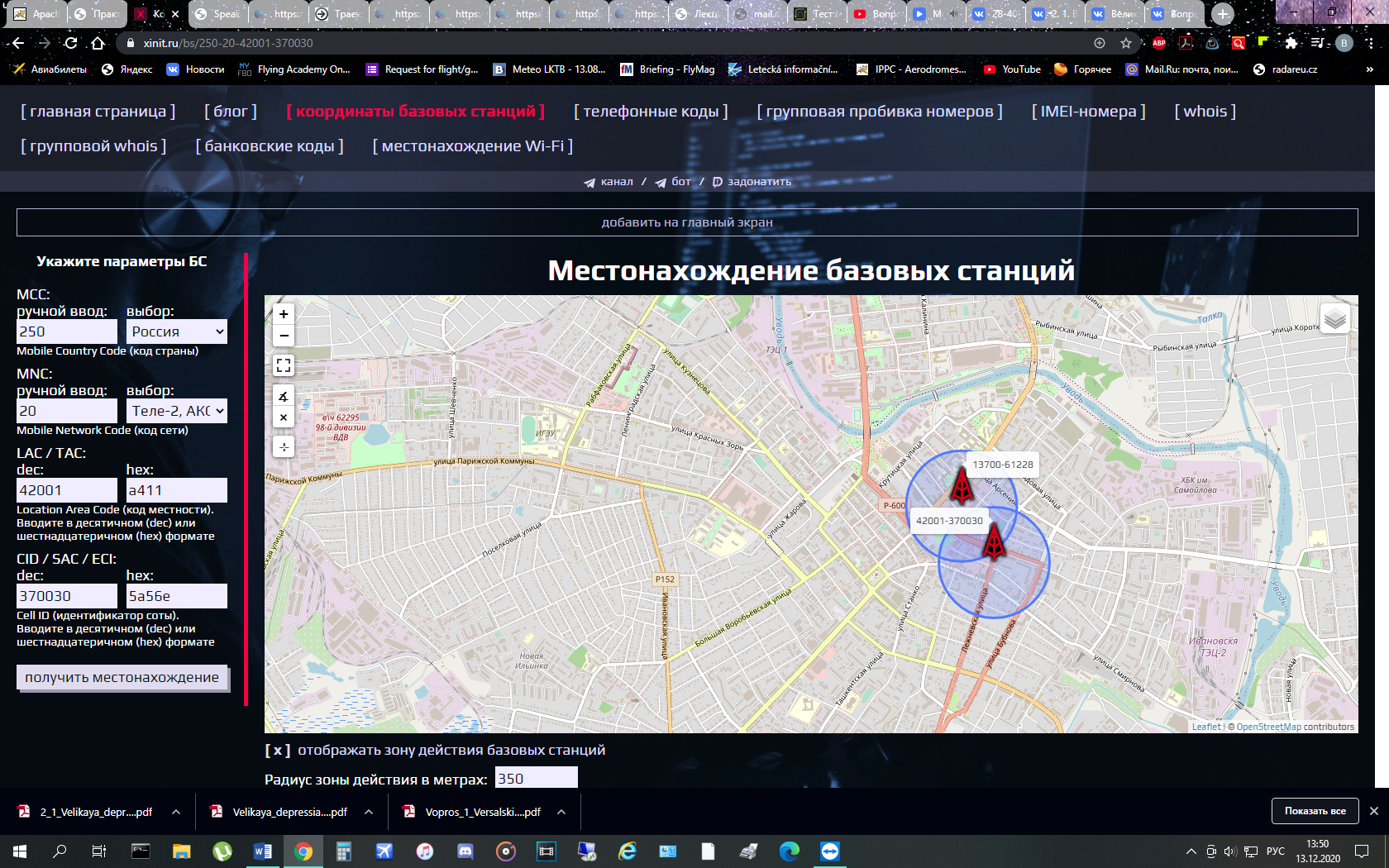
7 практика

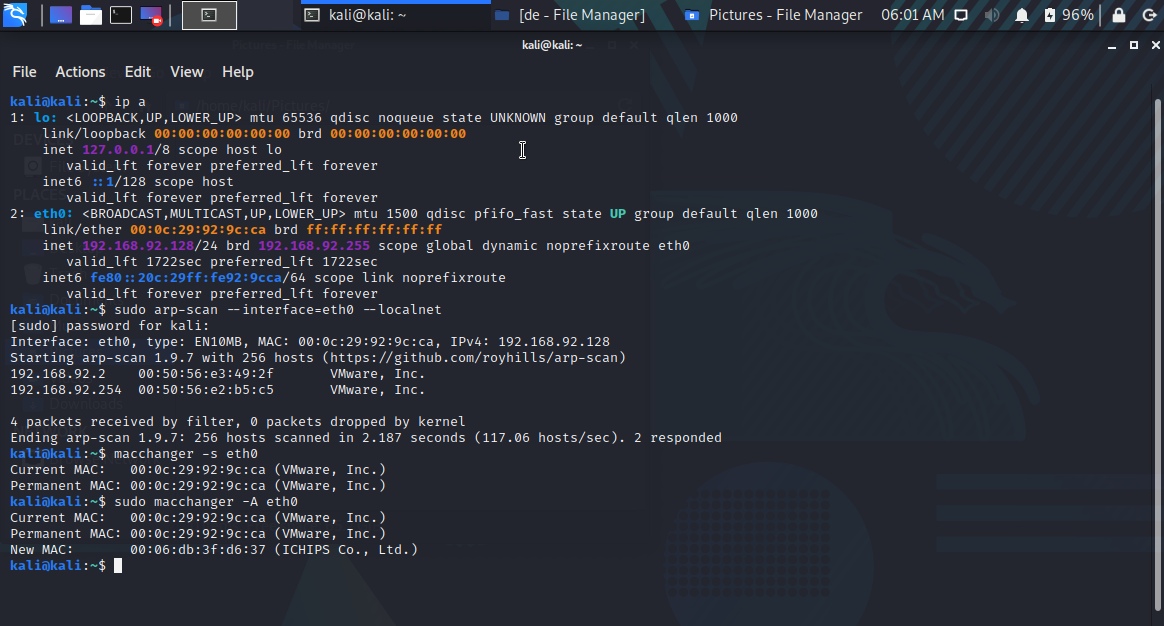
1. Установили приложения для получения данных о подключении:



Данные приложения позволяют извлечь идентификаторы базовых станций (БС), требующиеся для обнаружения местоположения станций:

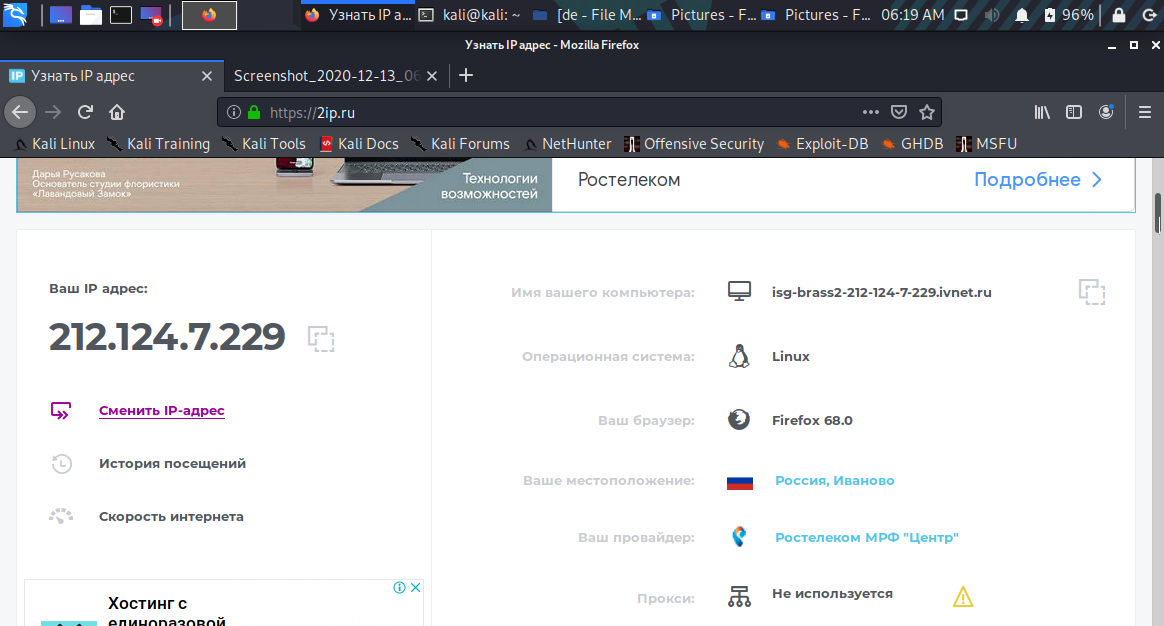
1. MAC – адрес

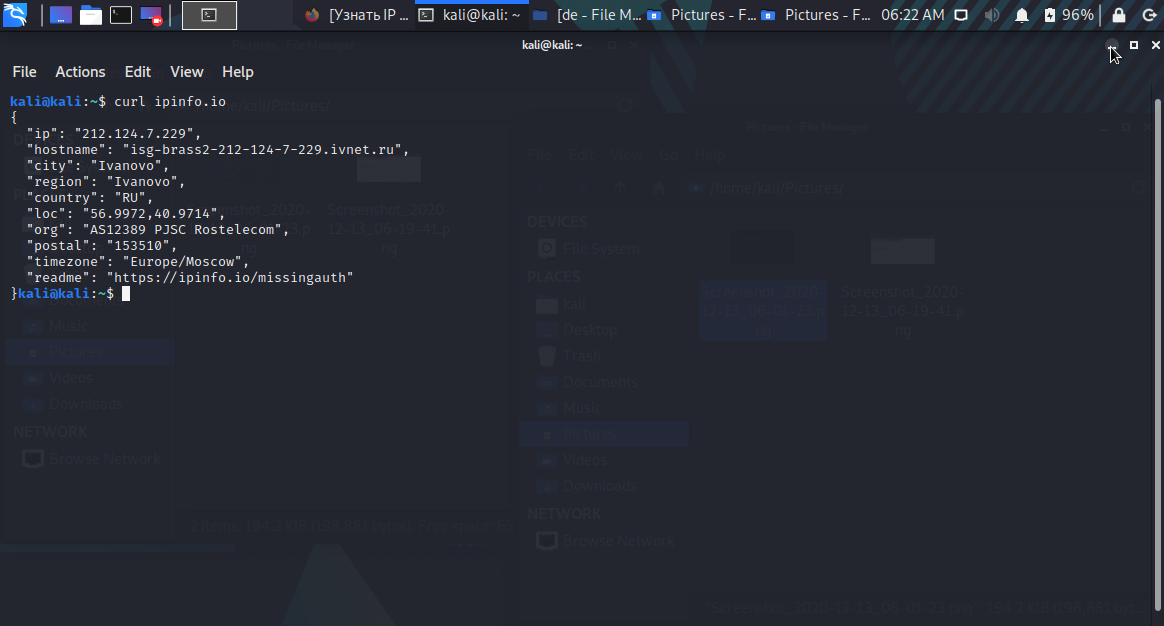
Определили свой mac-адрес и определили производителя по нему, а затем поменяли его и посмотрели новое значение:



1. IP – адрес

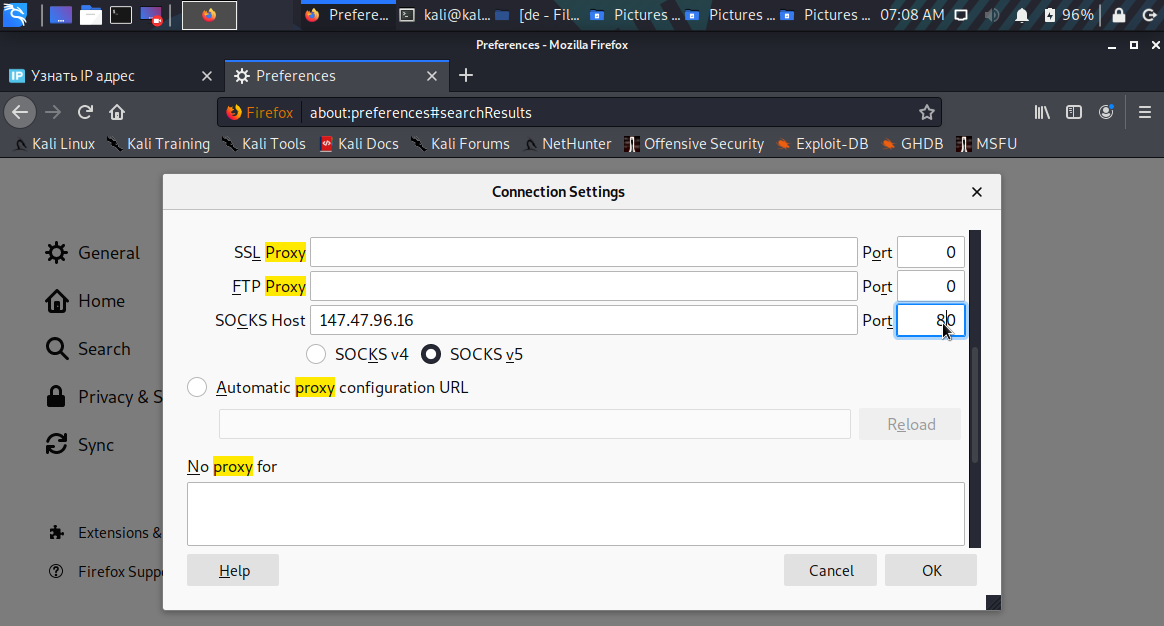
Для определения выходного ip – адреса я воспользовалась онлайн сервисом <https://2ip.ru>

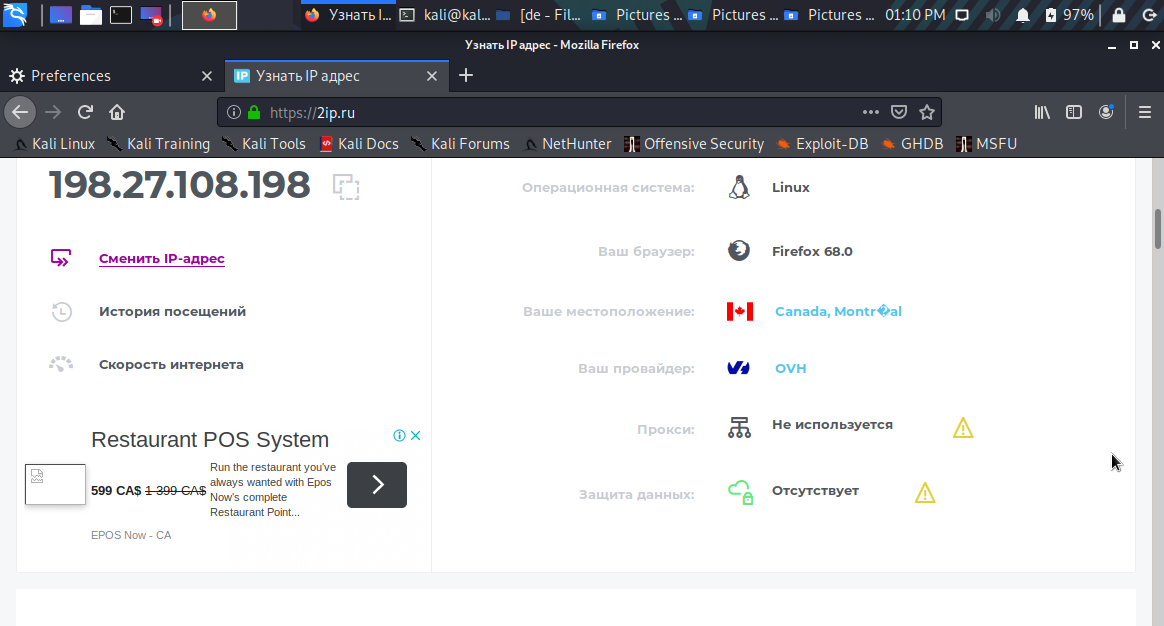


А также с помощью команды curl ipinfo.io

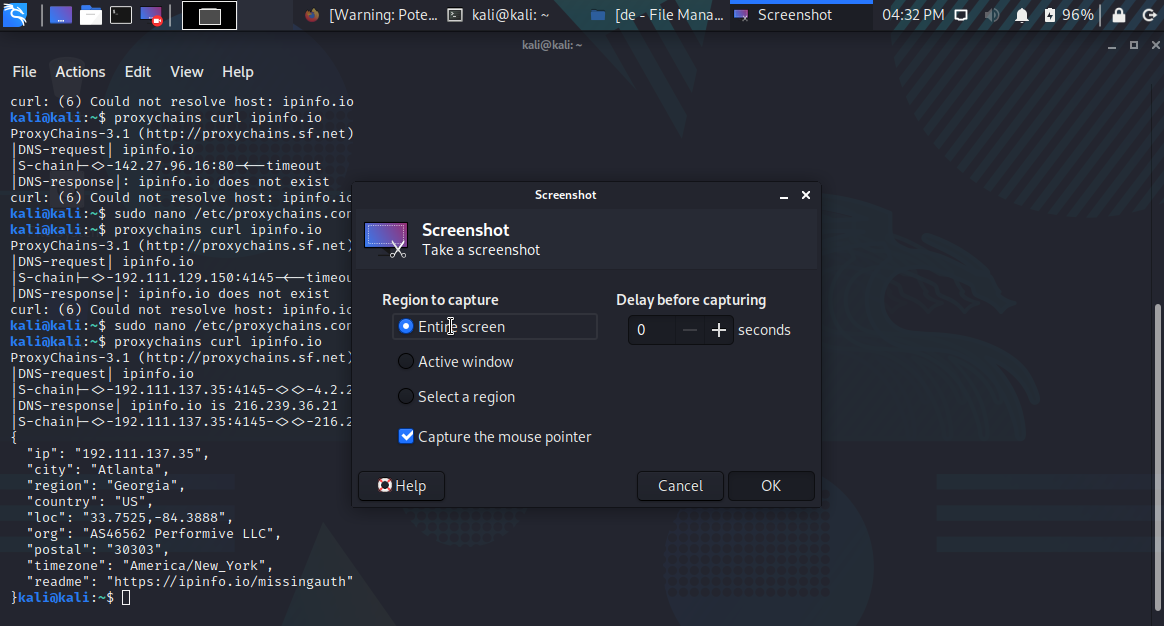
1. Socks прокси

На сайте http://free-proxy.cz/ru/ нашла работоспособный proxy и отобразила информацию о выходном ip.



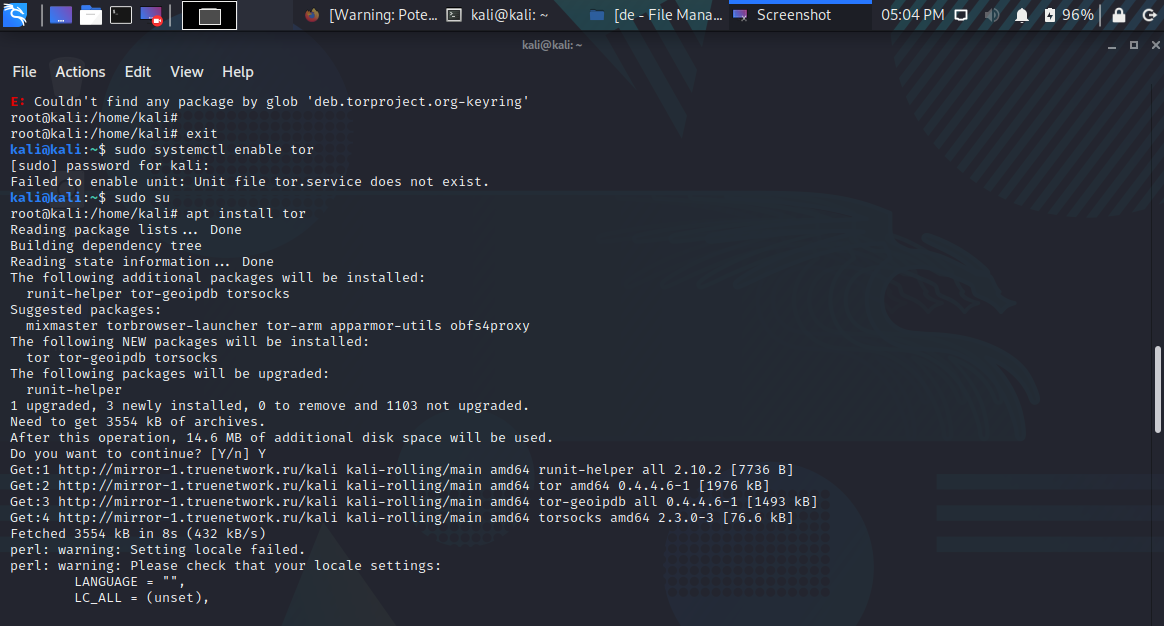


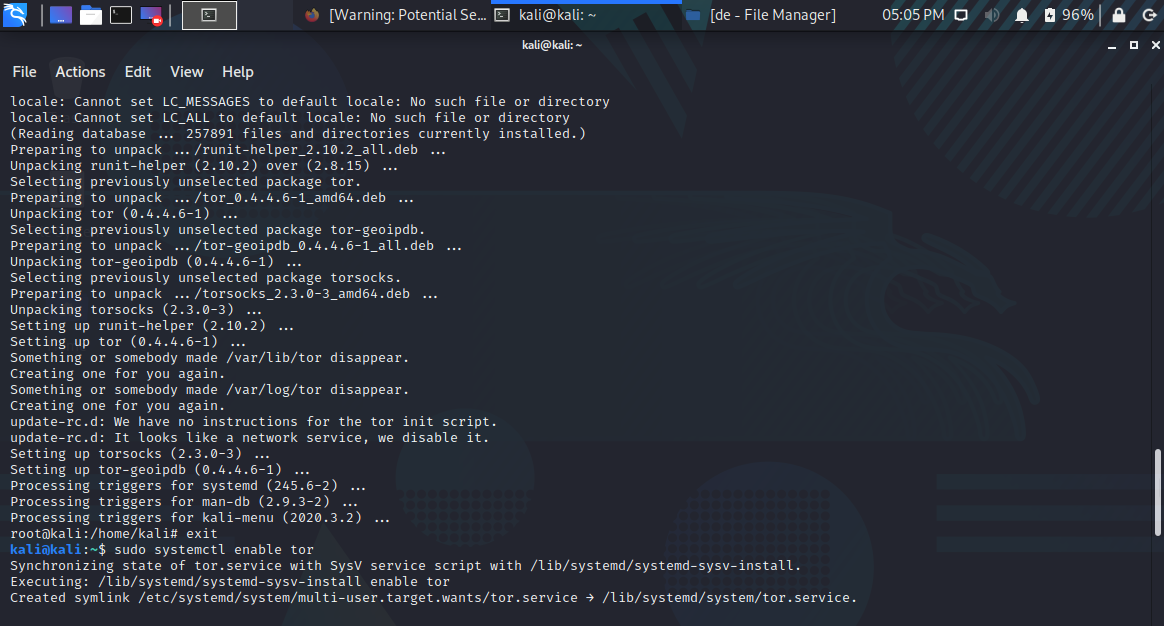
Как оказалось, вышла небольшая накладка, но информацию видно четко

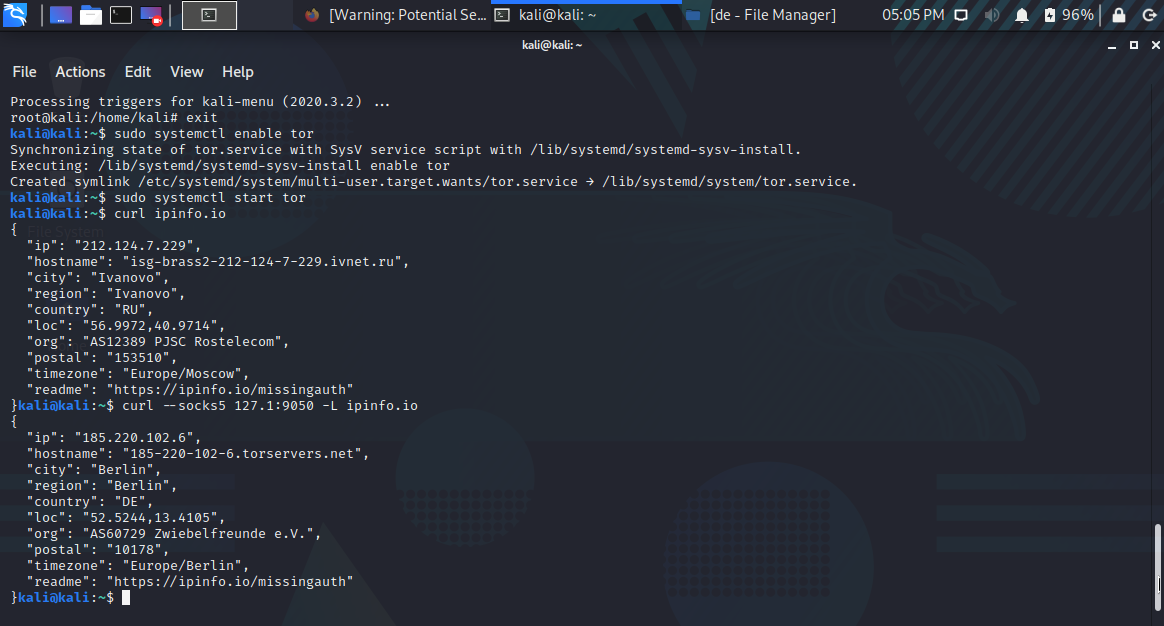


1. Установка TOR и Проверка работоспособности tor

Установила tor из репозиториев Ubuntu

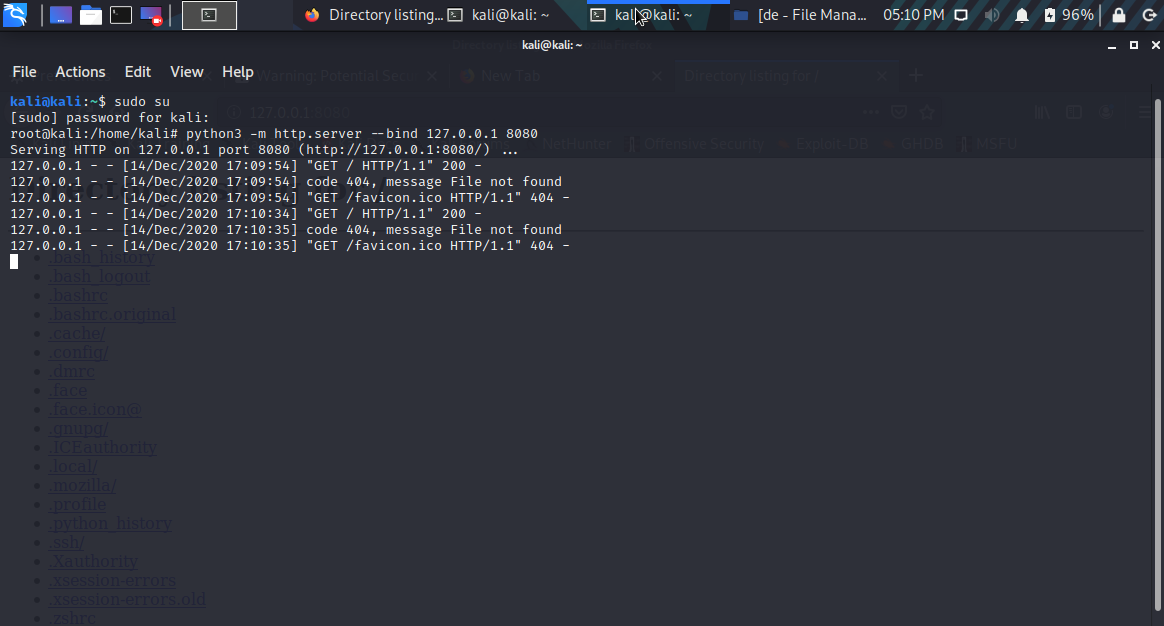




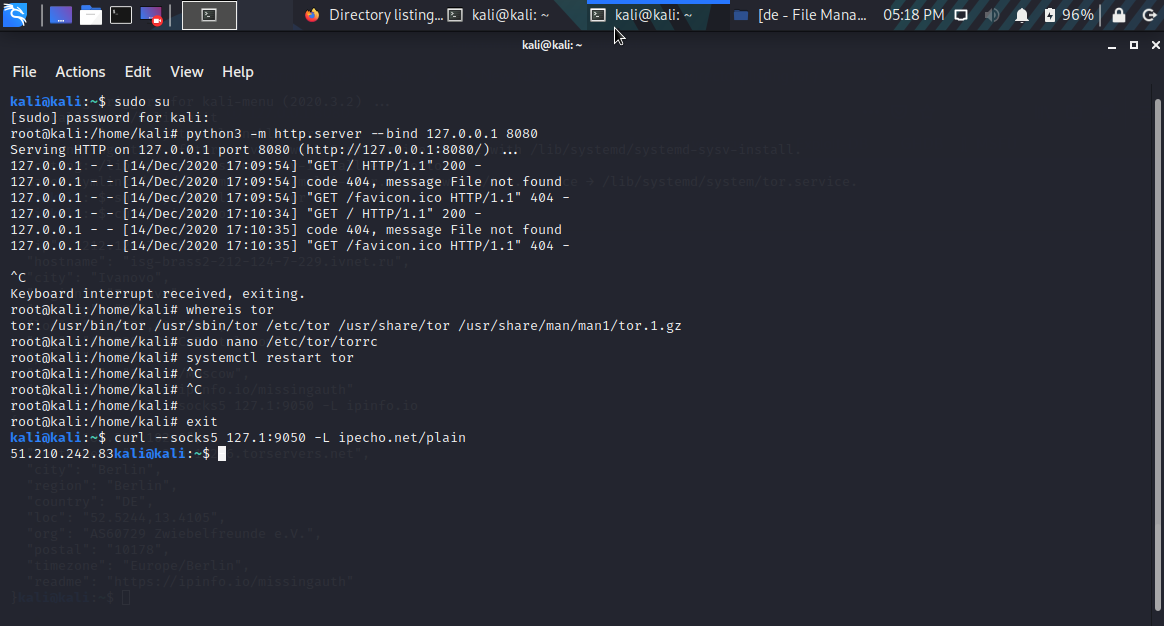
Запустили и добавили службы Tor в автозагрузку, также проверили запуск и соединения с tor сетью

1. Настройка HiddenService для WEB – сервера

Проверили работоспособность работы tor

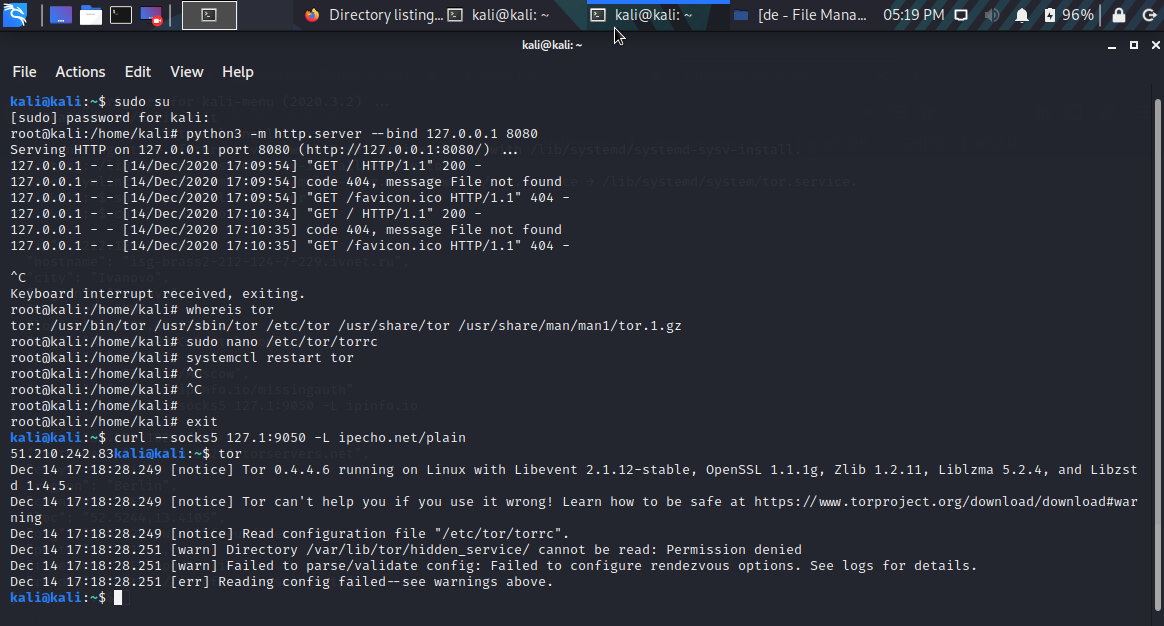


В браузере открыли данную страницу и убедились в работоспособности сервера (к сожалению, в ходе работы был утерян этот скриншот)

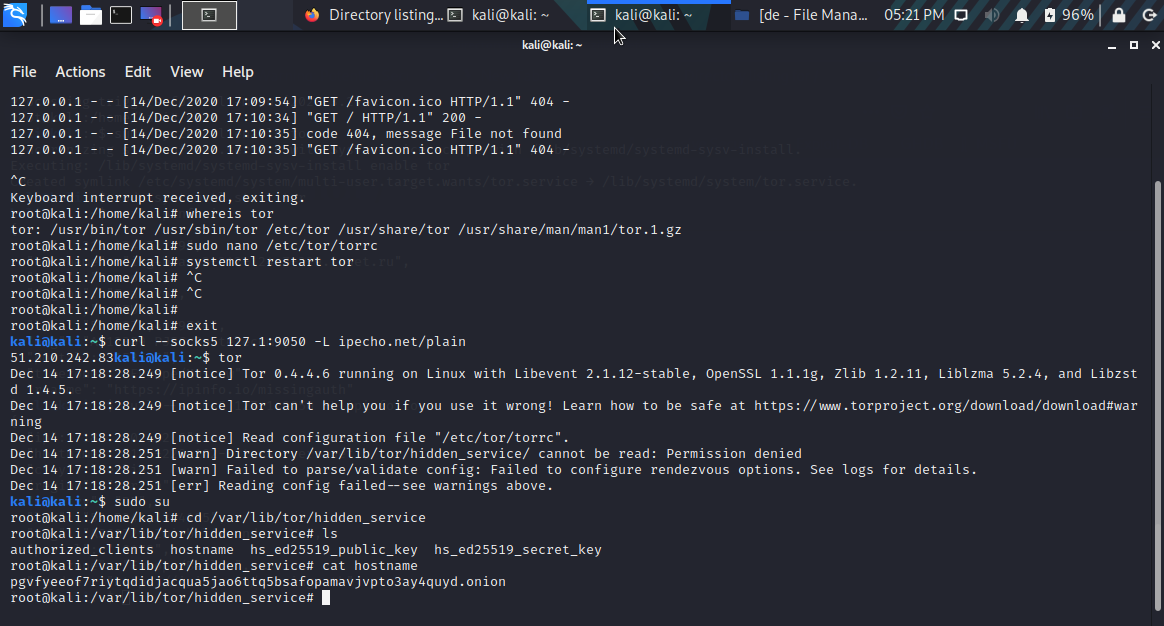
Далее произвели настройку tor и узнали место, в которое был установлен Tor

Нашли конфигурационный файл torrc и изменили его. Для проверки работоспособности tor т произвела повторный запрос через прокси. Произвели запуск tor от имени пользователя

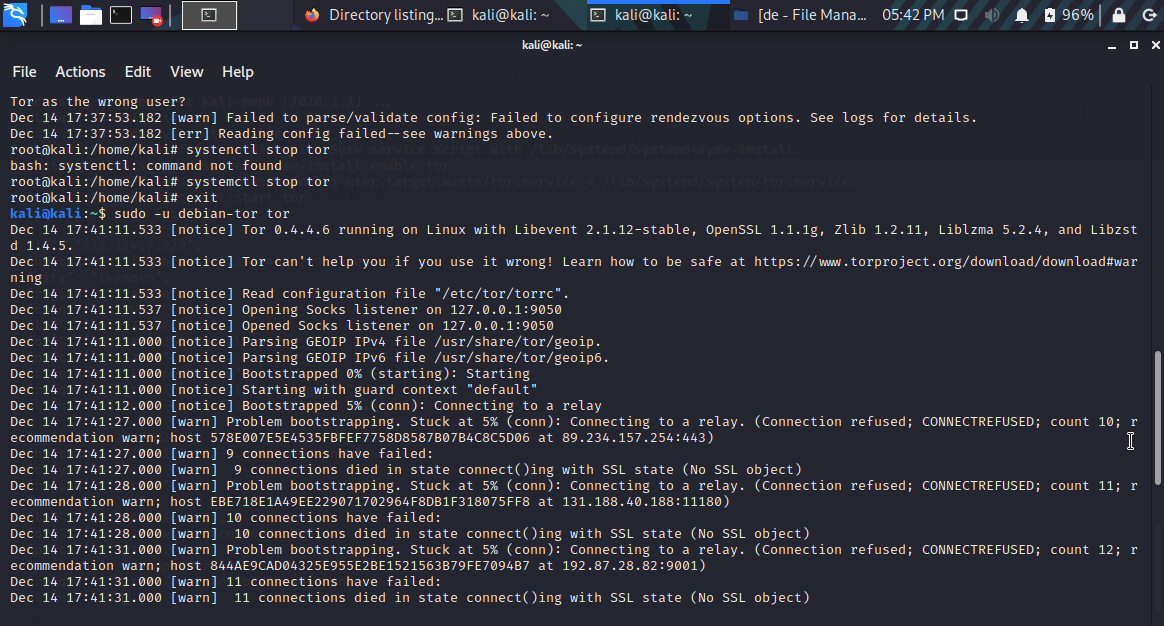
(но тут я поняла, что что-то идет не так, и потом запускала уже тор с помощью команды sudo –u debian-tor tor)

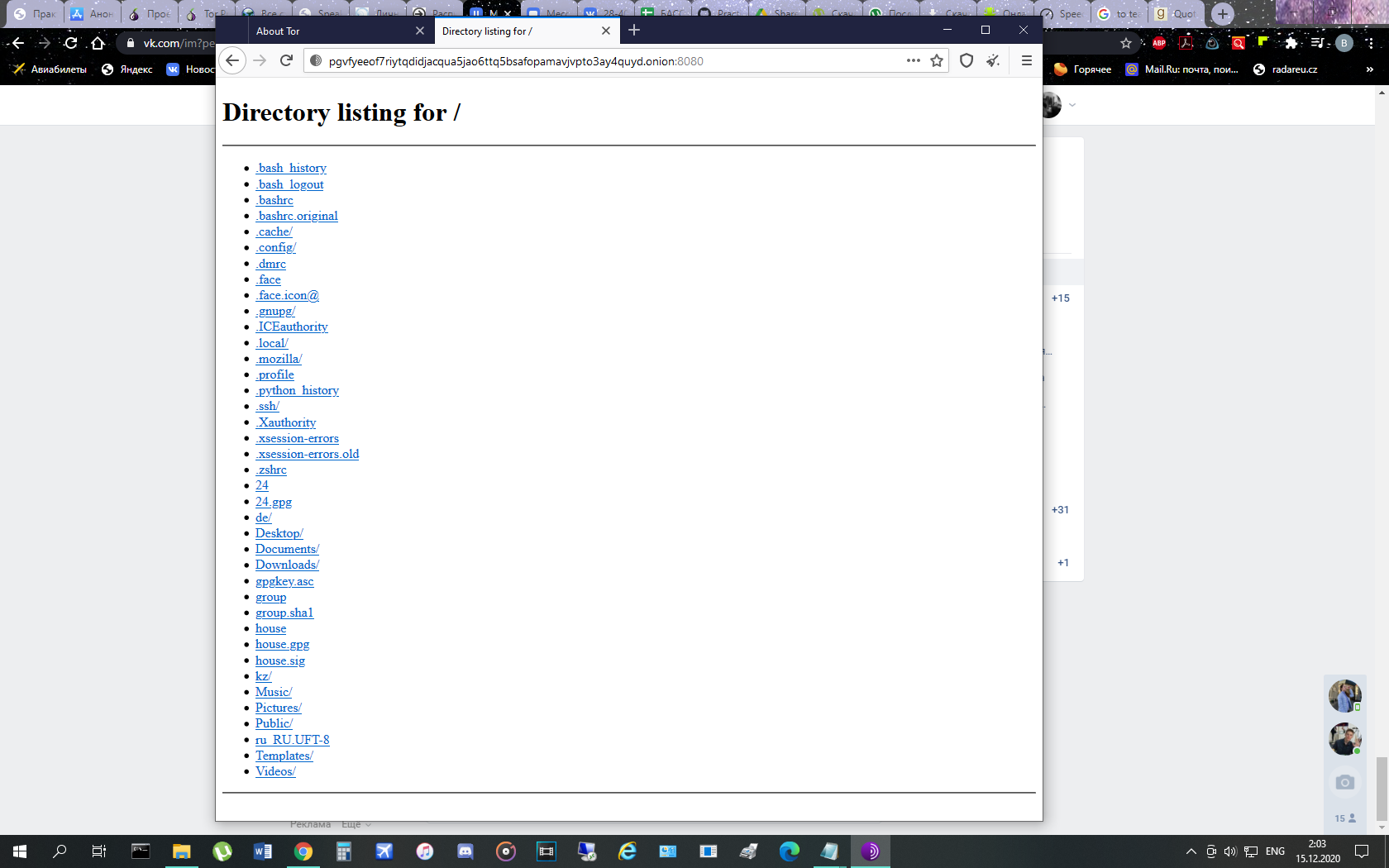


При запуске Tor с новой конфигурацией автоматически сгенерирован «.onion-адрес». Эта информация храниться в «/var/lib/tor/hidden\_service»



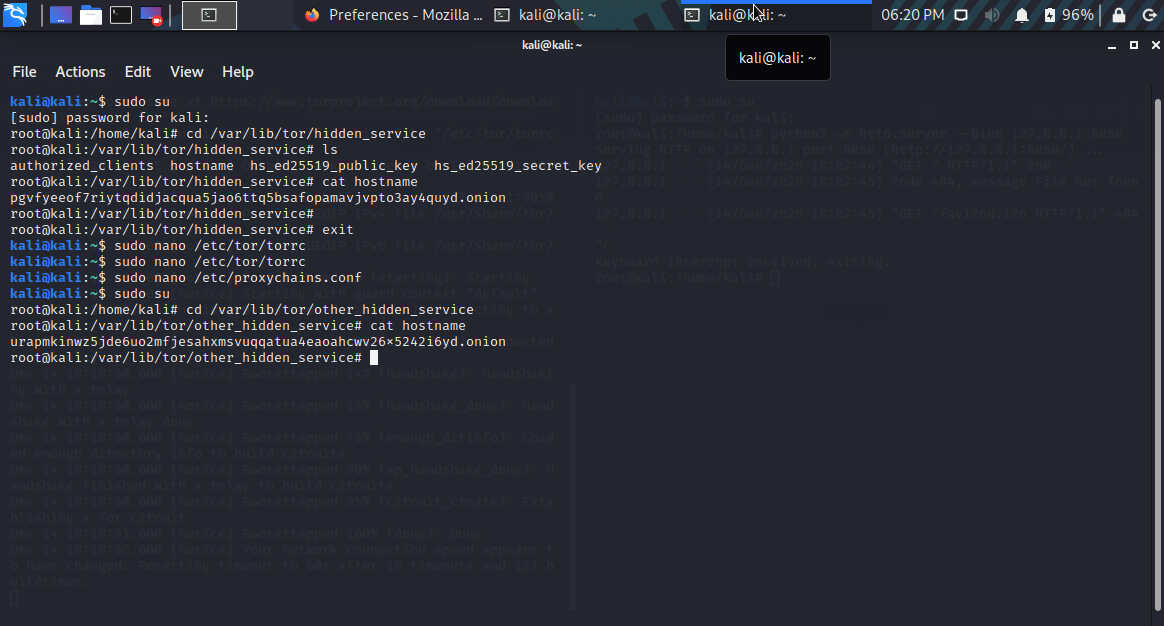
остановила предыдущие попытки захода в тор и заново его запустила

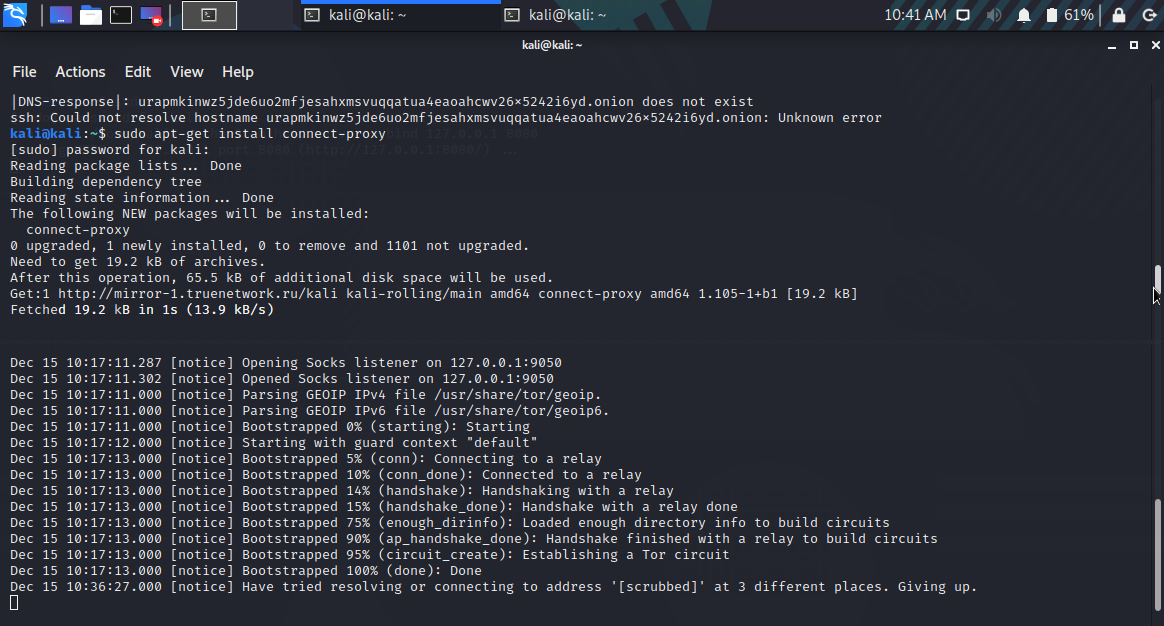


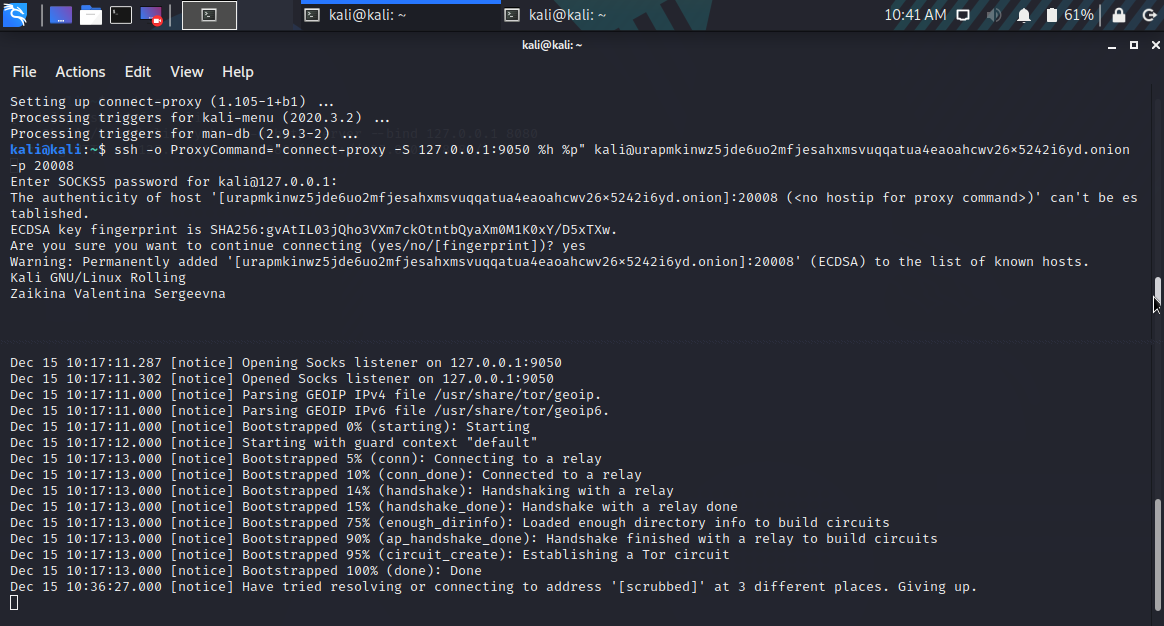
И после перешла на созданный сайт через тор-браузер

1. SSH – сервер

Нашла конфигурационный файл torrc и модифицировала его, после отобразила значение «.onion» из директории «other\_hidden\_service», а также изменила конфигурационный файл proxychains (но этот момент был утерян)

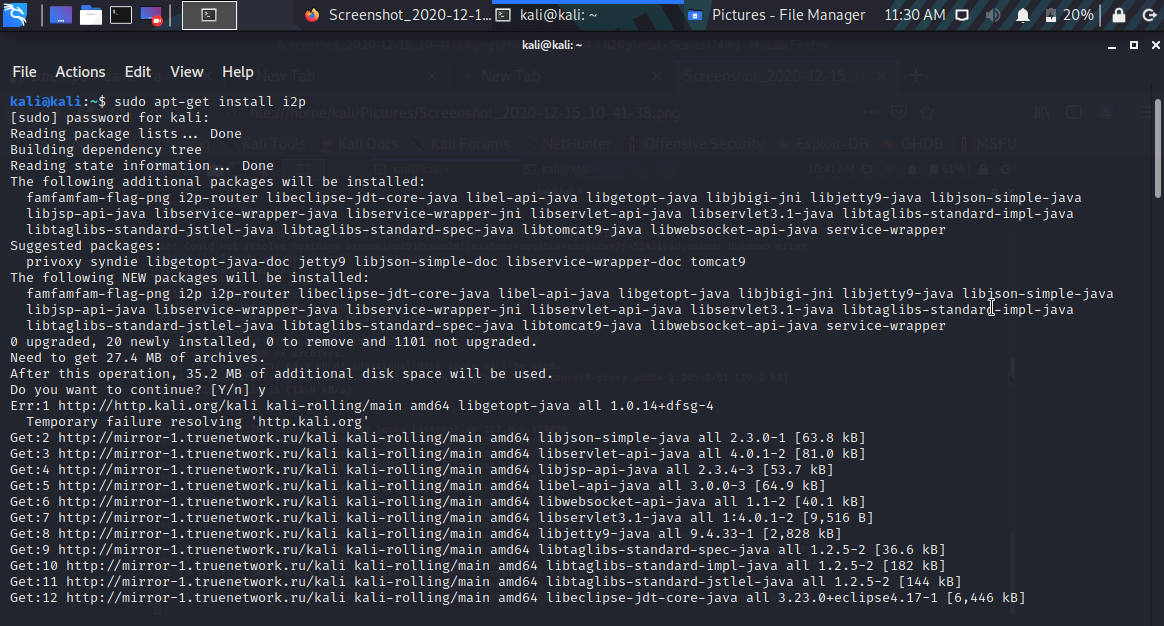


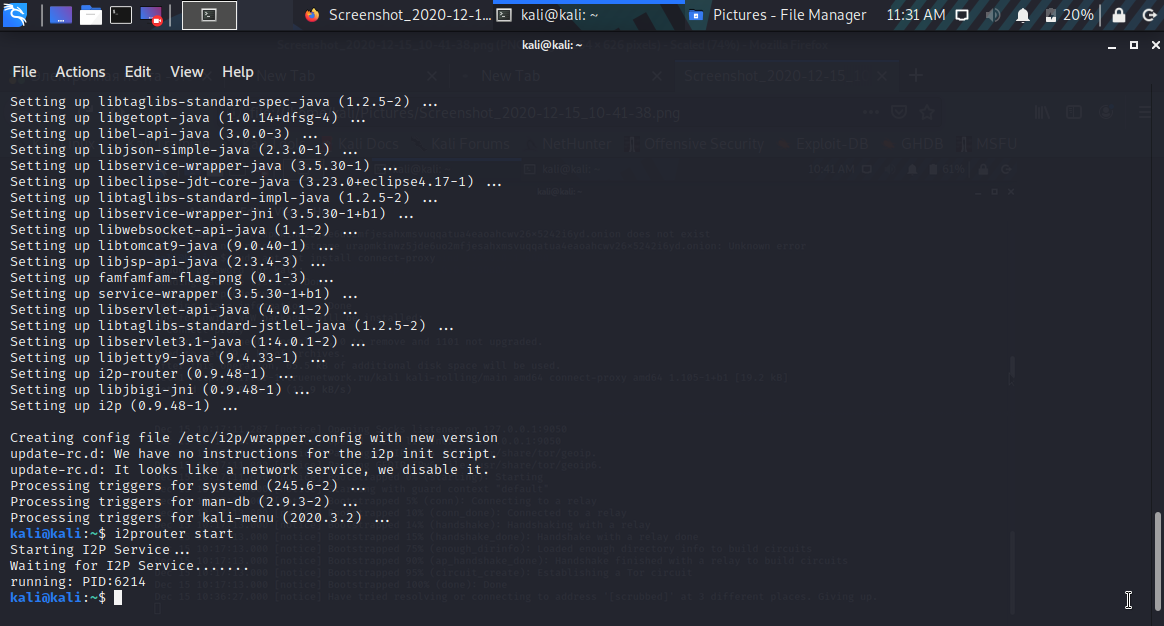
Также с помощью использованием утилиты «connect-proxy» произвела подключение к ssh серверу (но так как в этот момент я разделила терминал на две части и я не досмотрела на скриншоте показано не все)

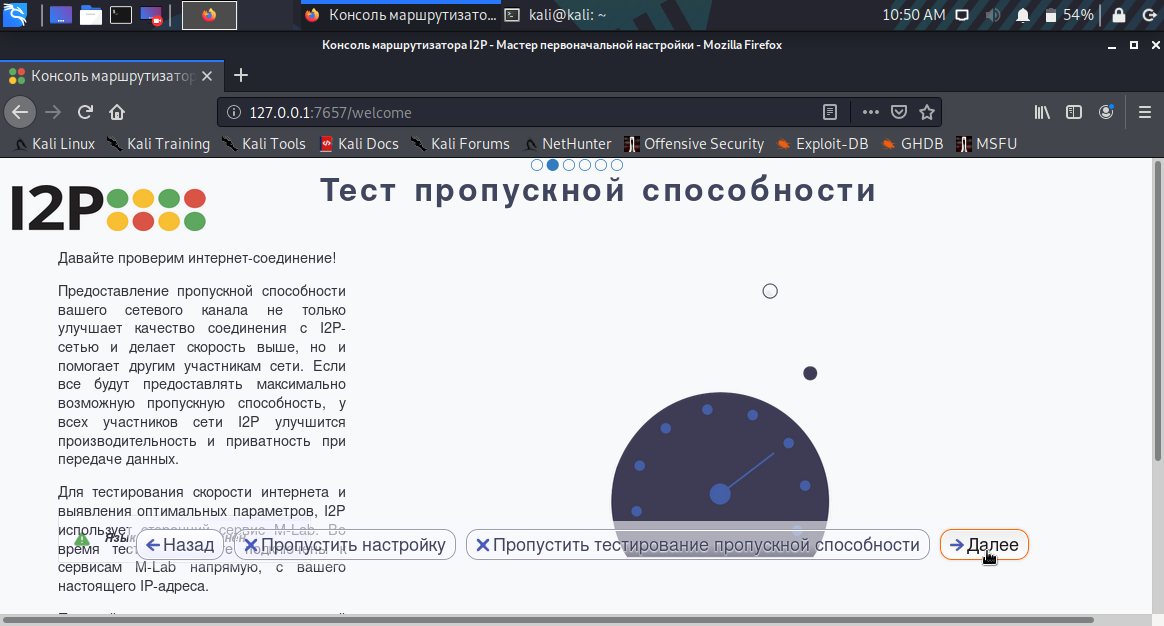


1. I2P установка

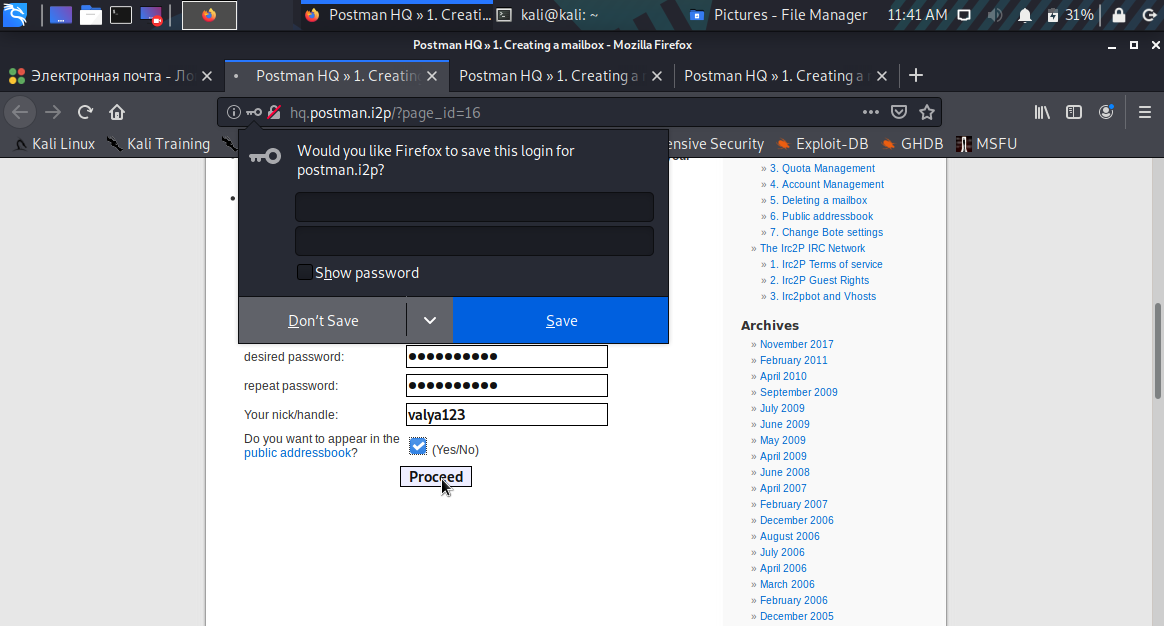
Установила пакет i2p, затем произвела запуск программного роутера для подключения к сети I2P.

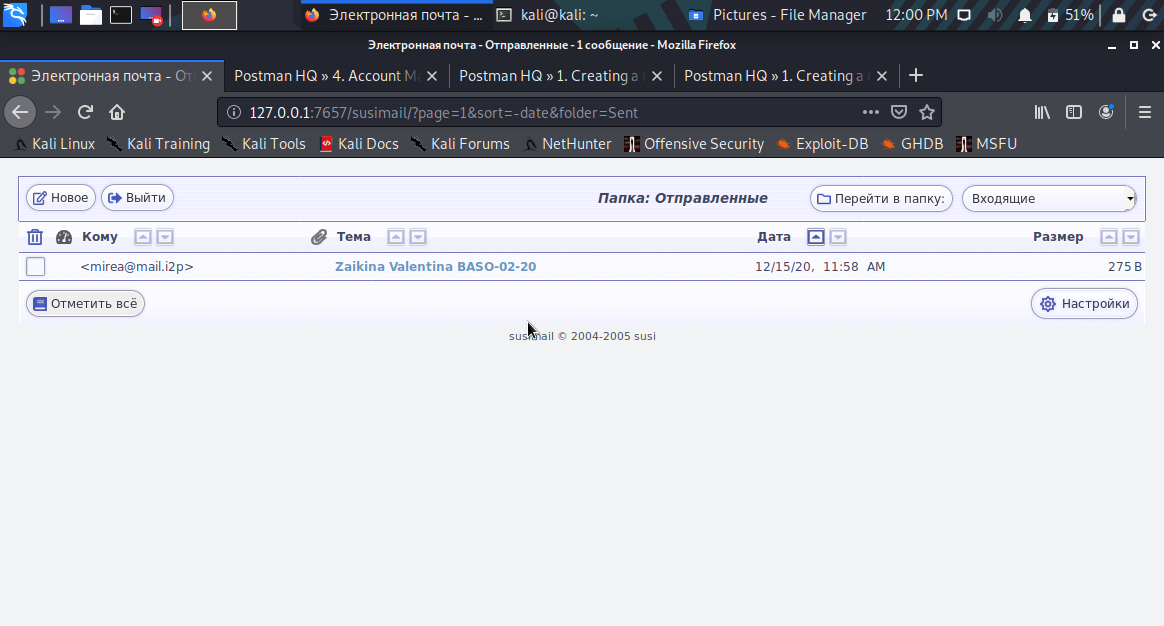






После этого произвела проверку доступности и пропускной способности соединения, а после перешла на консоль маршрутизатора I2P и произвела настройку прокси сервера у браузера. Далее перешла в сетевые настройки по адресу http://127.0.0.1:7657/confignet

1. Электронная почта

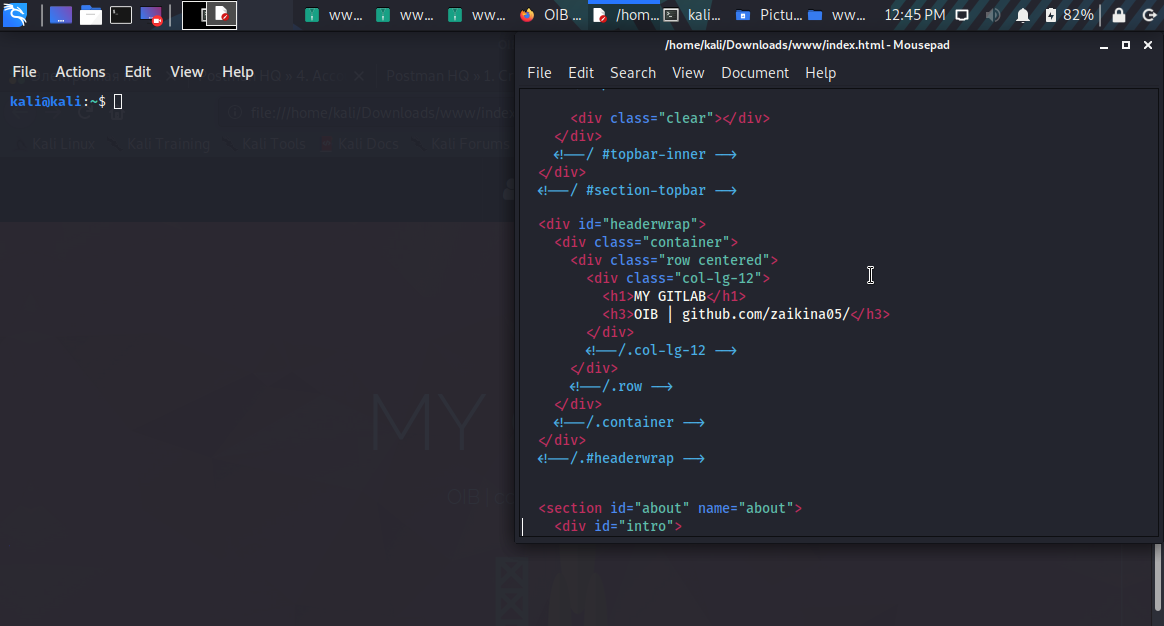


Создала аккаунт и произвела все необходимые настройки, после этого отправила письмо на указанный адрес.

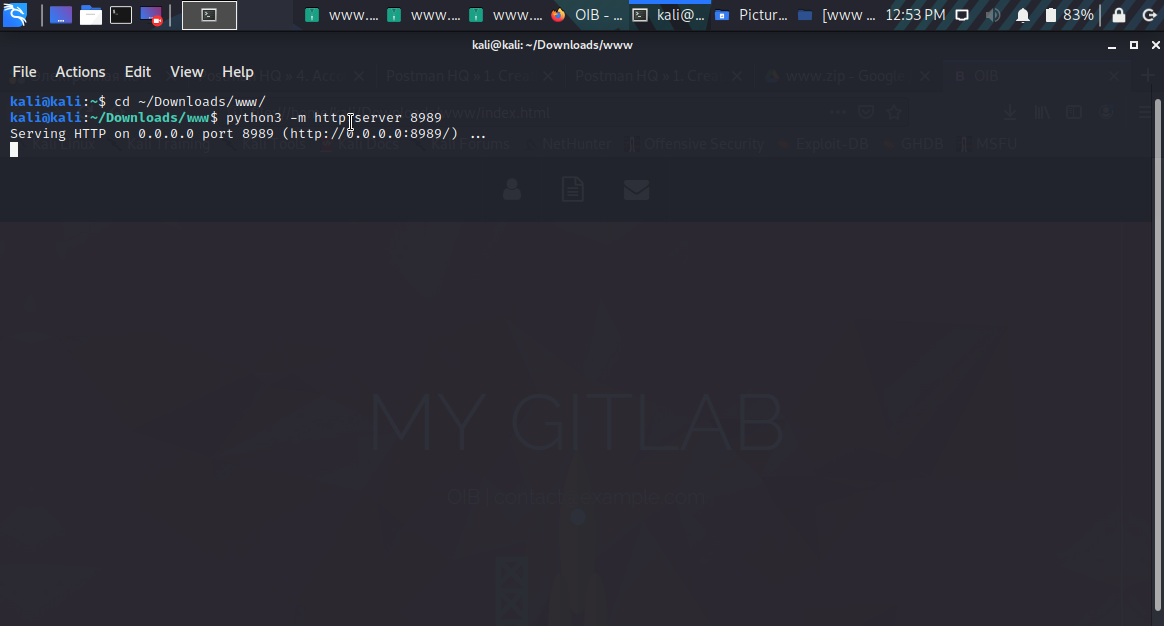
1. Размещение сайта

По ссылке (https://drive.google.com/file/d/1aqcVzTMEVzgopmTYUZSt8dSHqaoo\_JLe/view? usp=sharing) скачала и разархивировала файл в папку ~/Downloads. Открыла файл index.html в браузере



В данную страницу внесла необходимые данные:

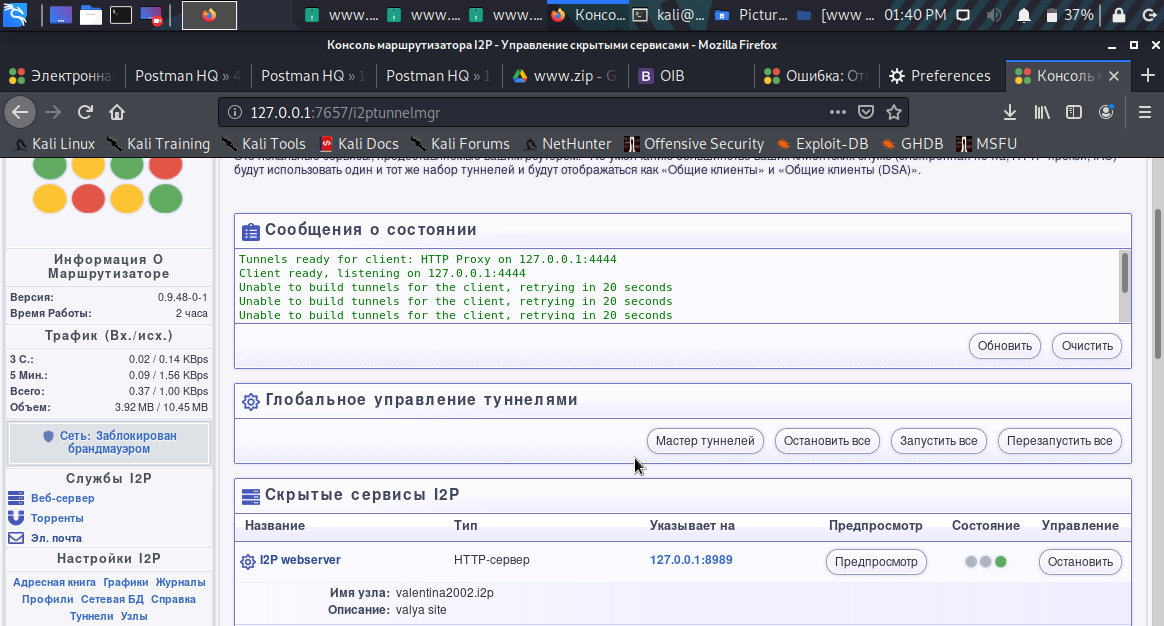
Открыла терминал и перешла в директорию, где располагается файл index.html. а также запустила веб-сервер



После выполненных действий открыла браузер перешла по адресу



Разместила сайт в сети i2p. Из консоли маршрутизатора i2p перешла в меню «Управление Скрытыми сервисами», произвела все необходимые настройки и запустила его.



Для проверки работоспособности скрытого сервиса я установила на мобильное устройство I2P клиент

