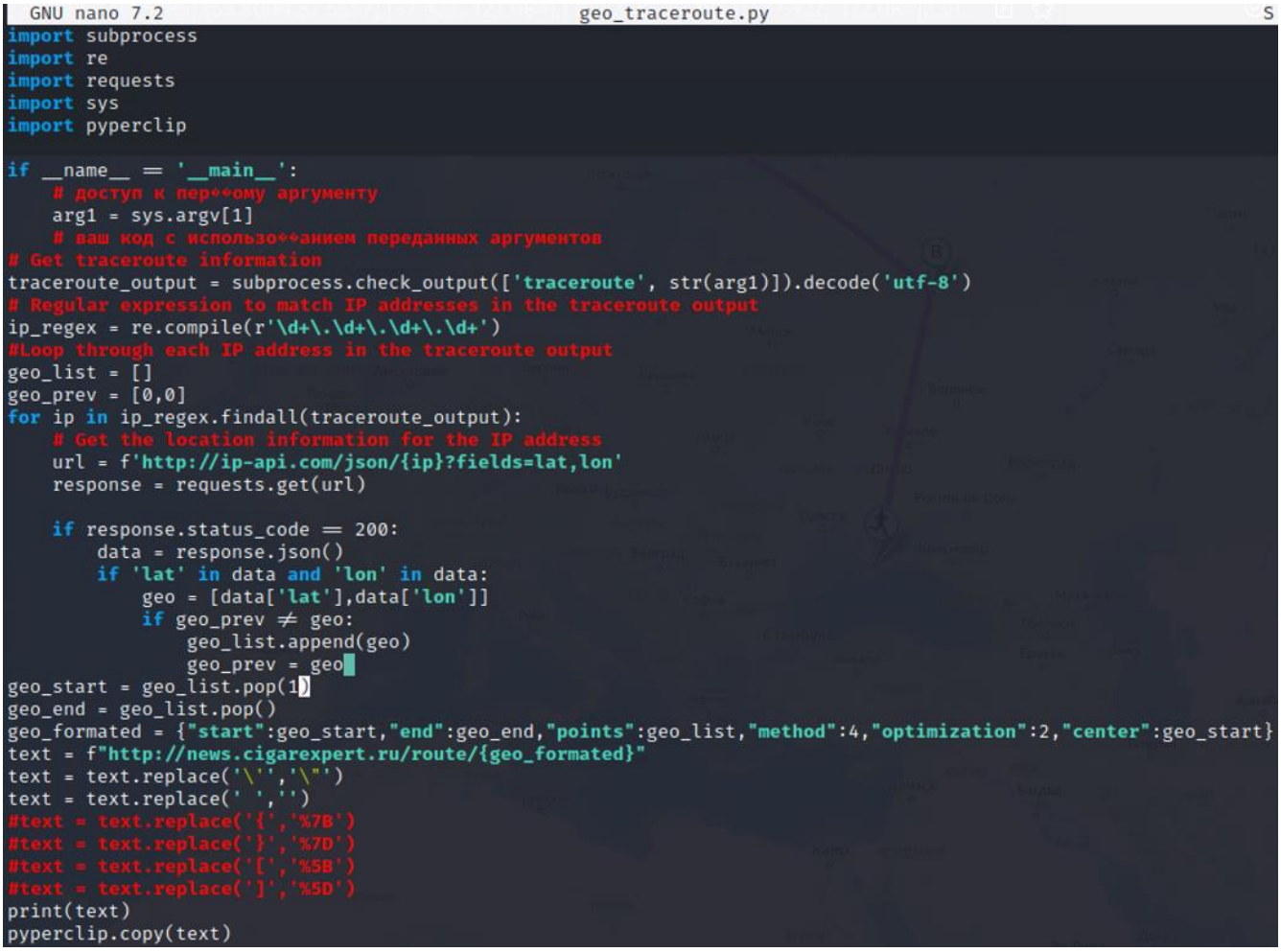
```
┌──(root㉿kali)-[/var/local]
└─# rrdtool graph net.png -v bytes/sec --slope-mode --imgformat PNG\
 DEF:input=eth0.rrd:input:AVERAGE DEF:output=eth0.rrd:output:AVERAGE\
 CDEF:output_neg=output,-1,* AREA:input#32CD32:"In " "GPRINT:input:MAX: Max\\: %6.1lf\
 %s" "GPRINT:input:AVERAGE:Average\\: %6.1lf %S" "GPRINT:input:LAST:Current\\: %6.1lf\
 %S\\n" HRULE:0#000000 AREA:output_neg#0033CC:"Out" "GPRINT:output:MAX: Max\\:\
 %6.1lf %S" "GPRINT:output:AVERAGE:Average\\: %6.1lf %S"\
 "GPRINT:output:LAST:Current\\: %6.1lf %S\\n"

497×169
```

