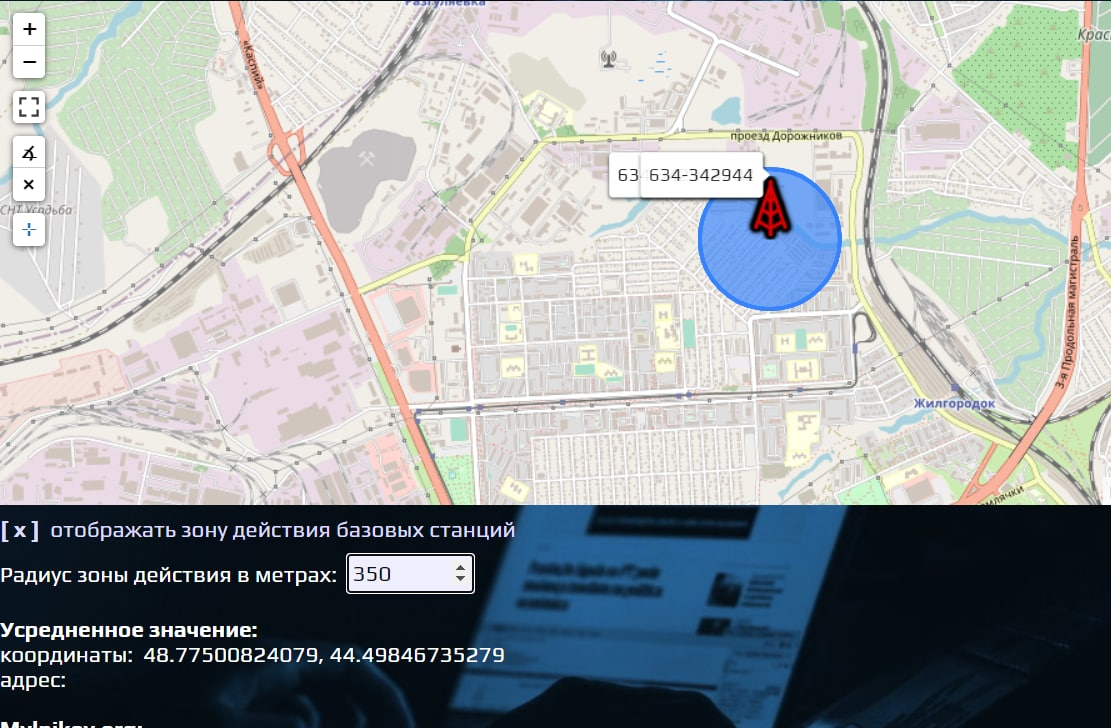
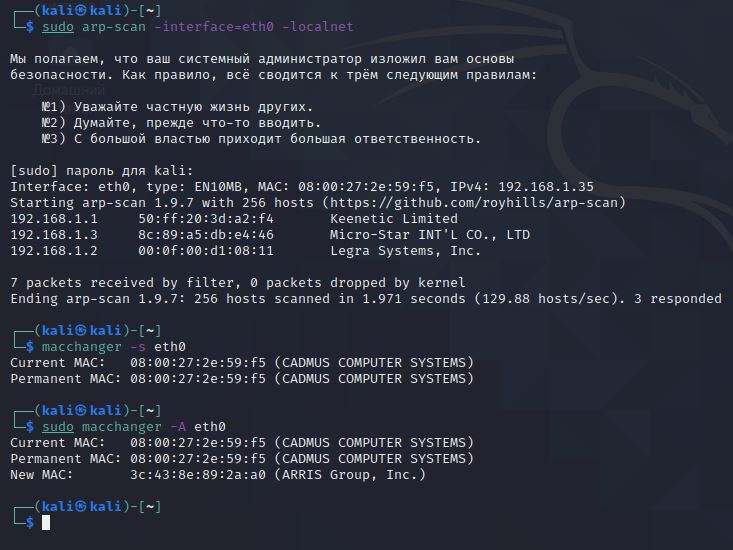
# Практика №7

1. Определение идентификаторов базовой станции

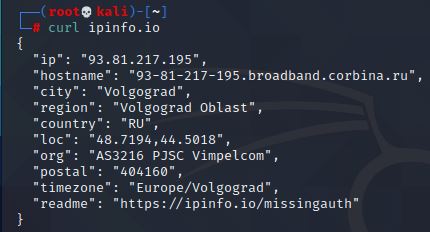
Я установил приложение netmonitor на свой телефон и получил идентификаторы сотовой вышки. После чего зашёл на сайт xinit.ru, ввёл данные сотовой вышки:



1. MAC-адрес

Для получения mac-адресов сети и определения производителя я запустил терминал и ввёл команду $ sudo arp-scan –interface=eth0 –localnet. Далее я ввёл команду $ macchanger –s eth0, чтобы узнать значение mac до изменения значения. После этого я ввёл команду $ sudo macchanger –A eth0 и получил новое значение mac для сетевого устройства, которое идентифицируется как Arpis:

1. IP-адрес

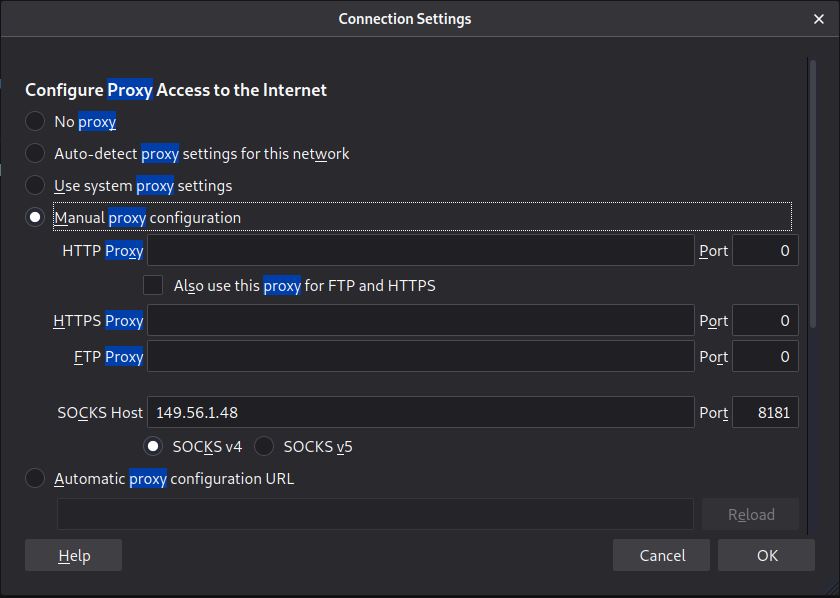
Я зашёл в Kali Linux через суперпользователя (root), чтобы узнать выходной ip-адрес в глобальной сети. После ввода команды $ curl ipinfo.io терминал мне выводит следующее:

Выведенный в командной строке Kali Linux ip-адрес совпал с ip-адресом в глобальной сети.