График



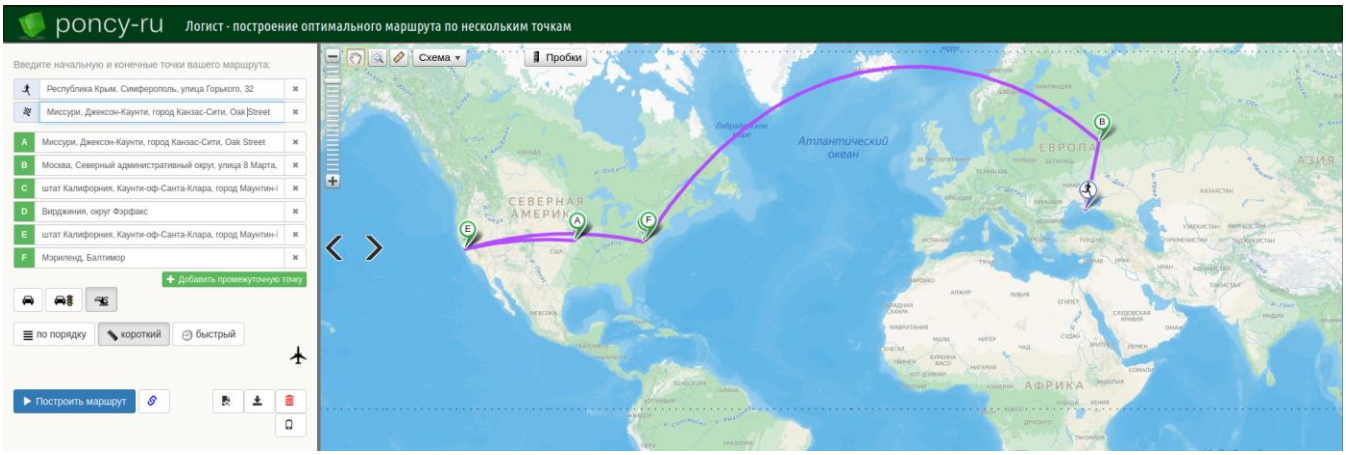
6. Проверить работоспособность при обращении к некоторым общедоступным веб-ресурсам при помощи утилит трассировки маршрута

Тело скрипта



Пример скрипта

```
┌──(kali㉿kali)-[/var/local/geo_traceroute]
└─$ python3 geo_traceroute.py kaggle.com
http://news.cigarexpert.ru/route/{"start":[44.9529,34.0919],"end":[39.0997,-94.5785],"points":[[39.0997,-94.5785],[5
5.8004,37.5557],[37.422,-122.084],[38.8754,-77.3853],[37.422,-122.084],[39.2891,-76.5583]],"method":4,"optimization"
:2,"center":[44.9529,34.0919]}
```



Вывод: В ходе данной лабораторной работе я получил навыков использования утилит мониторинга сети, сбор статистической информации и представление ее в графическом виде, написал скрипты для выполнения данных задач, также проверил работу утилит и приобрел навыки написания скриптов