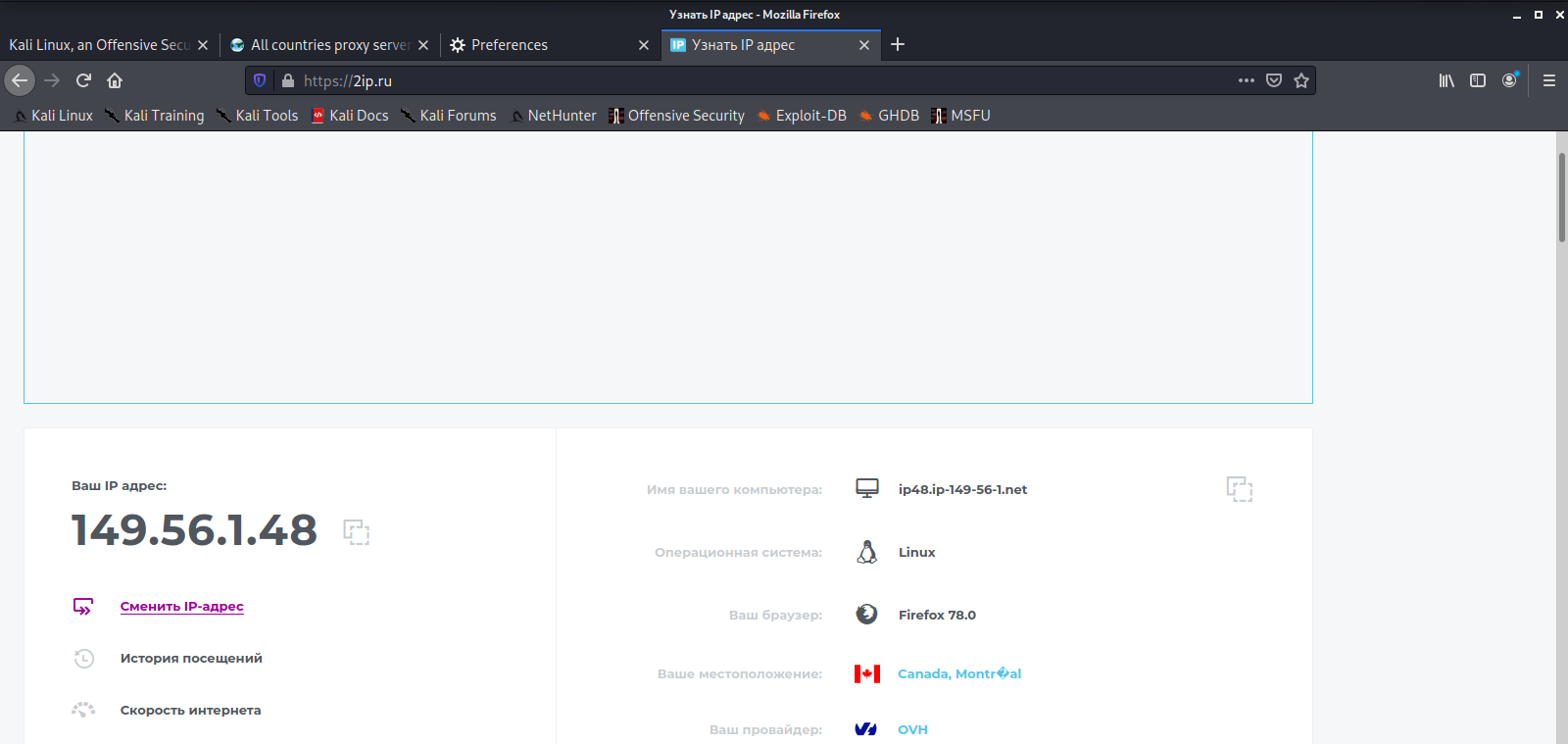
1. Выход в Интернет через proxy

Я зашёл на сайт с прокси и выбрал канадский ip-адрес с портом 8181:

F:\screenshots\2020-12-07 20_30_30.jpg

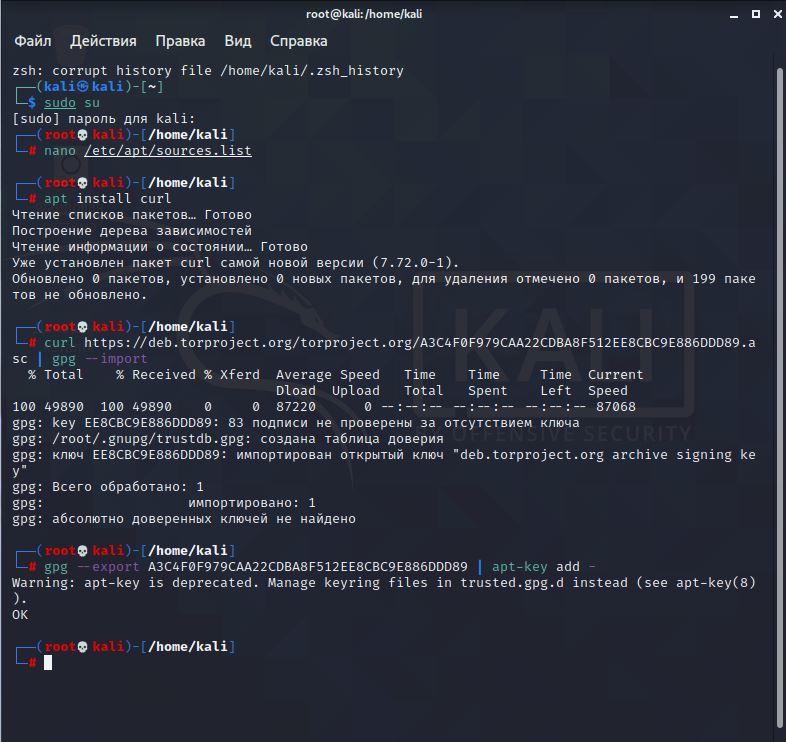


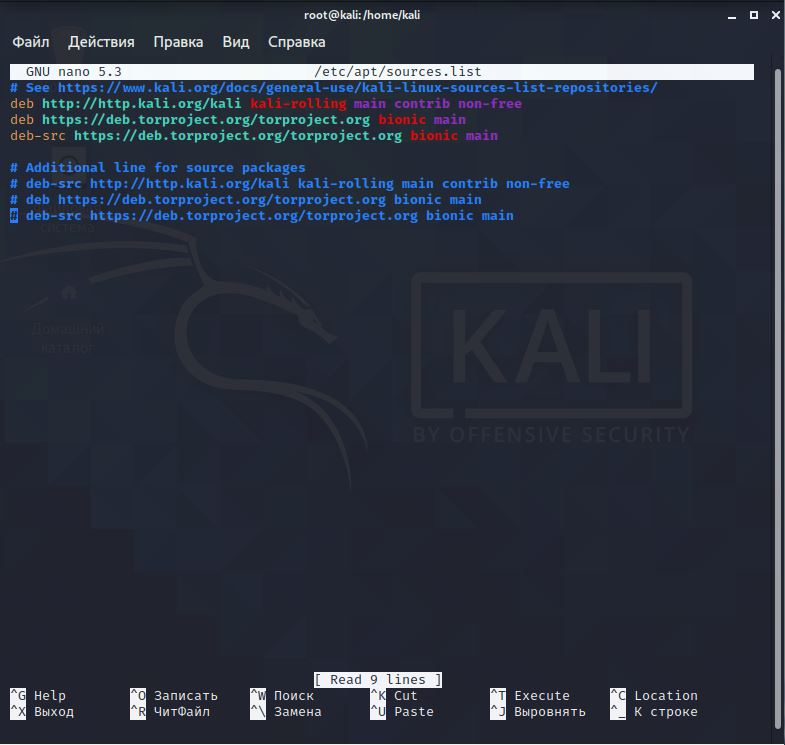
Затем зашёл на сайт 2ip.ru, который показывает тот ip-адрес, что я вписал в настройки браузера:

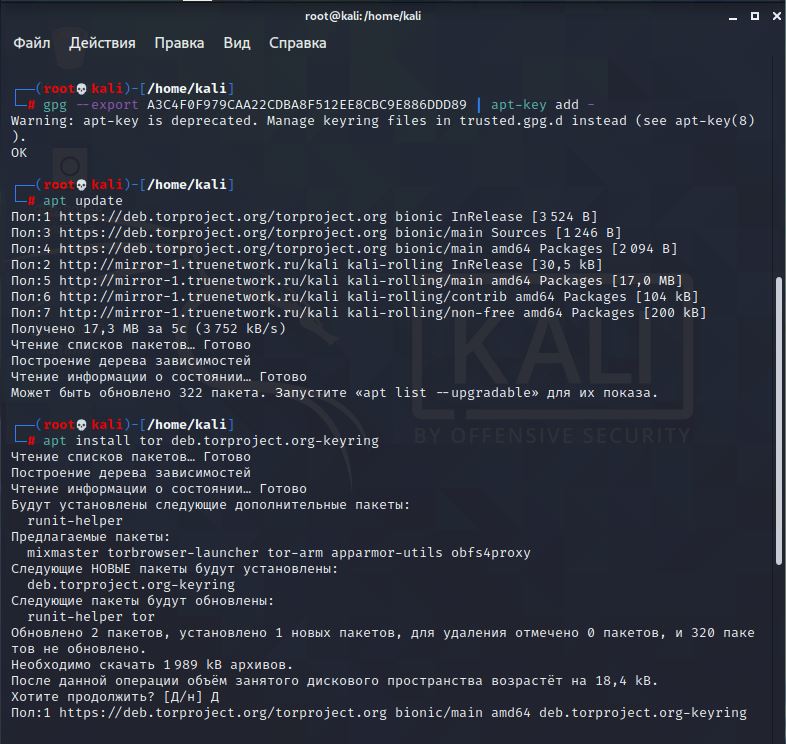


1. Установка TOR

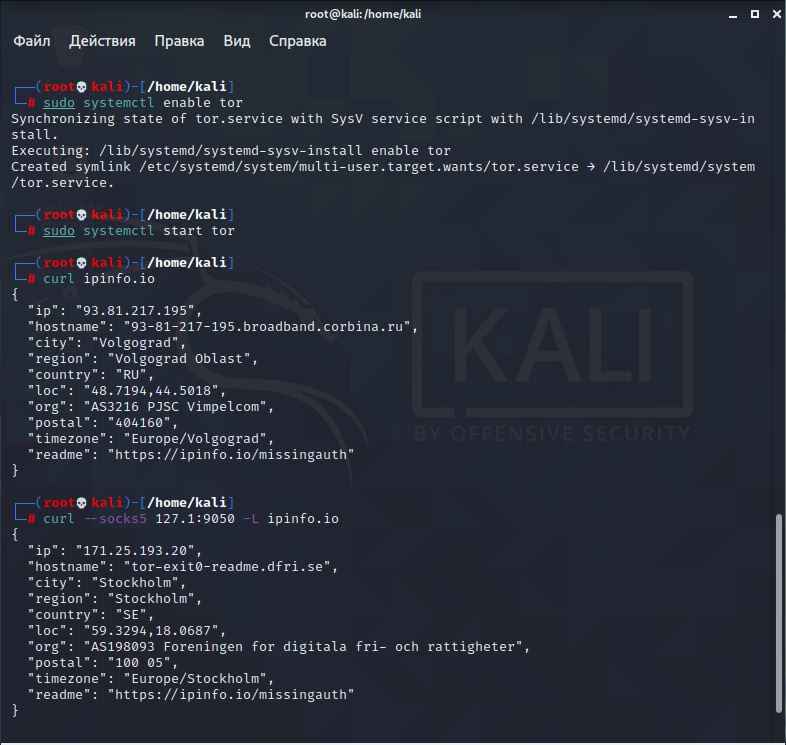
Сначала я ввёл команду $ sudo apt install tor, чтобы установить tor, затем с помощью команды $ sudo su перешёл в суперпользователя. Чтобы модифицировать файл sources.list, я ввёл команду # nano /etc/apt/sources.list. У меня открылось окно, куда я добавил адрес репозитория Torproject. После модификации я ввёл строчку # apt install curl, чтобы установить библиотеку curl для работы с URL-адресами и возможности работать с самыми разными протоколами. После установки я импортировал ключ из репозитория, введя команду # curl … | gpg –import, а после экcпортировал, введя команду # gpg – export “ключ” | apt-key add -:





После чего обновил систему через ввод команды # apt update и установил tor через ввод команды # apt install tor deb.torproject.org-keyring:

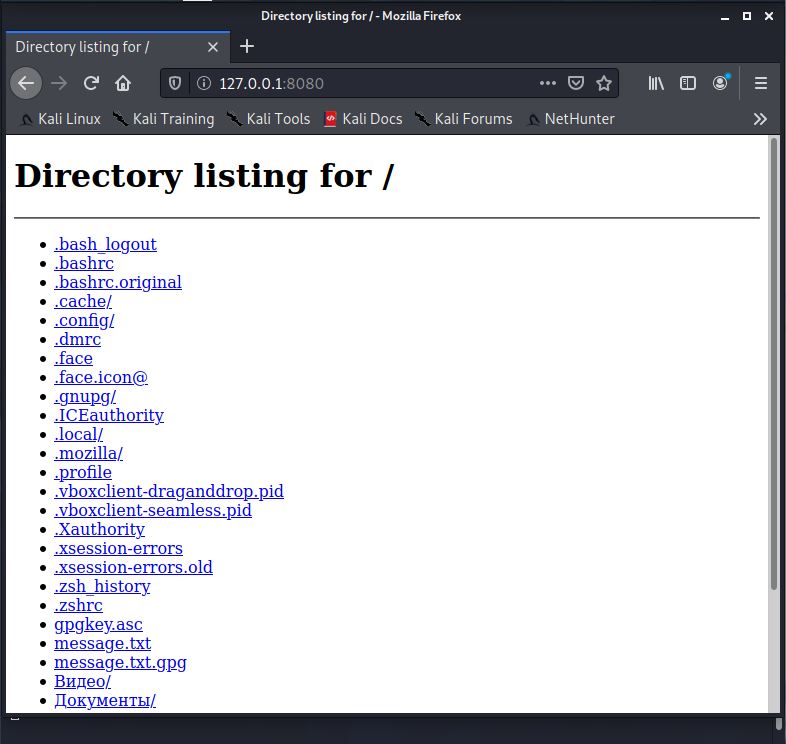
С помощью команд # sudo systemctl enable tor и # sudo systemctl start tor я запустил и добавил службу Tor в автозагрузку. С помощью команды # curl ipinfo.io я проверил свой текущий IP-адрес, а, введя команду # curl –socks5 127.1:9050 –L ipinfo.io я проверил свой IP-адрес через tor:



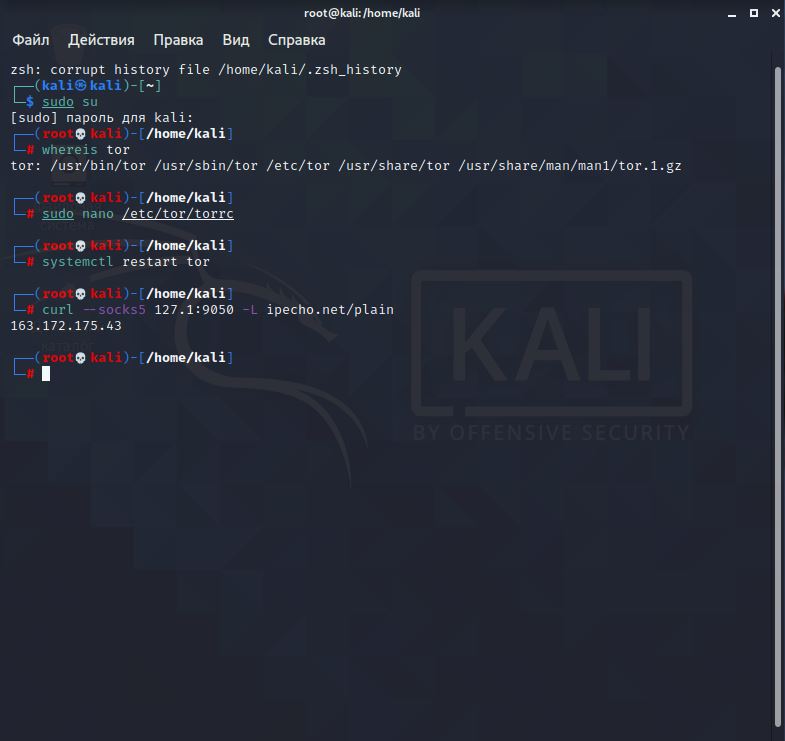
Для проверки работоспособности tor я запустил тестовый web-сервер с помощью команды # python3 –m http.server – bind 127.0.0.1 8080:

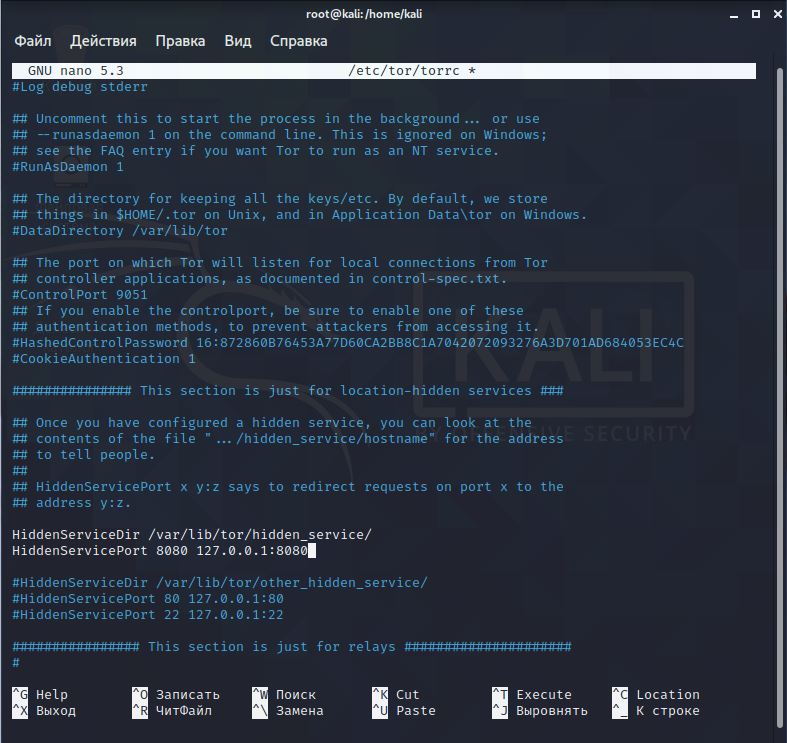


В поисковую строку браузера я ввёл 127.0.0.1 8080, чтобы проверить работоспособность сервера:

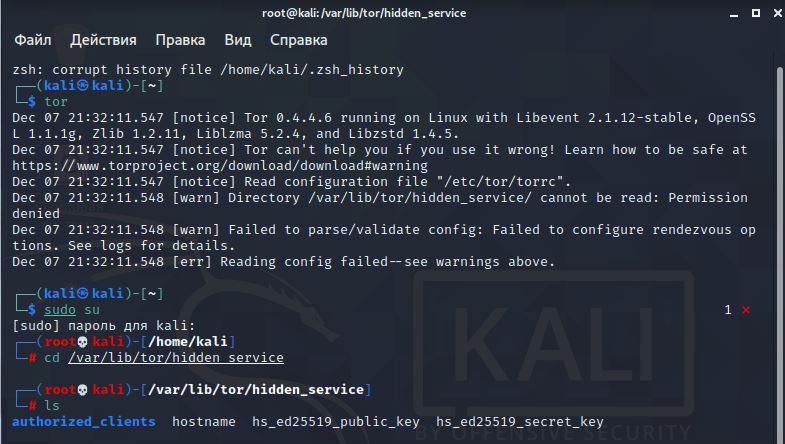


Далее, чтобы узнать, где находится установленный tor, я ввёл команду # whereis tor. После того, как я узнал, где находится tor, ввёл команду # sudo nano /etc/tor/torrc, чтобы найти конфигурационный файл. Мне открылось окно с содержимым конфигурационного файла, где я отредактировал 2 строчки. Далее, чтобы узнать, что tor работает, я написал ту же команду, что и в тот раз, и узнал свой IP-адрес через tor:

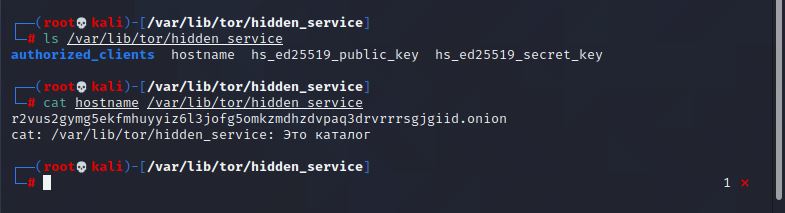




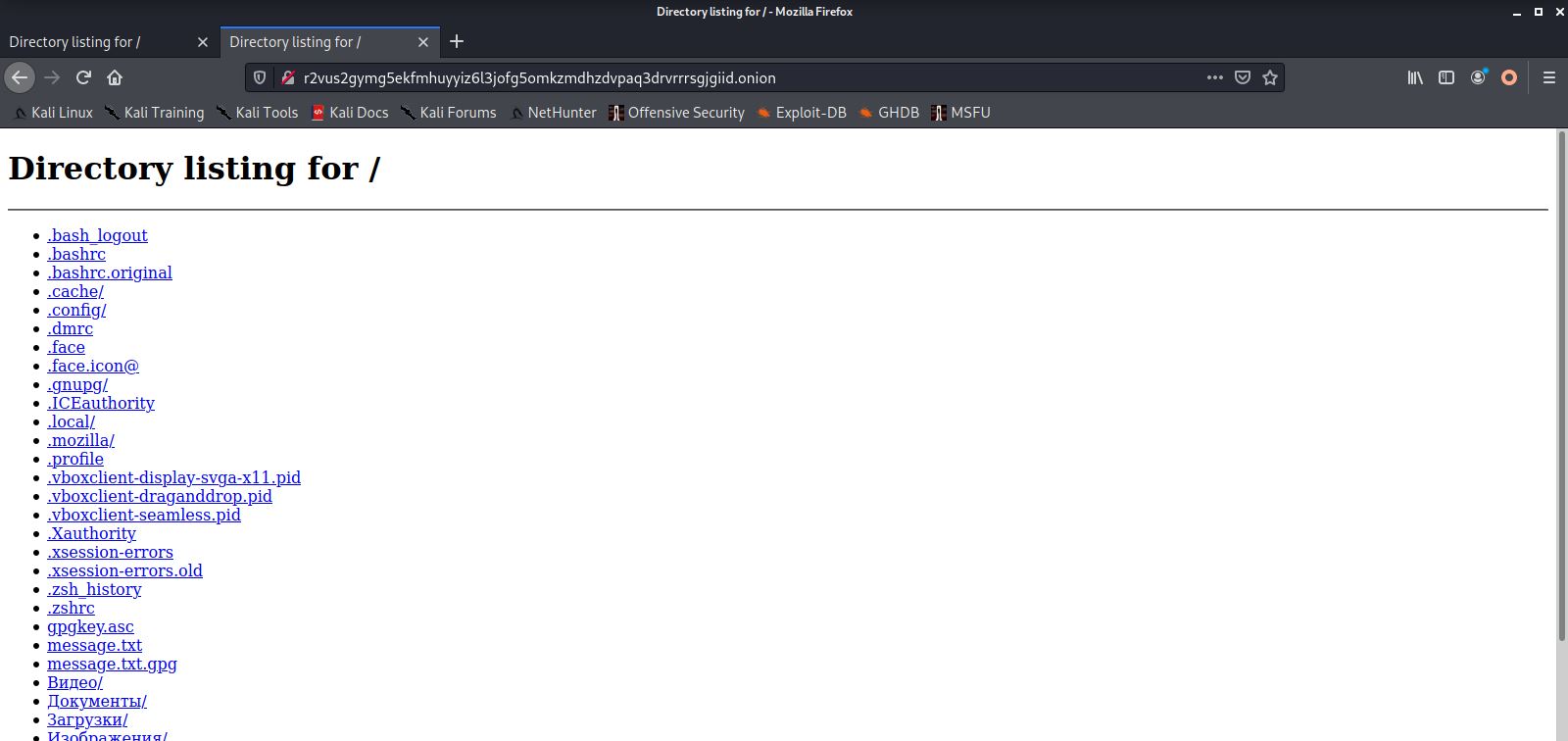
Чтобы перейти в директорию /var/lib/tor/hidden\_service, где содержится сгенерированный .onion-адрес, я ввёл команду # cd /var/lib/tor/hidden\_service. Чтобы убедиться, что в этой директории находятся файлы hostname и secret\_key, я ввёл команду # ls var/lib//tor/hidden\_service:



Чтобы получить сгенерированный .onion-адрес, я ввёл команду # cat hostname /var/lib/tor/hidden\_service:

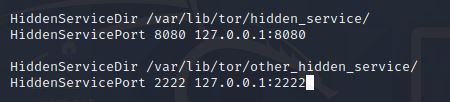


Я скопировал .onion-адрес созданного сервера из командной строки и перешёл на него в браузере:

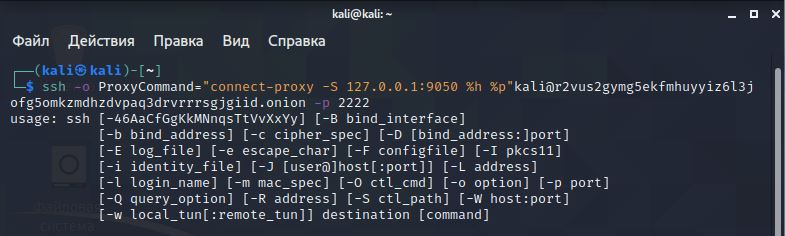


1. Подключение к SSH-серверу

Я открыл конфигурационный файл torrc с помощью команды # sudo nano /etc/tor/torrc, расскоментировал и модифицировал следующие строки:

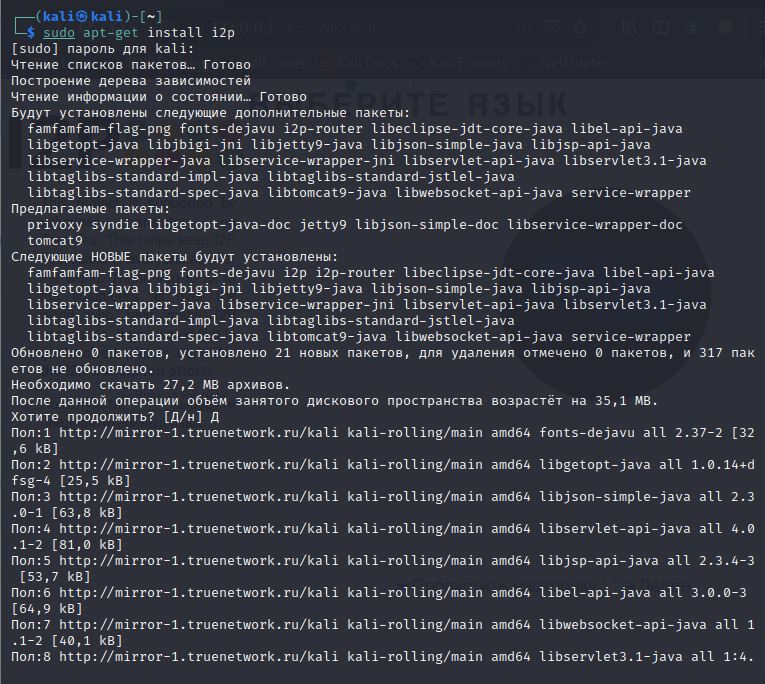


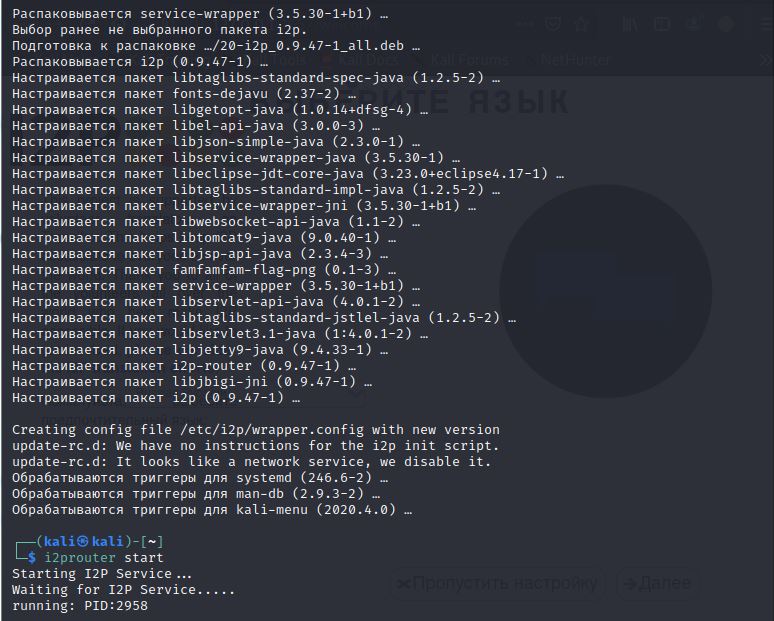
После чего перезапустил сервис с помощью команды # system restart tor и отобразил значение .onion из директории other\_hidden\_service, введя команду # cat hostname /var/lib/tor/other\_hidden\_service. После я модифицировал файл proxychains4. Далее я установил утилиту connect-proxy с помощью команды $ sudo apt-get install connect-proxy и произвёл подключение к ssh-серверу:

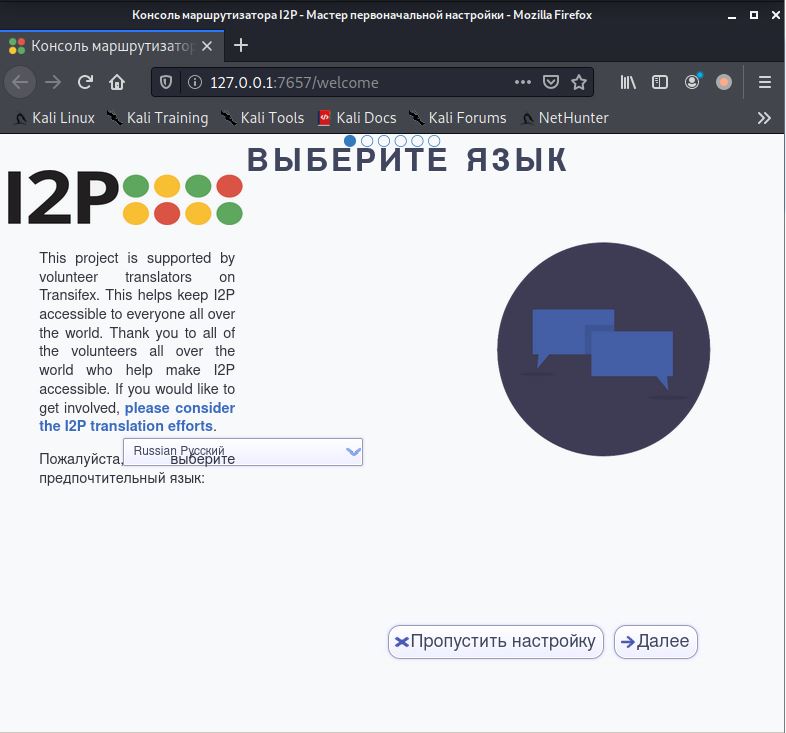


1. I2P

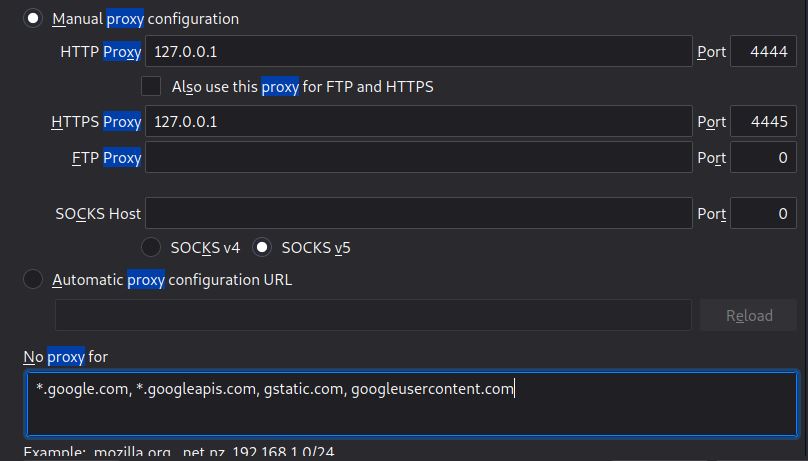
Для установки пакета i2p я ввёл команду $ sudo apt-get install i2p, а затем $ i2prouter start:



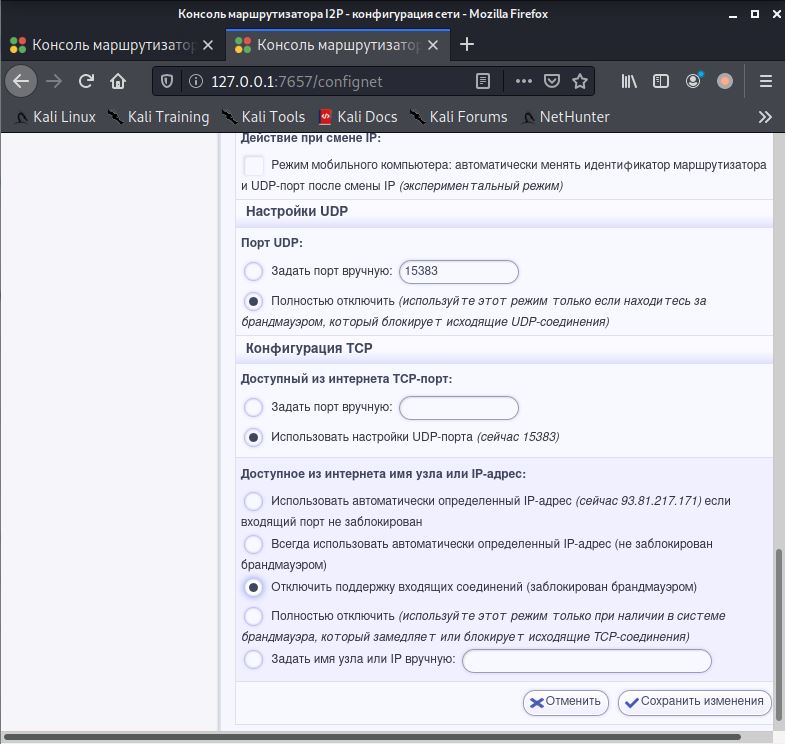


После чего у меня открылось окно браузера:

После первичной настройки сервиса я перешёл на консоль маршрутизатора I2P. Далее я зашёл в настройки браузера для того, чтобы настроить прокси-сервера следующим образом:

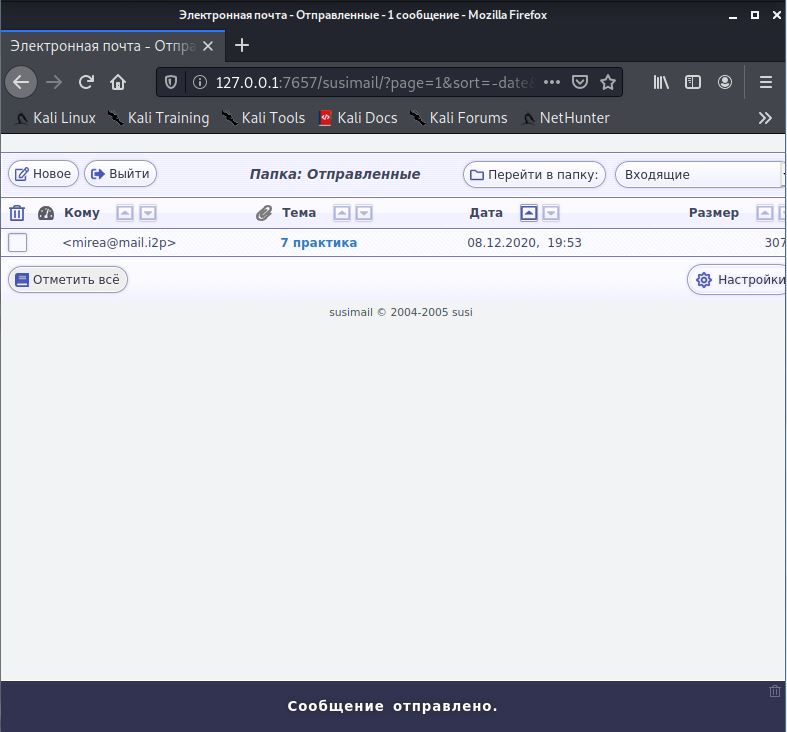


Далее я перешёл в сетевые настройки по адресу, указанному в методическом материале, и настроил следующим образом:



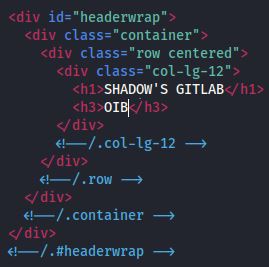
1. Электронная почта i2p

Письмо пришло Вам на почту [mirea@mail.i2p](mailto:mirea@mail.i2p) с почтового ящика [mrpotemkin@mail.i2p](mailto:mrpotemkin@mail.i2p):

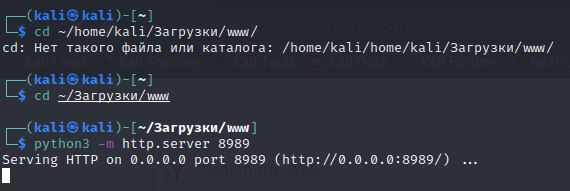


1. Размещение сайта

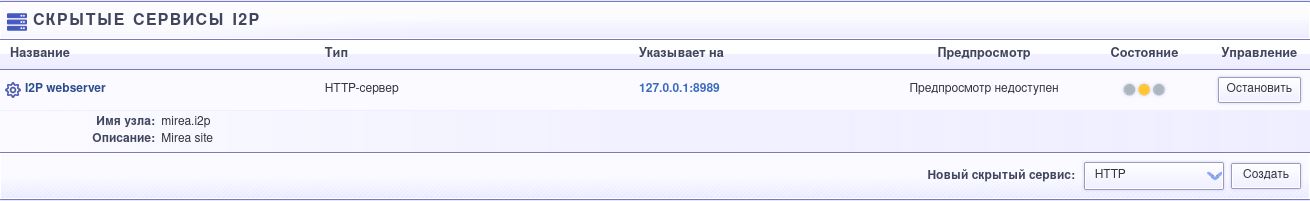
Я скачал пример сайта и разархивировал его в ~/Загрузки/www. Открыл файл index.html в браузере и его же как текстовый документ. Изменил 2 строчки на свои и сохранил файл:



После этого я запустил веб-сервер, предоставляемый вместе с python, с помощью команды $ python3 –m http.server 8989:



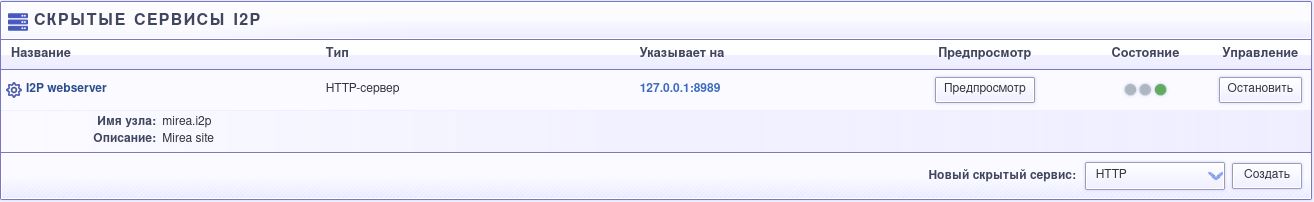
Далее из консоли маршрутизатора i2p я перешёл в меню “Управление скрытыми серверами” , настроил сервер согласно методическому материалу и запустил его:



Для проверки работоспособности скрытого сервиса я установил программу I2P Browser | Dark Web, указал локальный адрес назначения и нажал на него после создания записи:



Статус скрытого сервиса стал активным:



А в телефоне открылась страница сайта спустя несколько минут. Изменения в тех 2 строчках в файле index.html так же отобразились:

