|  |  |  |
| --- | --- | --- |
|  |  |  |
| МИНОБРНАУКИ РОССИИ | | |
| Федеральное государственное бюджетное образовательное учреждение  высшего образования  **«МИРЭА – Российскийтехнологическийуниверситет»**  **РТУ МИРЭА** | | |
| **Институт комплексной безопасности и специального приборостроения** | | |
|  |  |  |

Кафедра КБ-3 «Управление и моделирование систем»

**Отчет**

по дисципилне «Основы Информационной Безопасности»

Выполнил:

Студент 2 курса

Группа БИСО-03-19

Хачатярн Евгенйи

Арутюнович

Москва, 2020

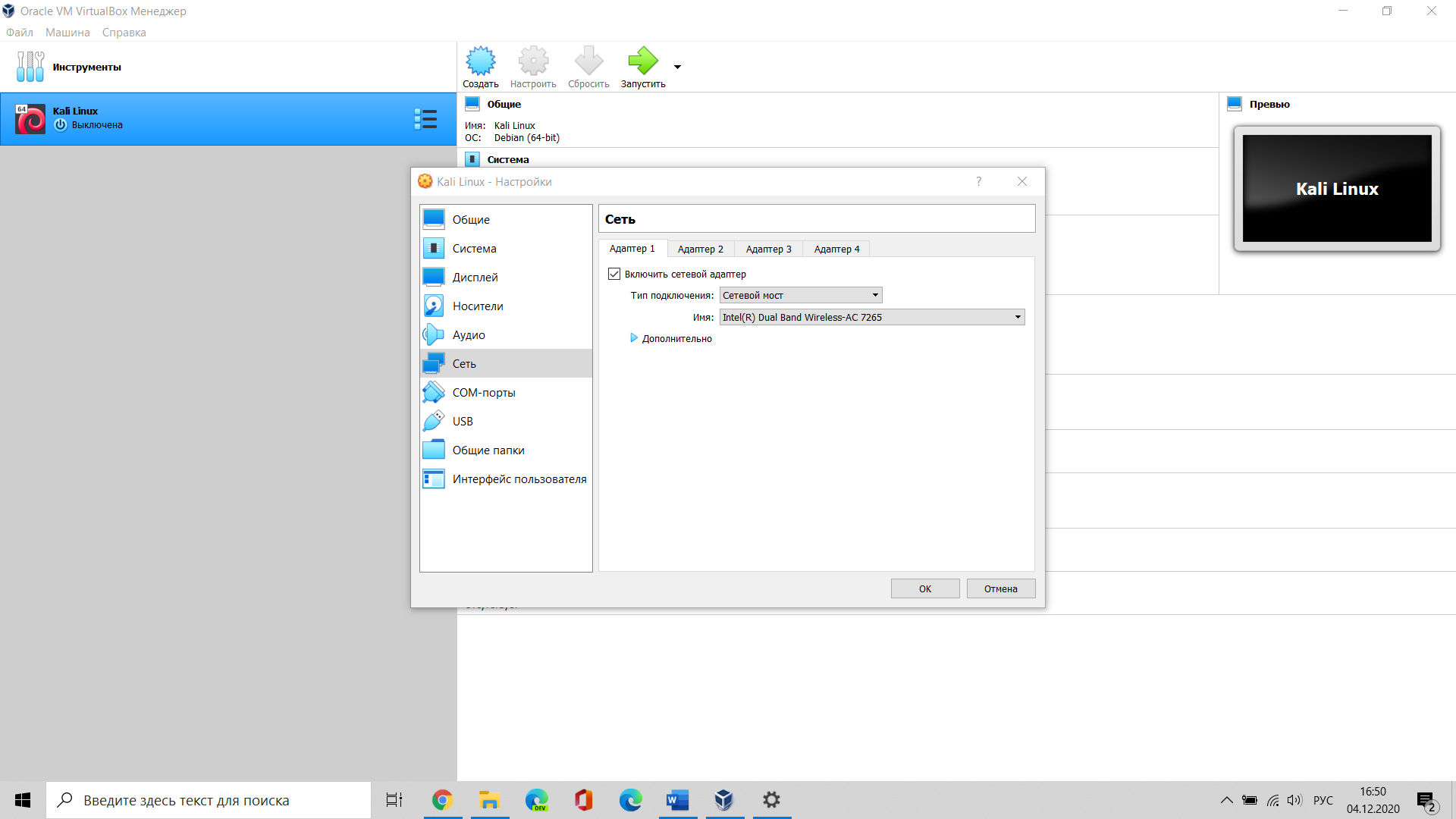
Мобильная сеть

Используя мобильное приложение FindTower, найдём идентификаторы базовых станций, а также местоположение на этих станций:

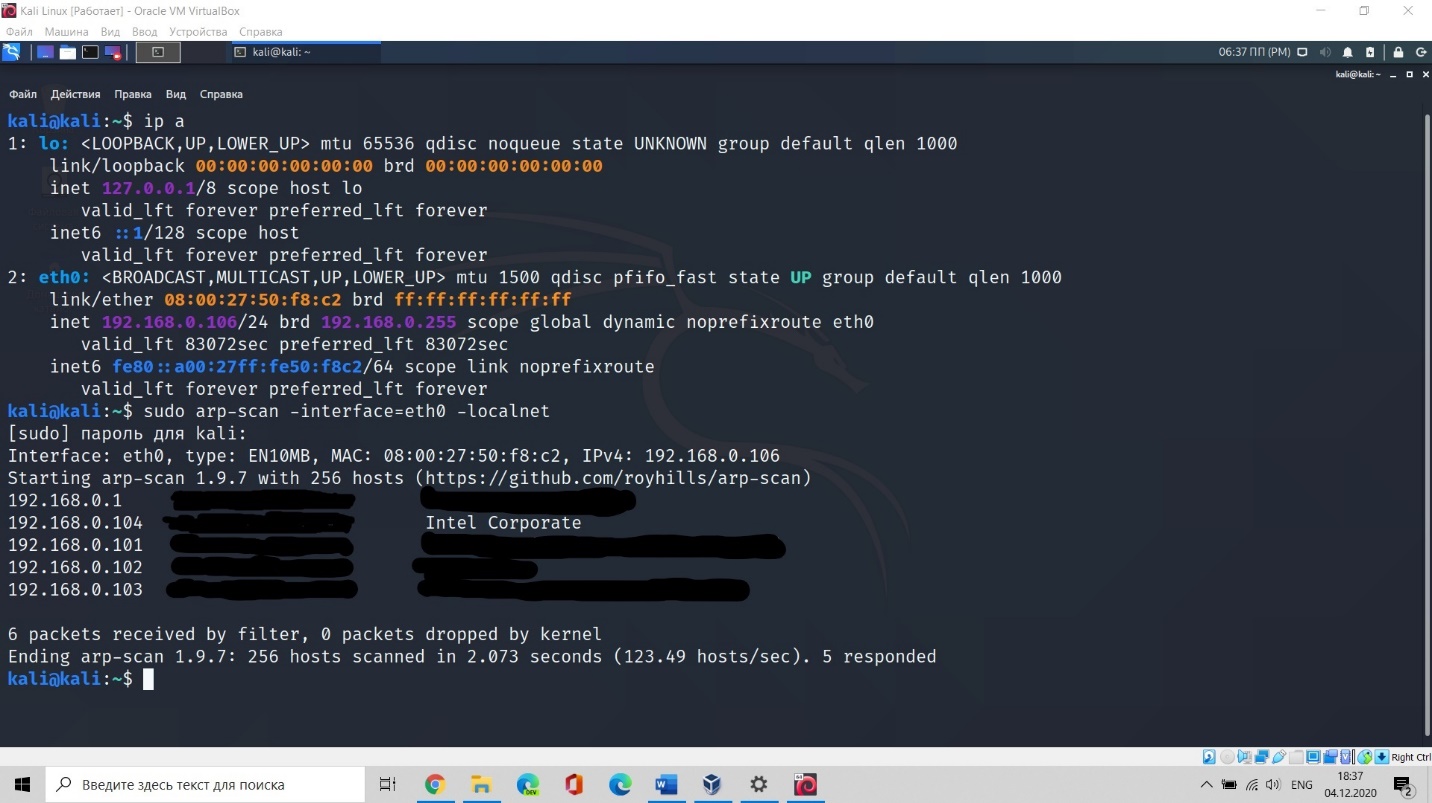


MAC – адрес

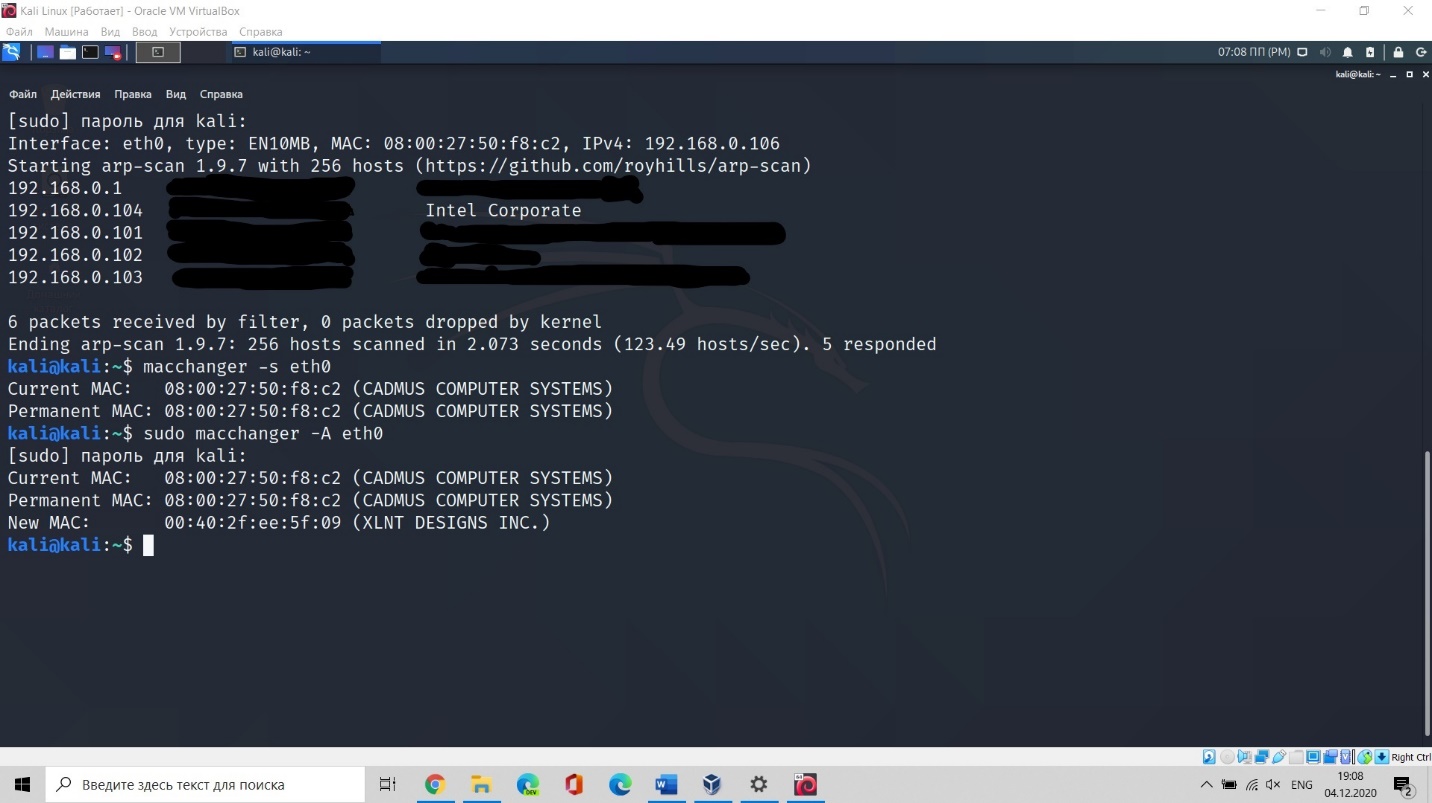
Переведём сетевые адаптеры у виртуальных ОС в режим “Мост/Bridge”.



Получим MAC – адрес сети и определим производителя:

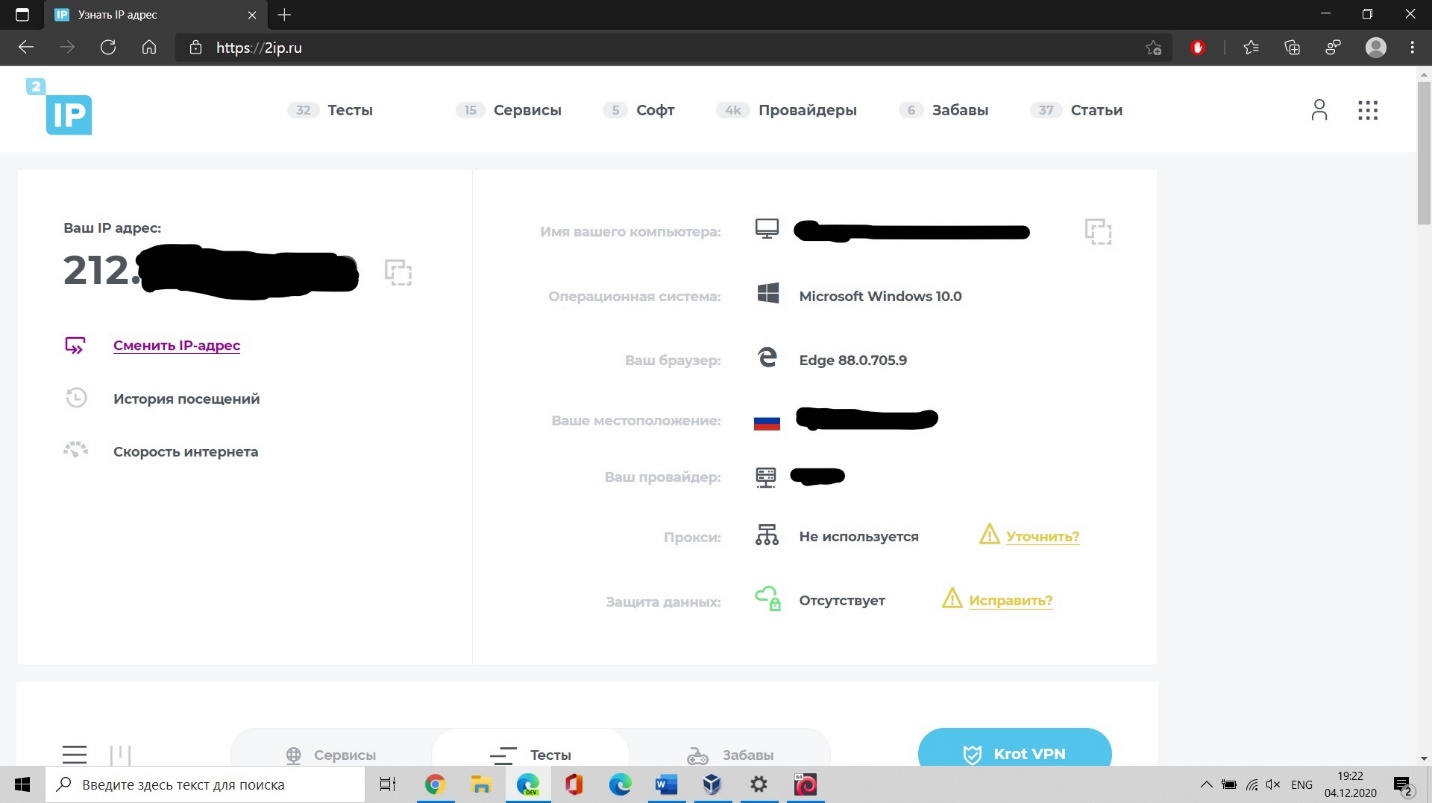


Изменим наш MAC – адрес:

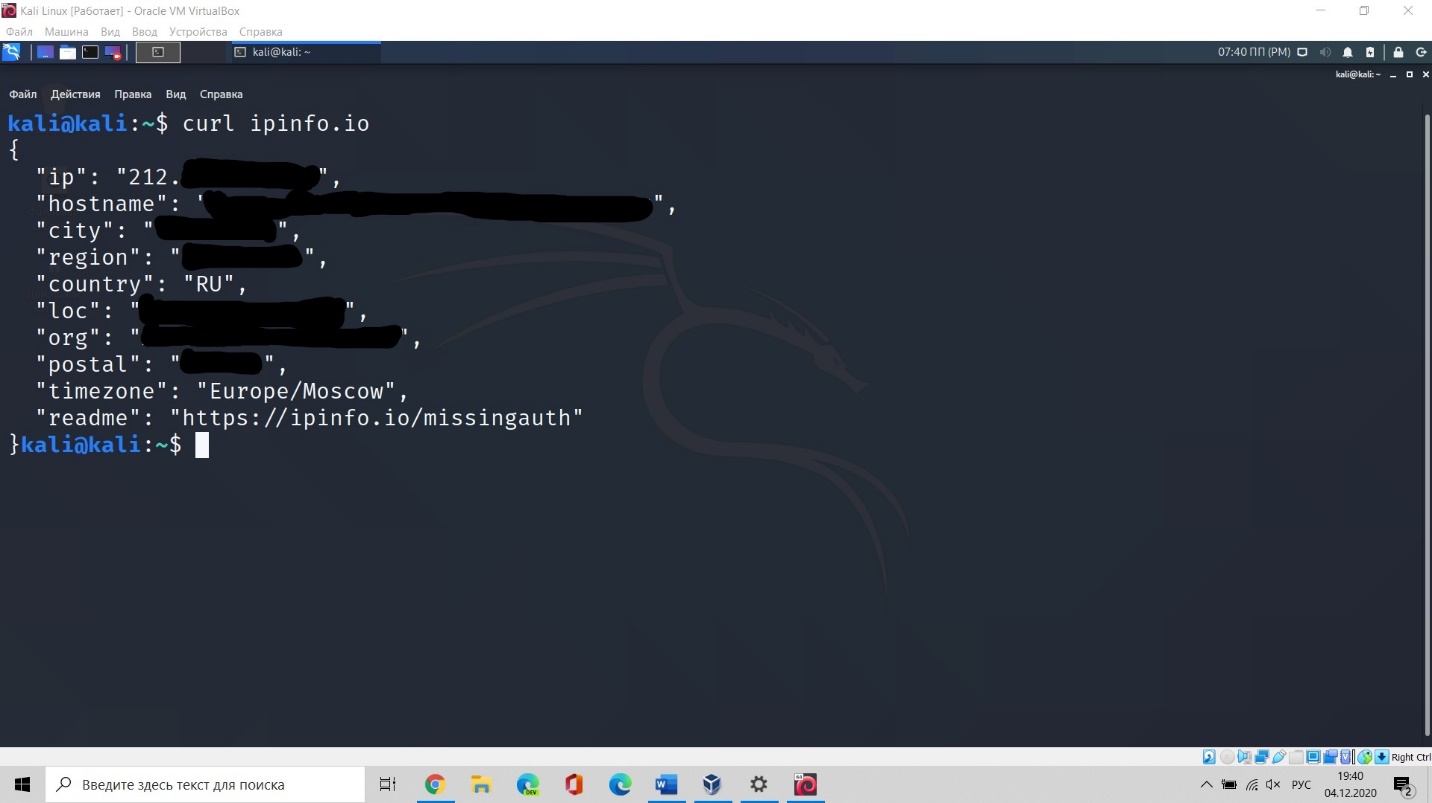


IP – адрес

Определим IP – адрес в сети используя браузер:



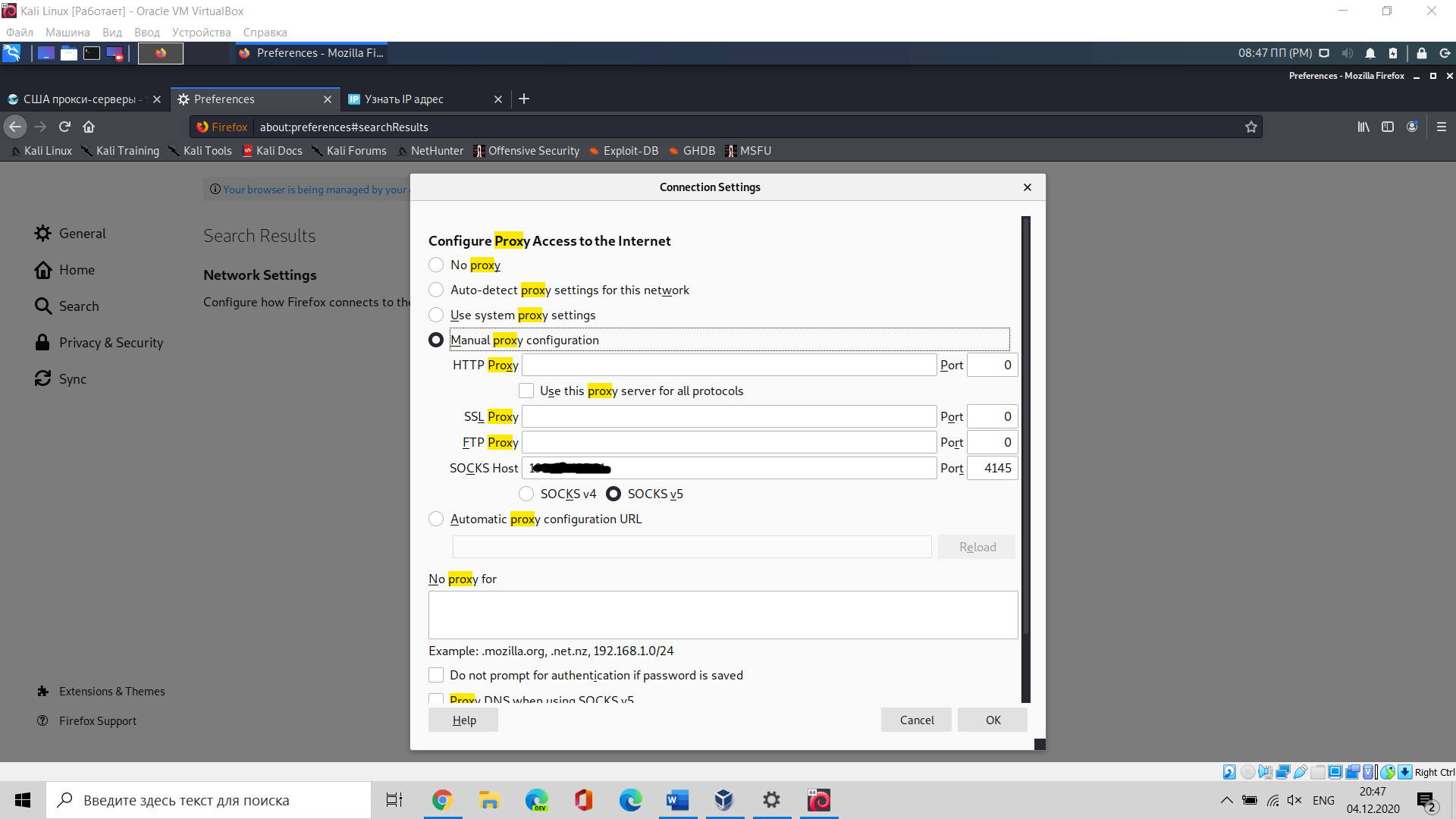
Используя Kali Linux:



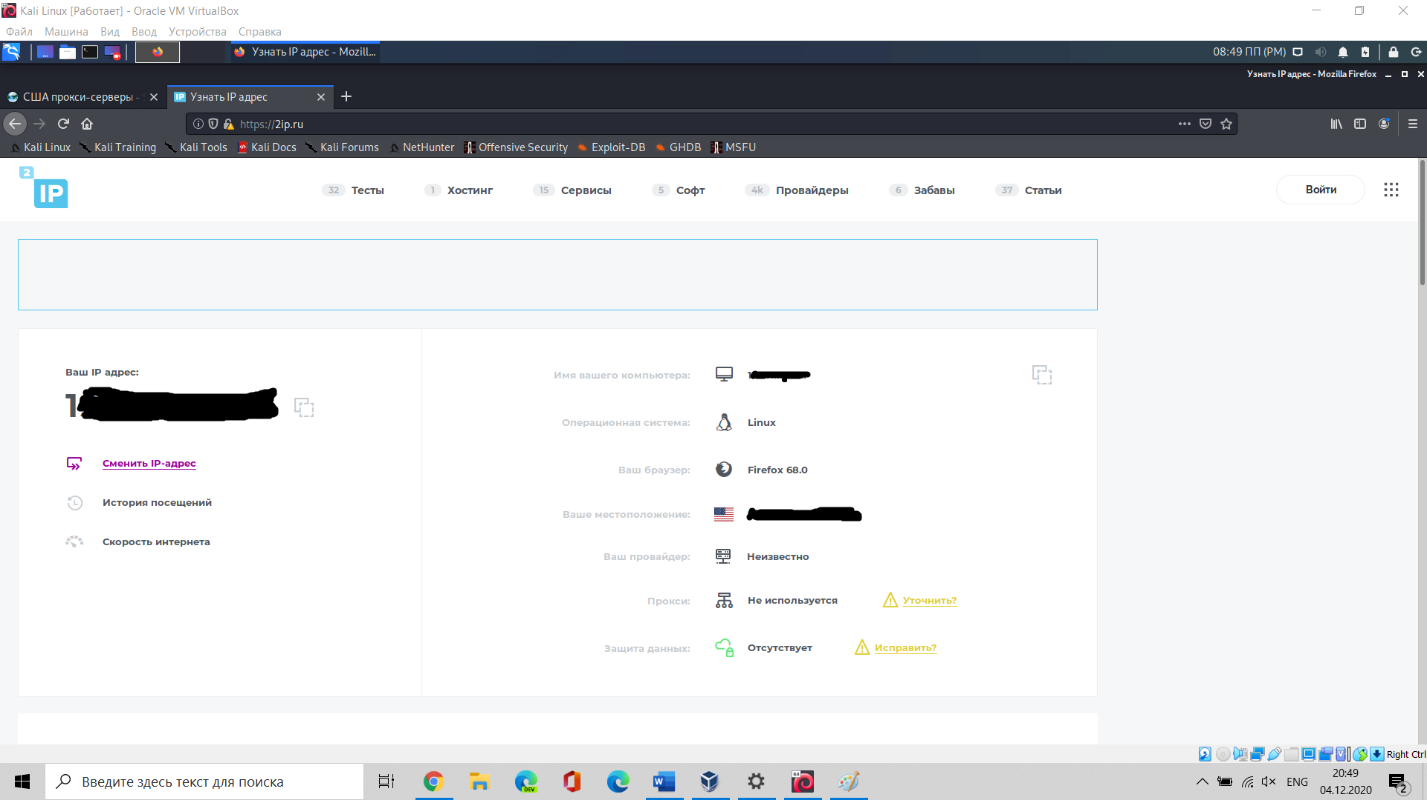
IP – адреса на сайте и Kali совпадают.

Прокси

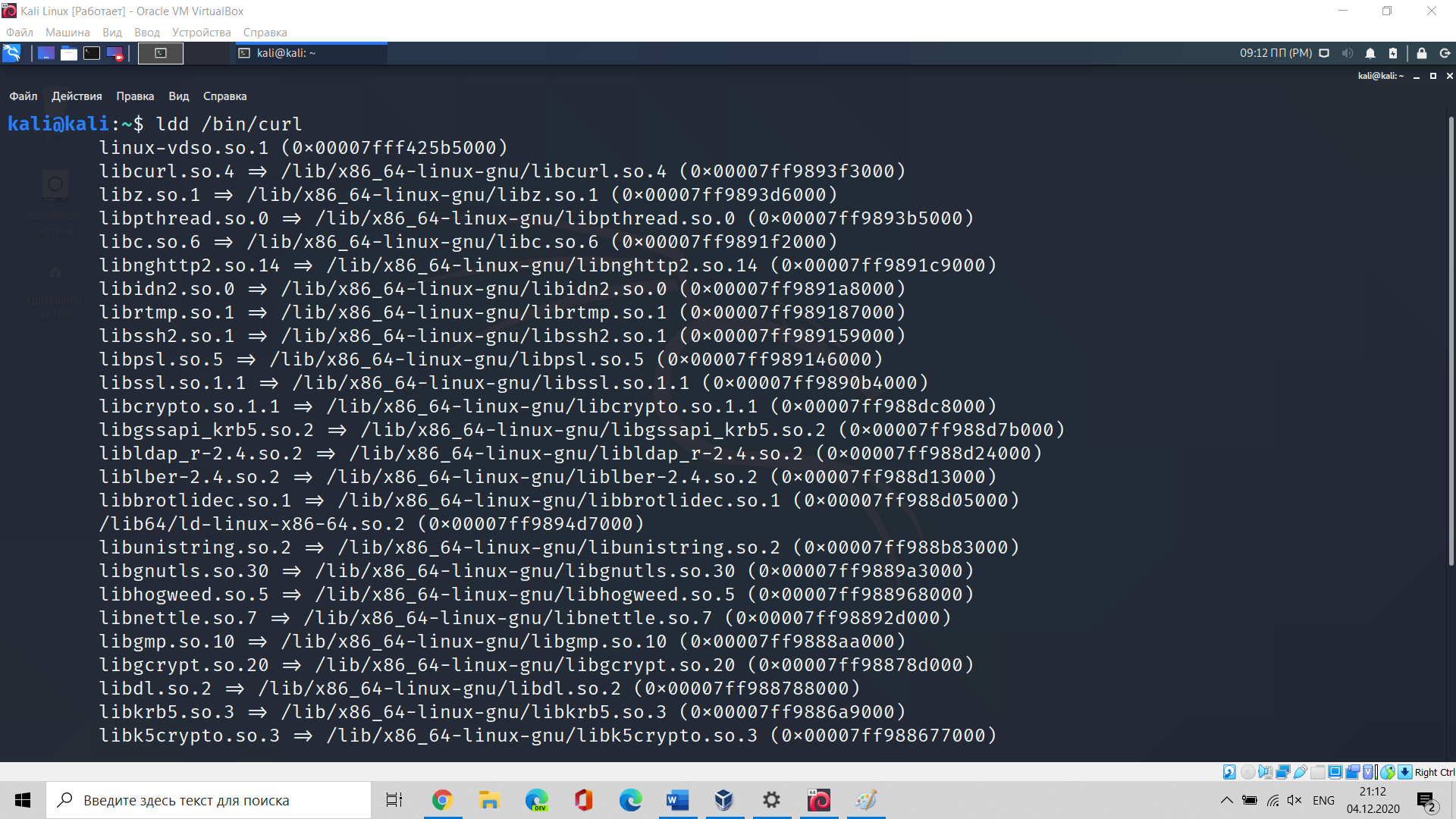
Настроим прокси на Kali Linux в браузере Mozilla Firefox:



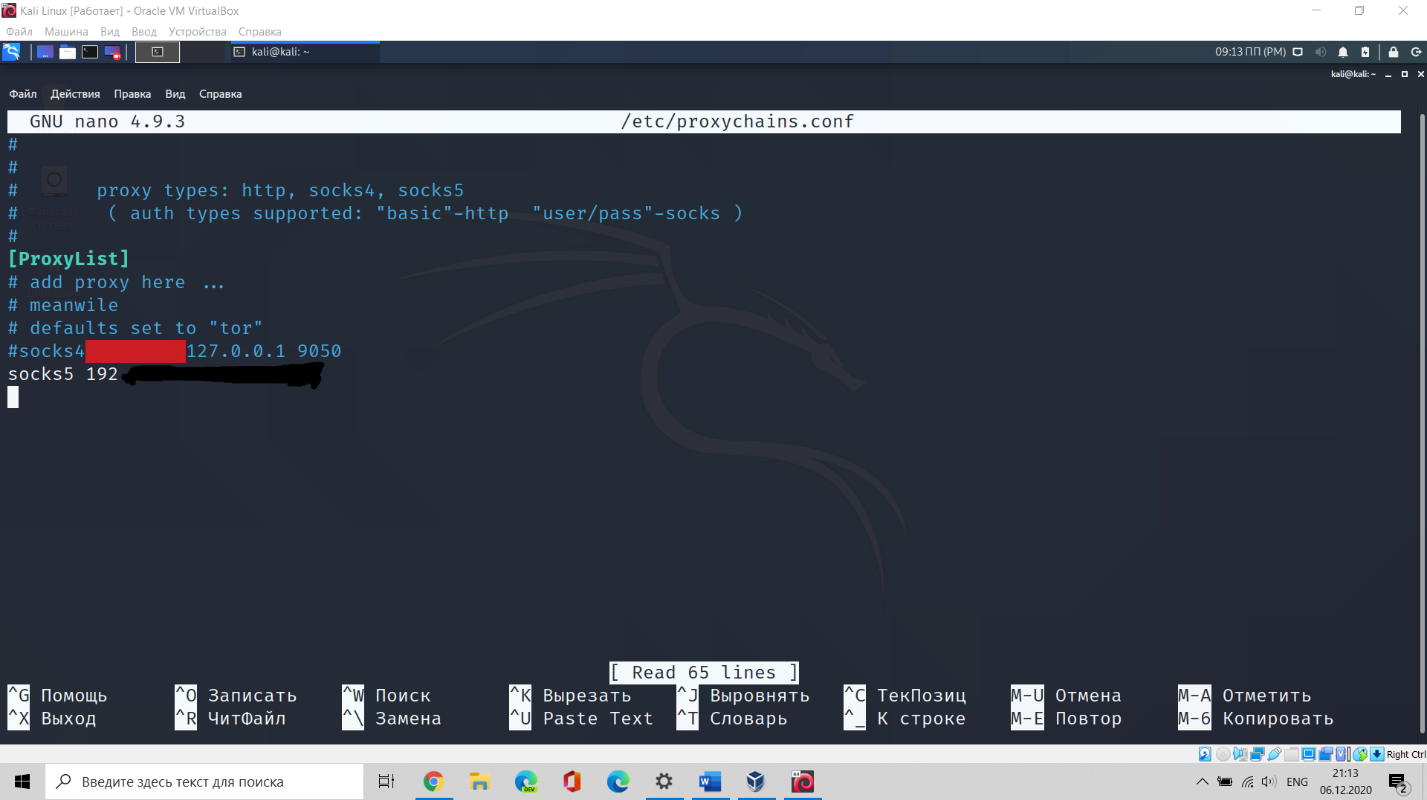
Проверим IP – адрес на сайте 2ip.ru:



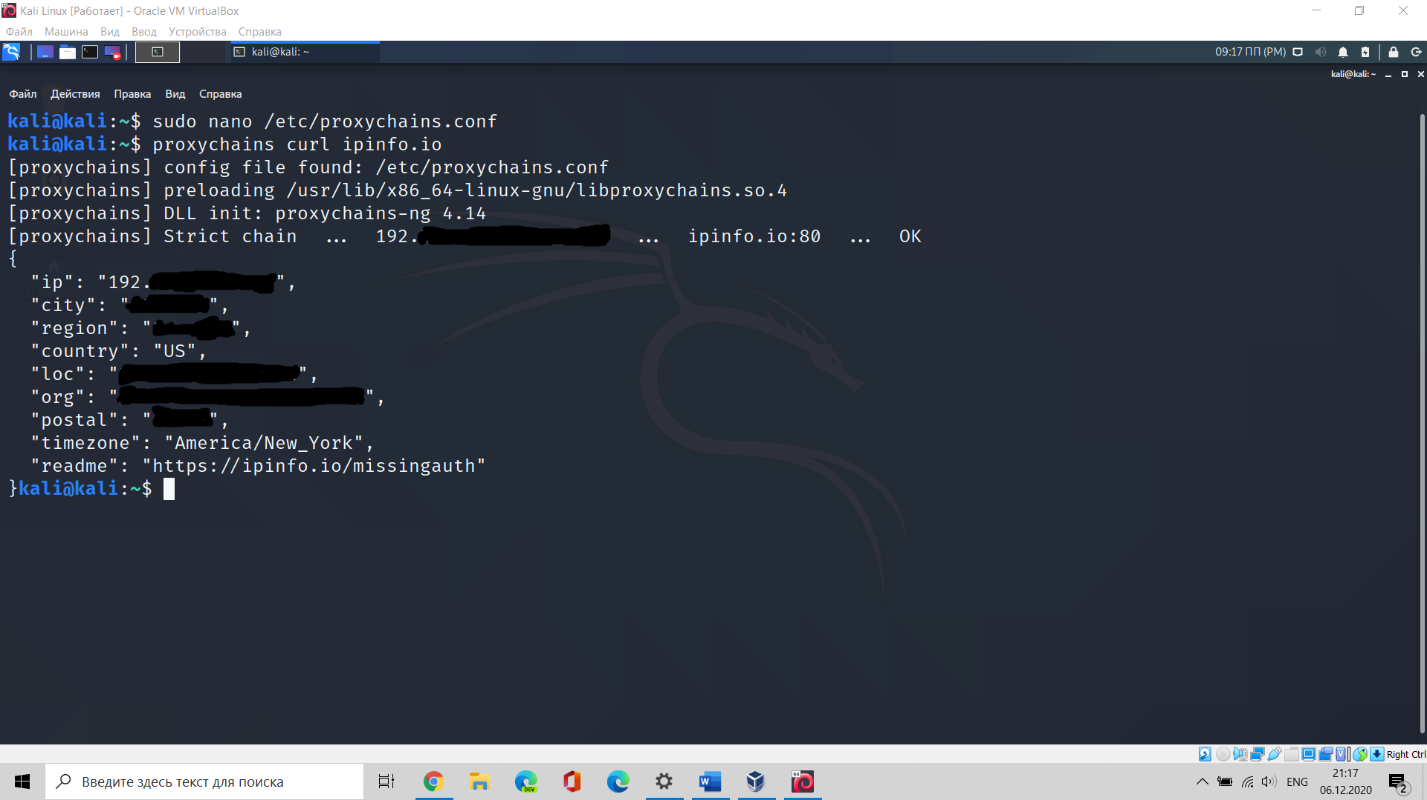
При помощи утилиты ldd посмотрим список разделяемых библиотек:



Добавим прокси-сервер в файл proxychains.conf:

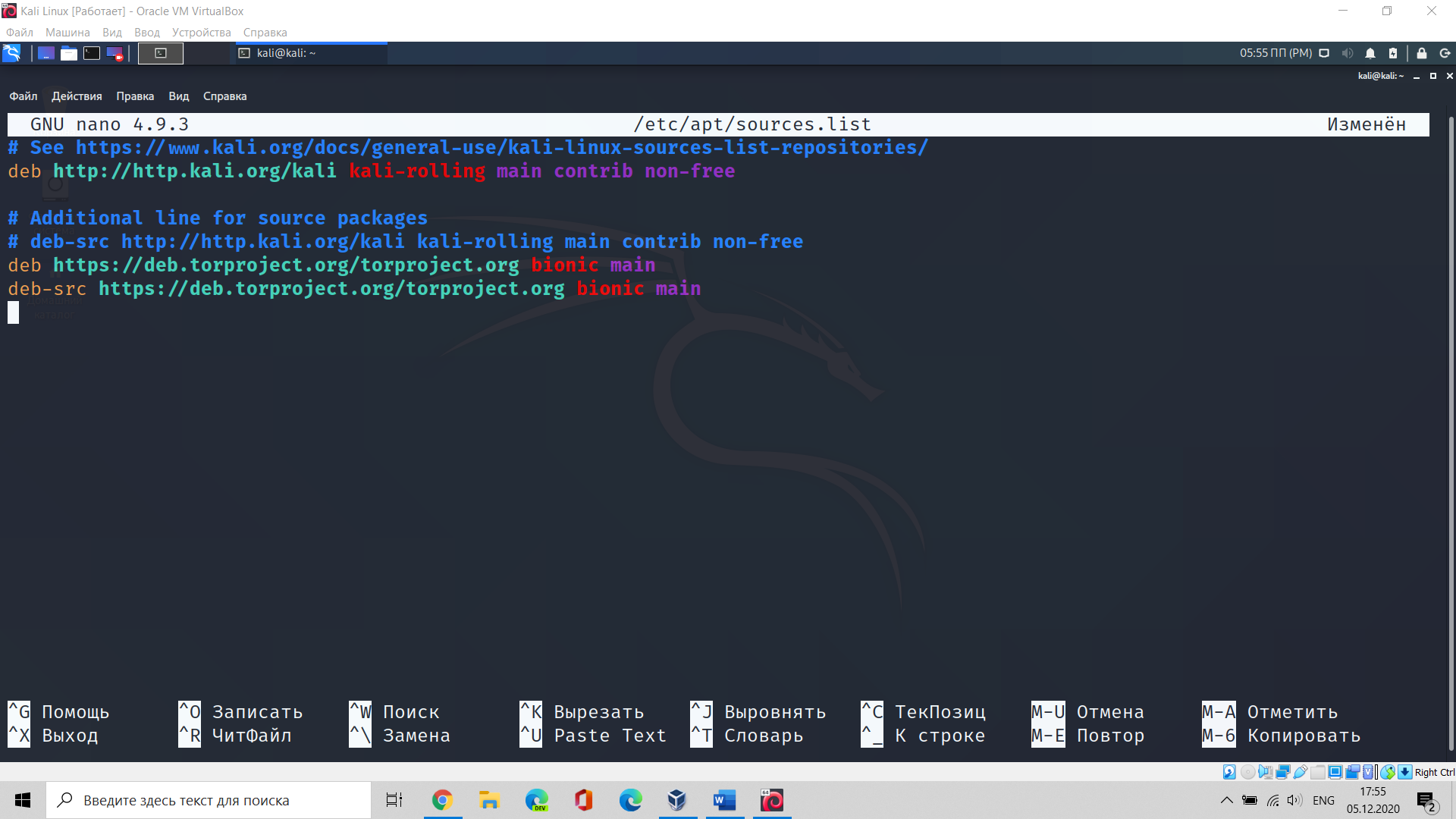


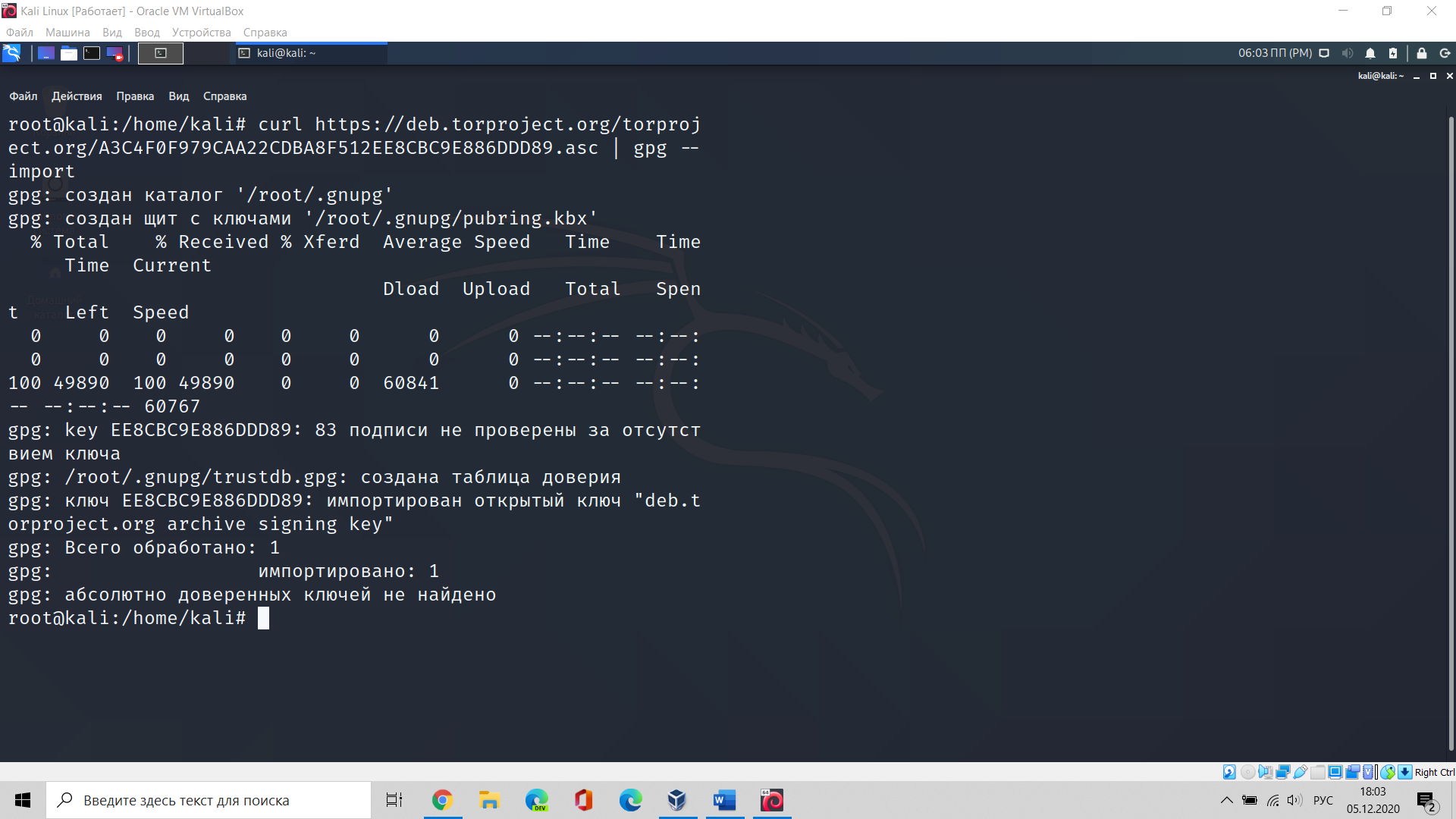
Посмотрим адрес прокси-сервера:

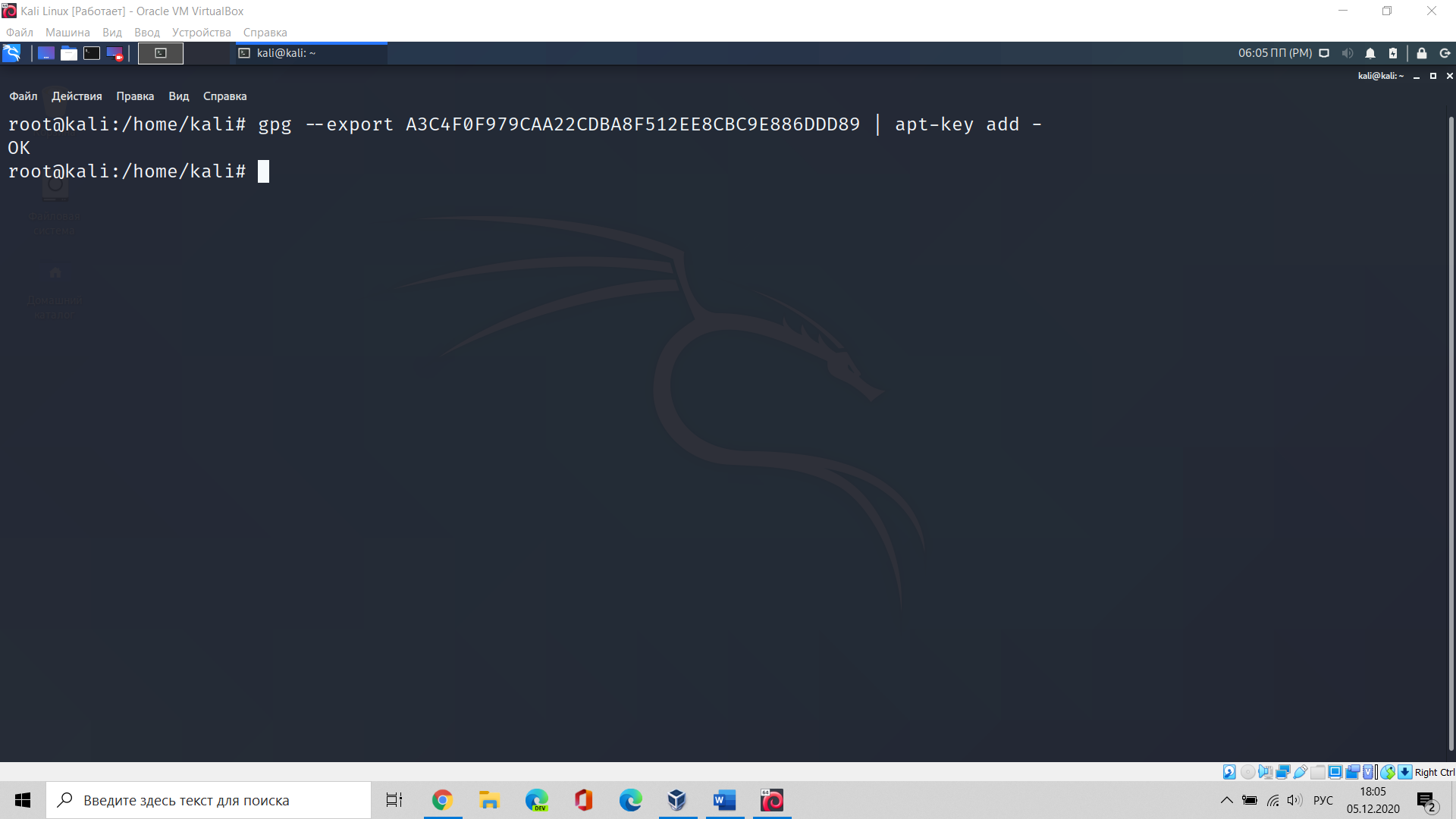
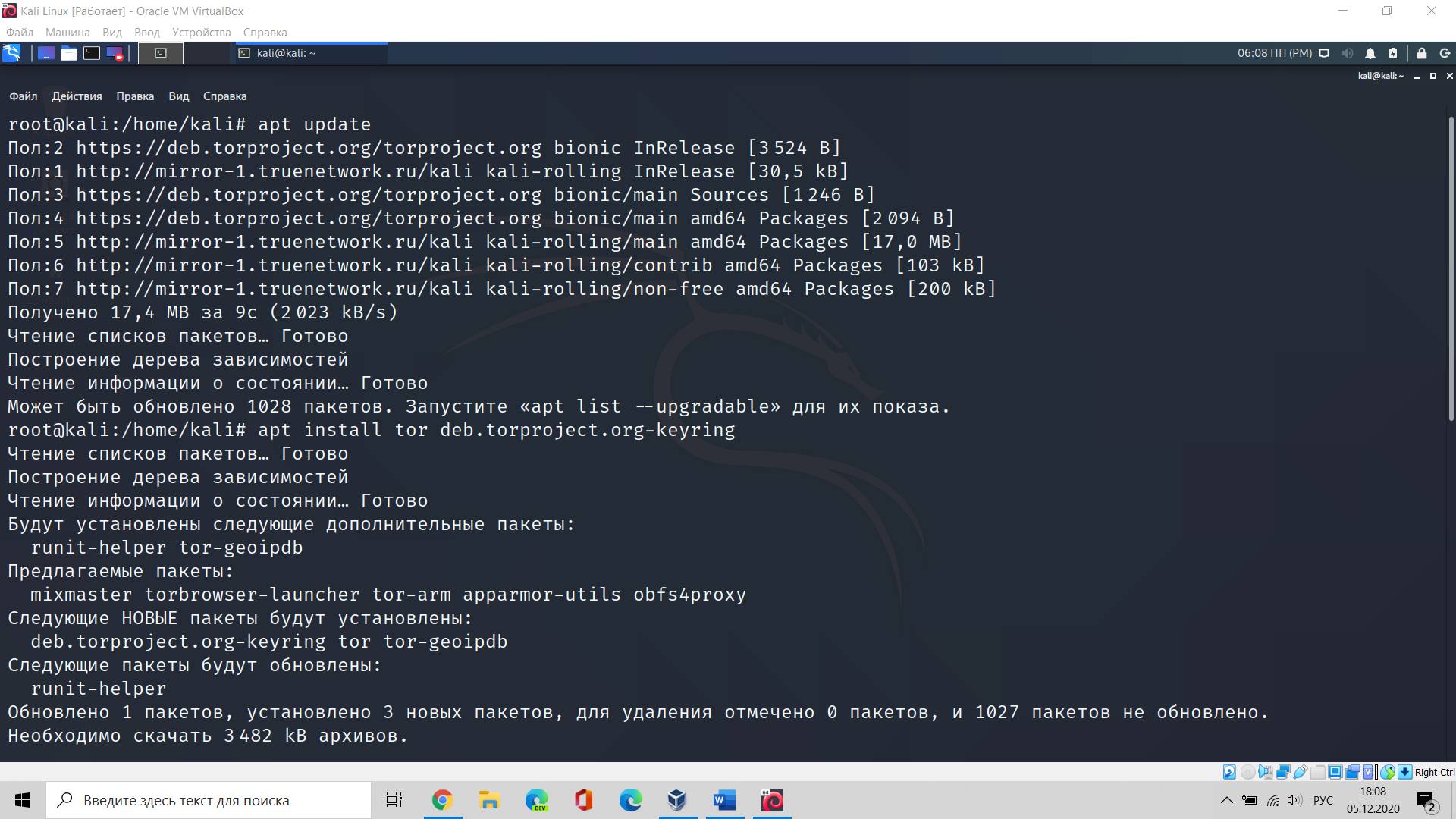


TOR

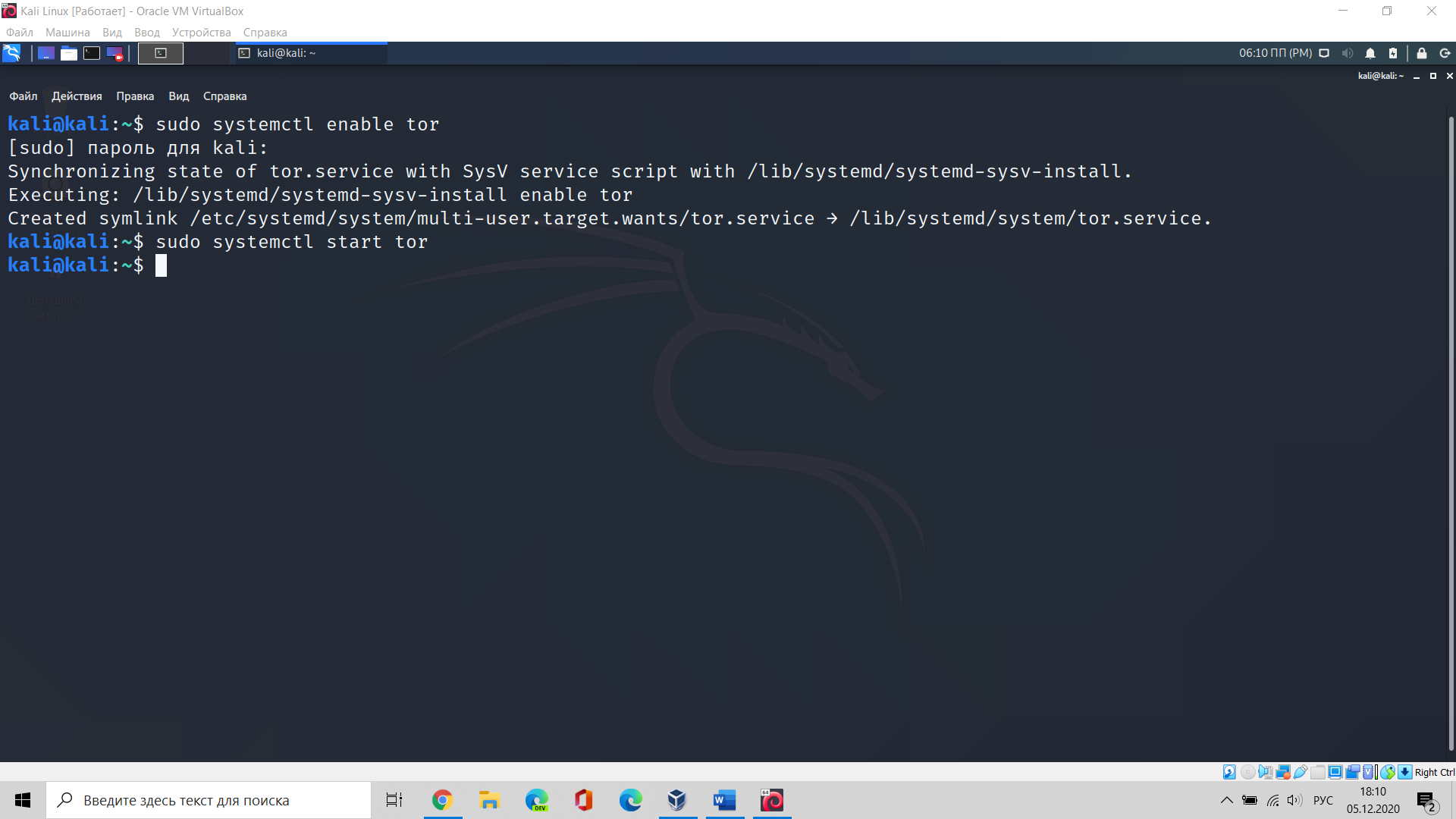
Добавим в файл sources.list две строки:



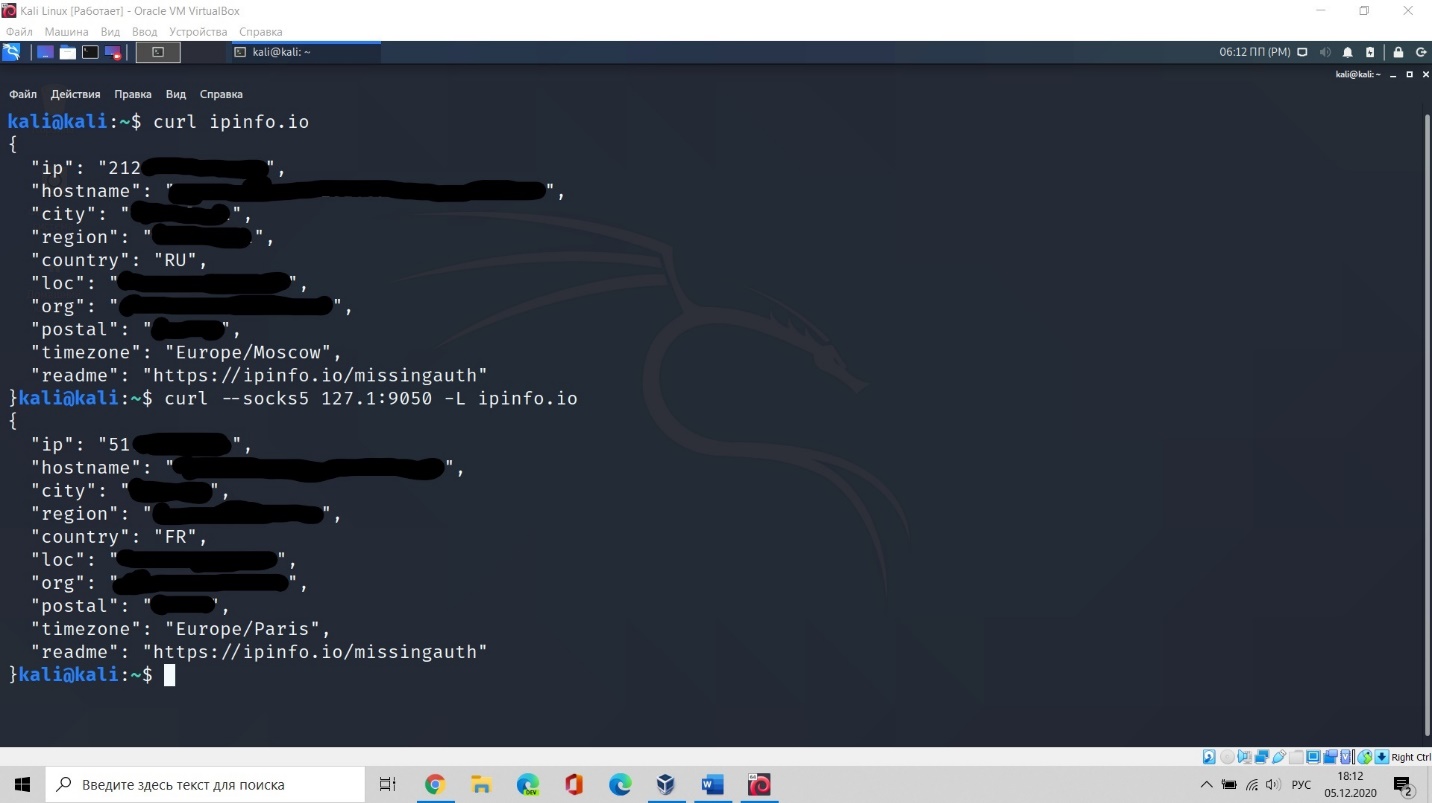
Добавим ключ gpg: 

 Обновим систему и установим TOR: 

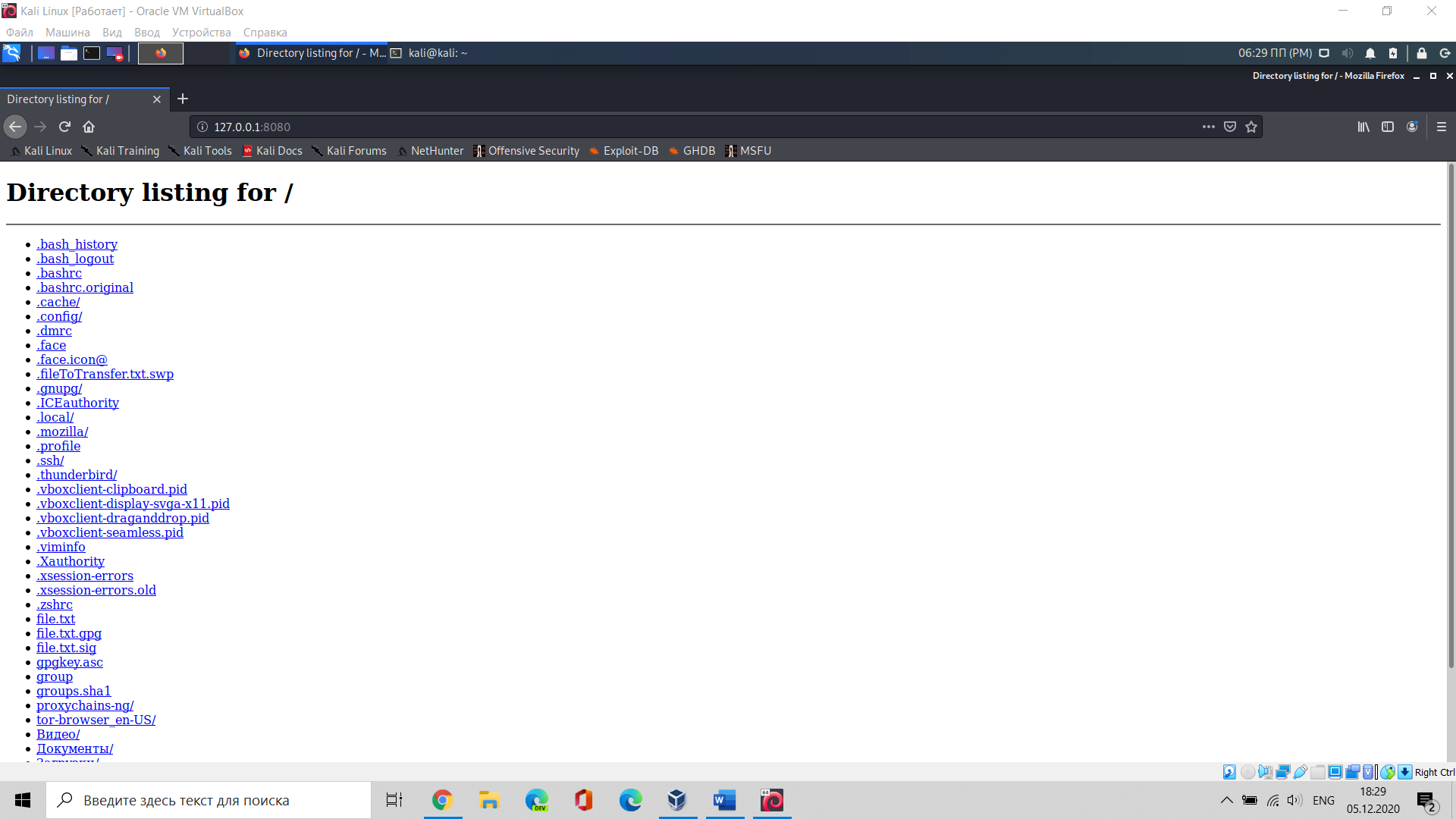
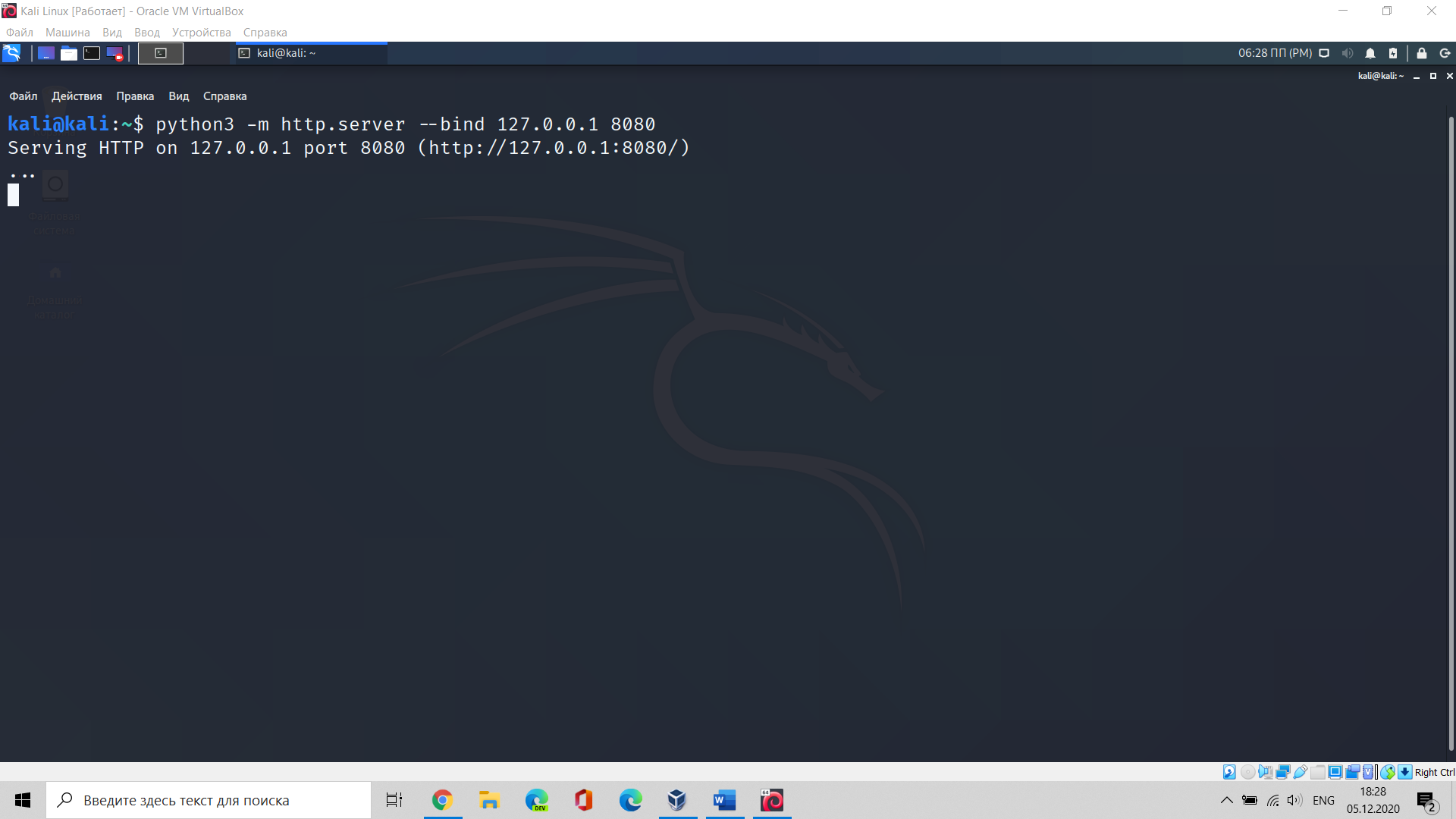
Запустим и добавим TOR в автозагрузку:



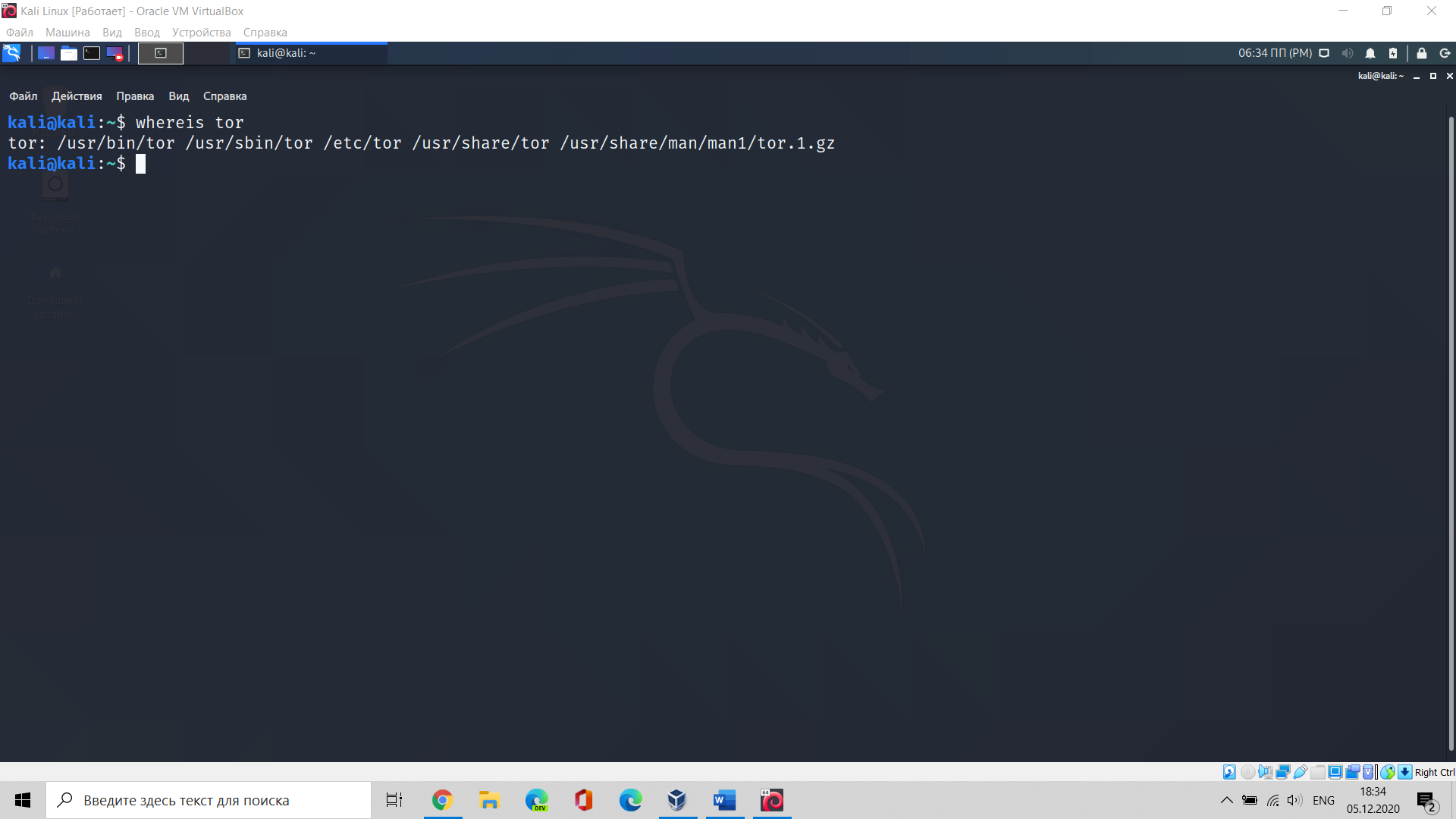
Проверим запуск и соединение с TOR:



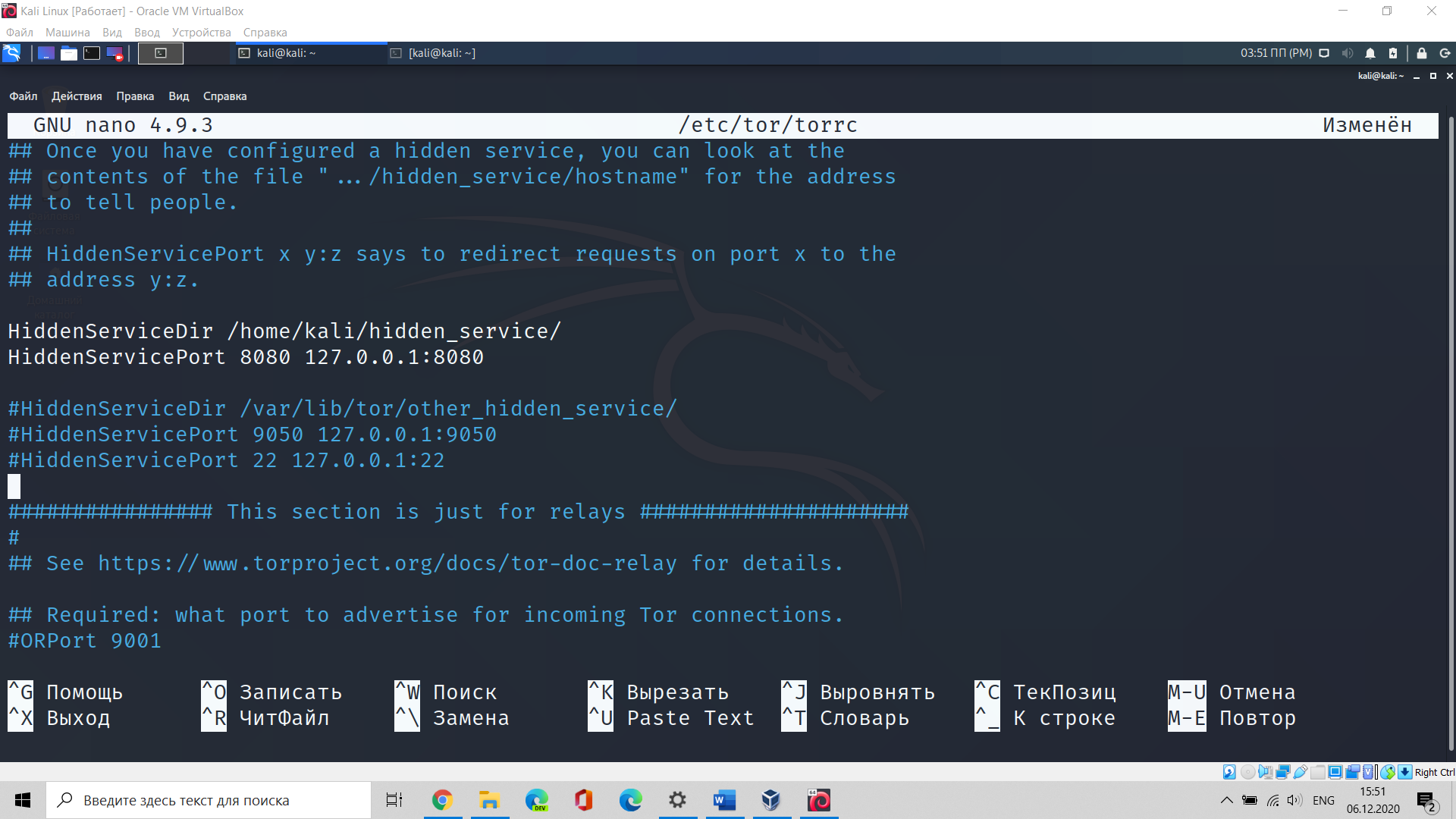
Произведём запуск тестового web сервера:



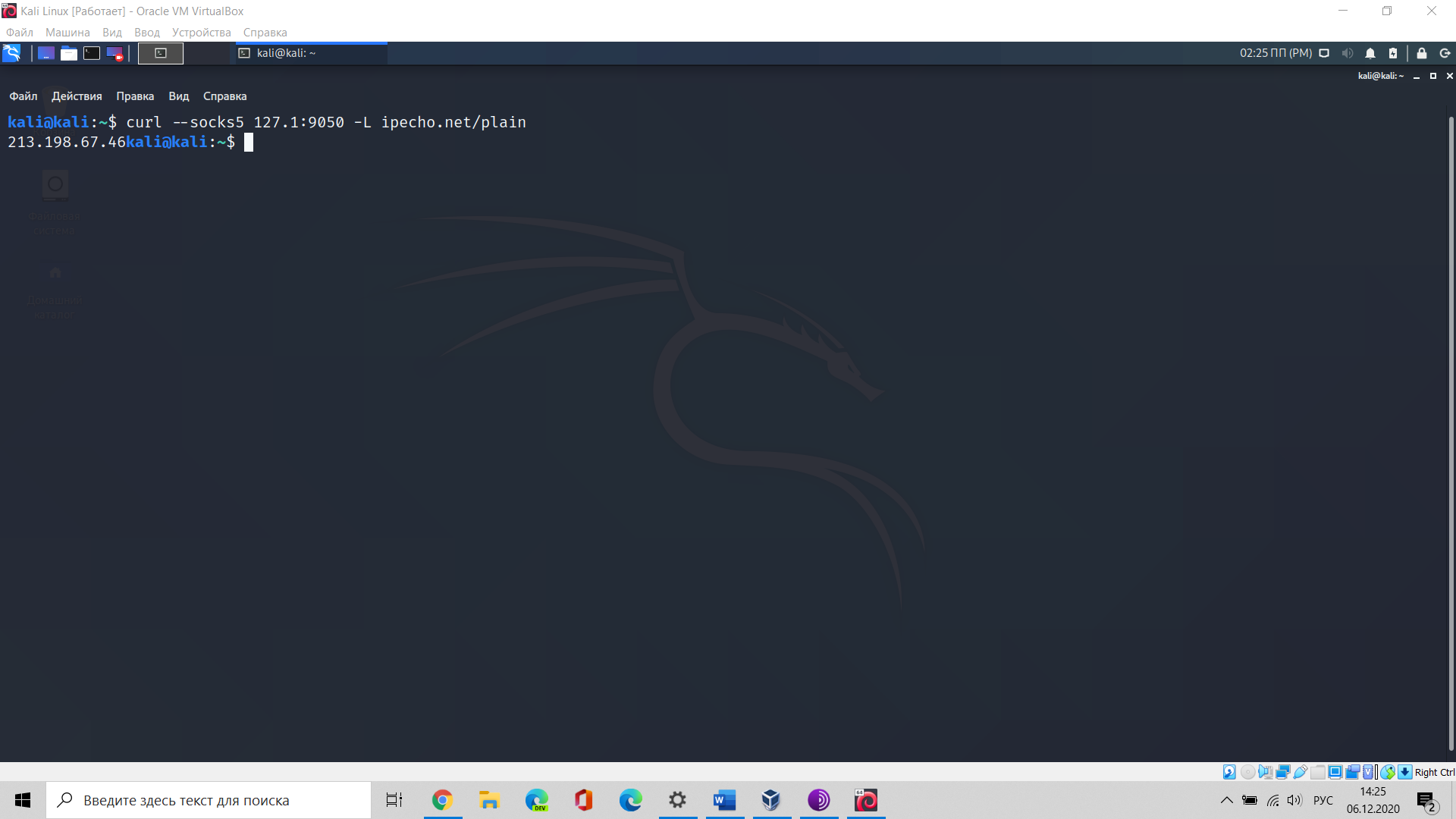
Узнаем место, где был установлен TOR:



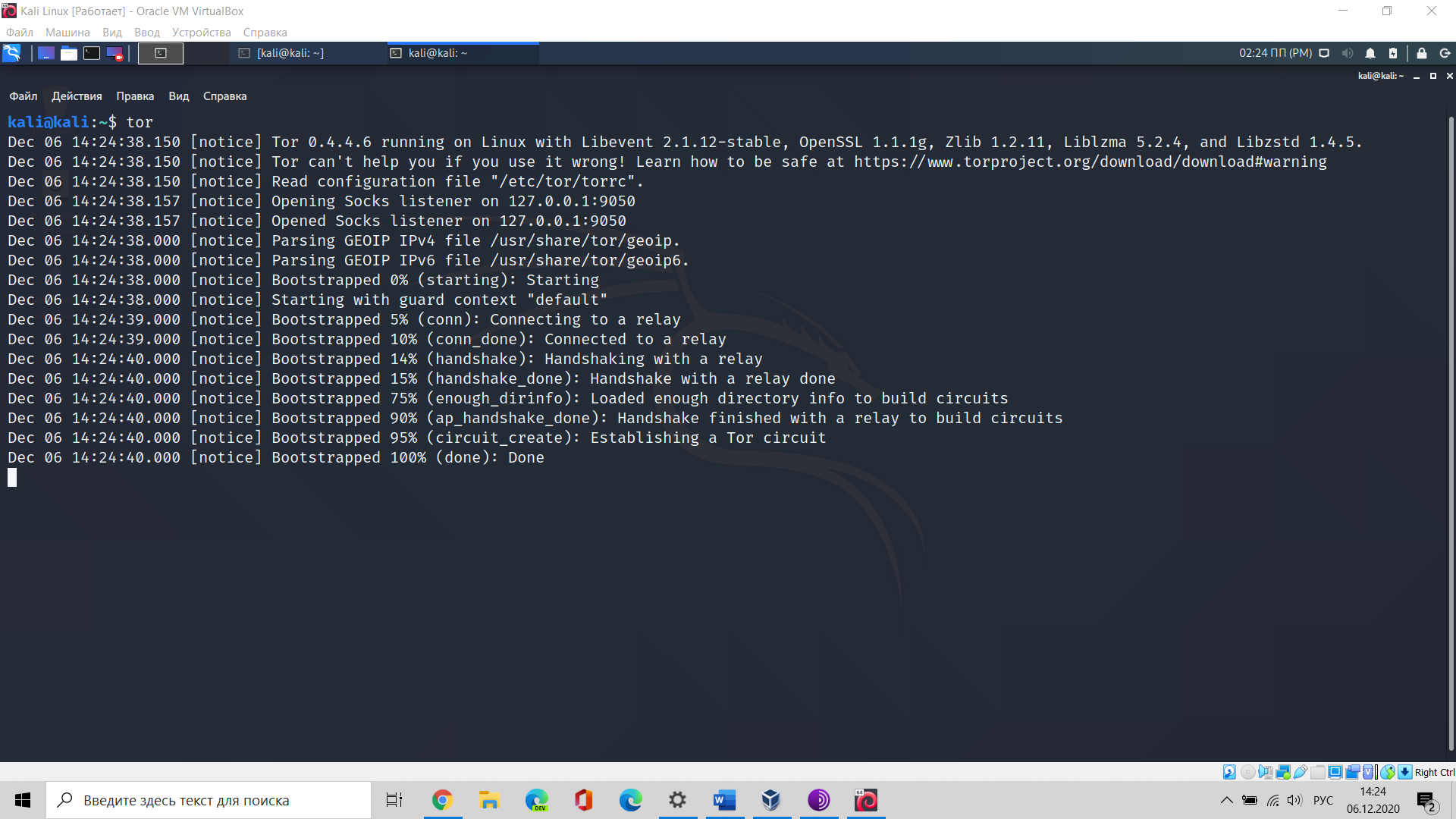
Раскомментируем и модифицируем строки в файле torrc:



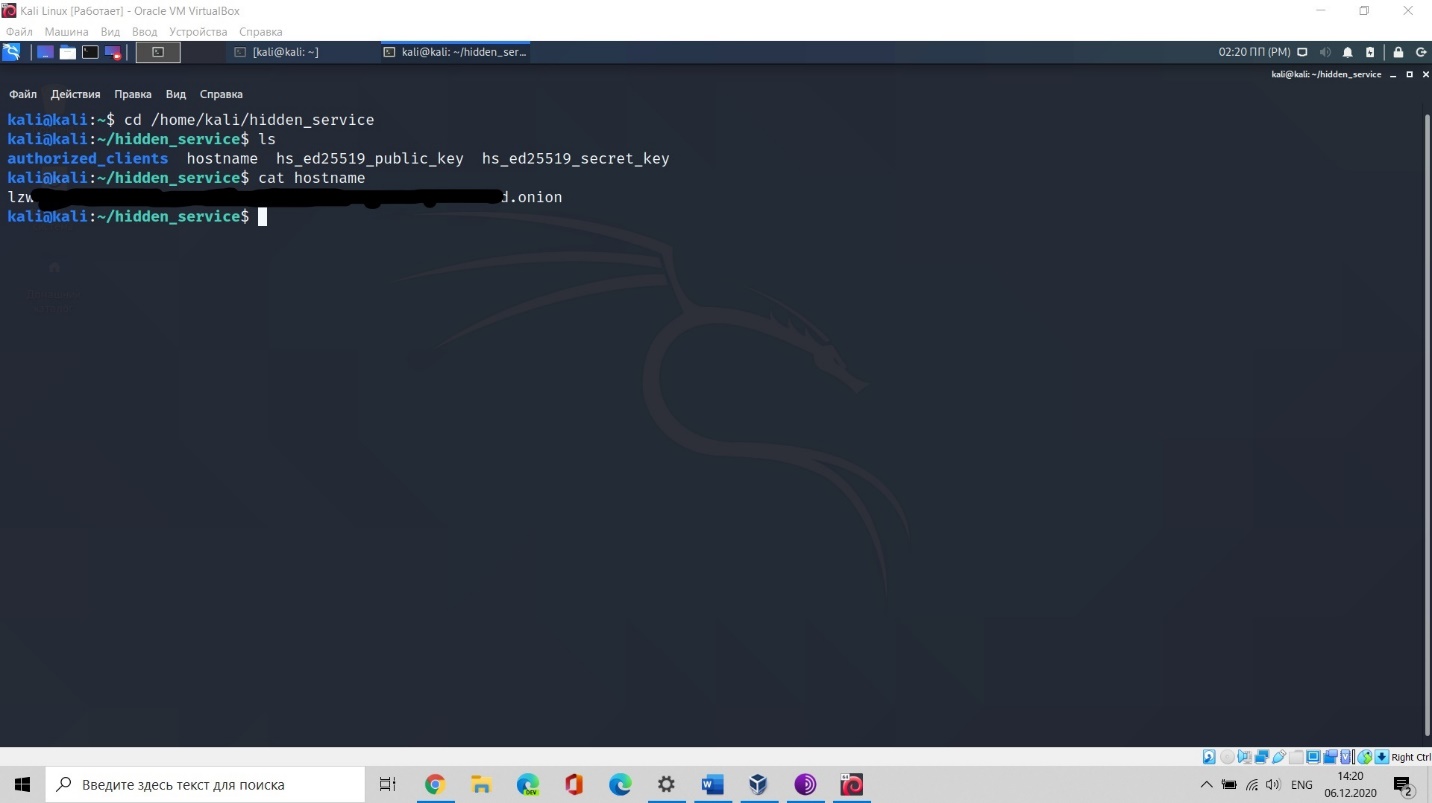
Перезапустим и произведём повторный запуск через прокси:



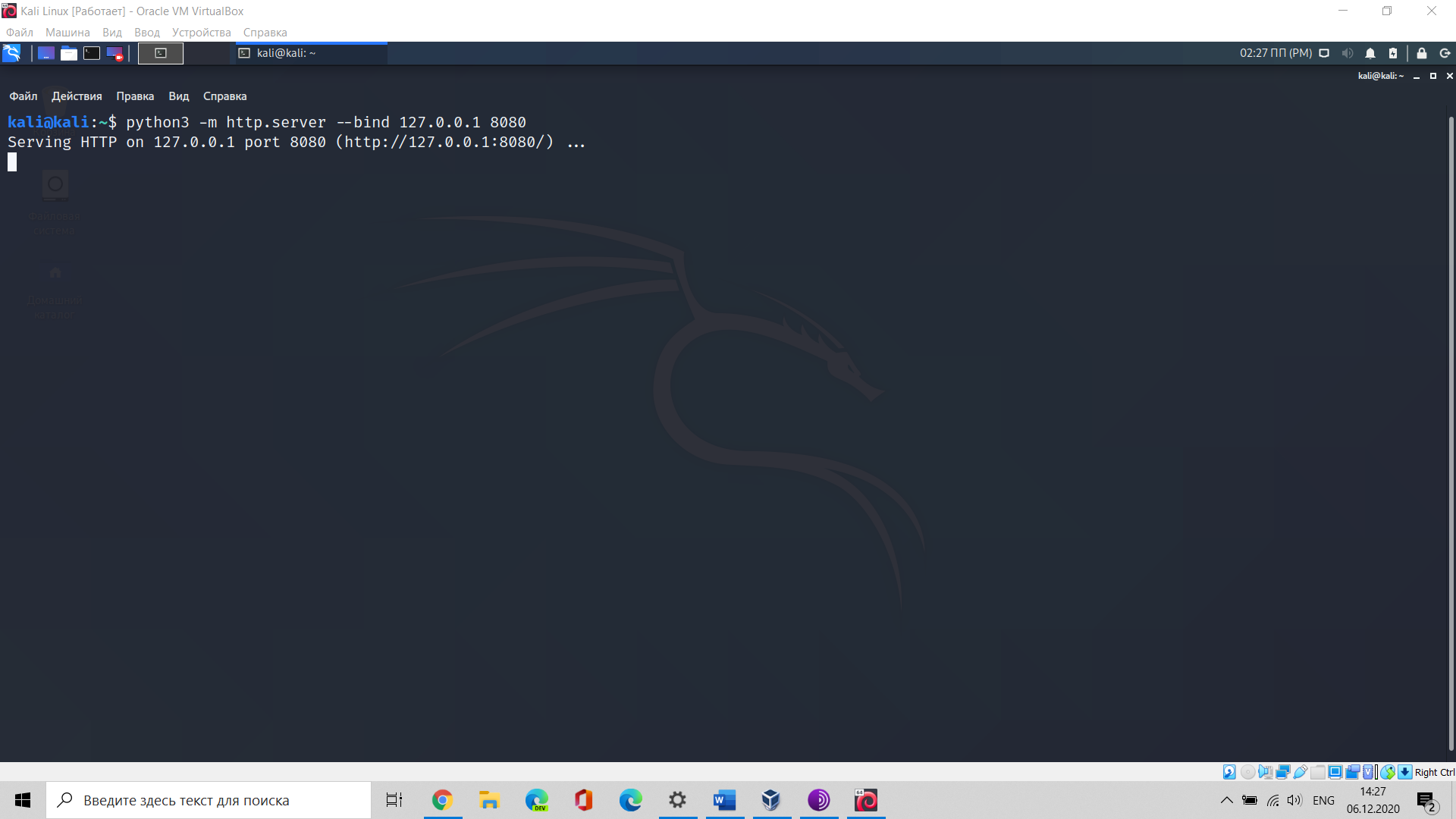
Запустим TOR от имени пользователя:



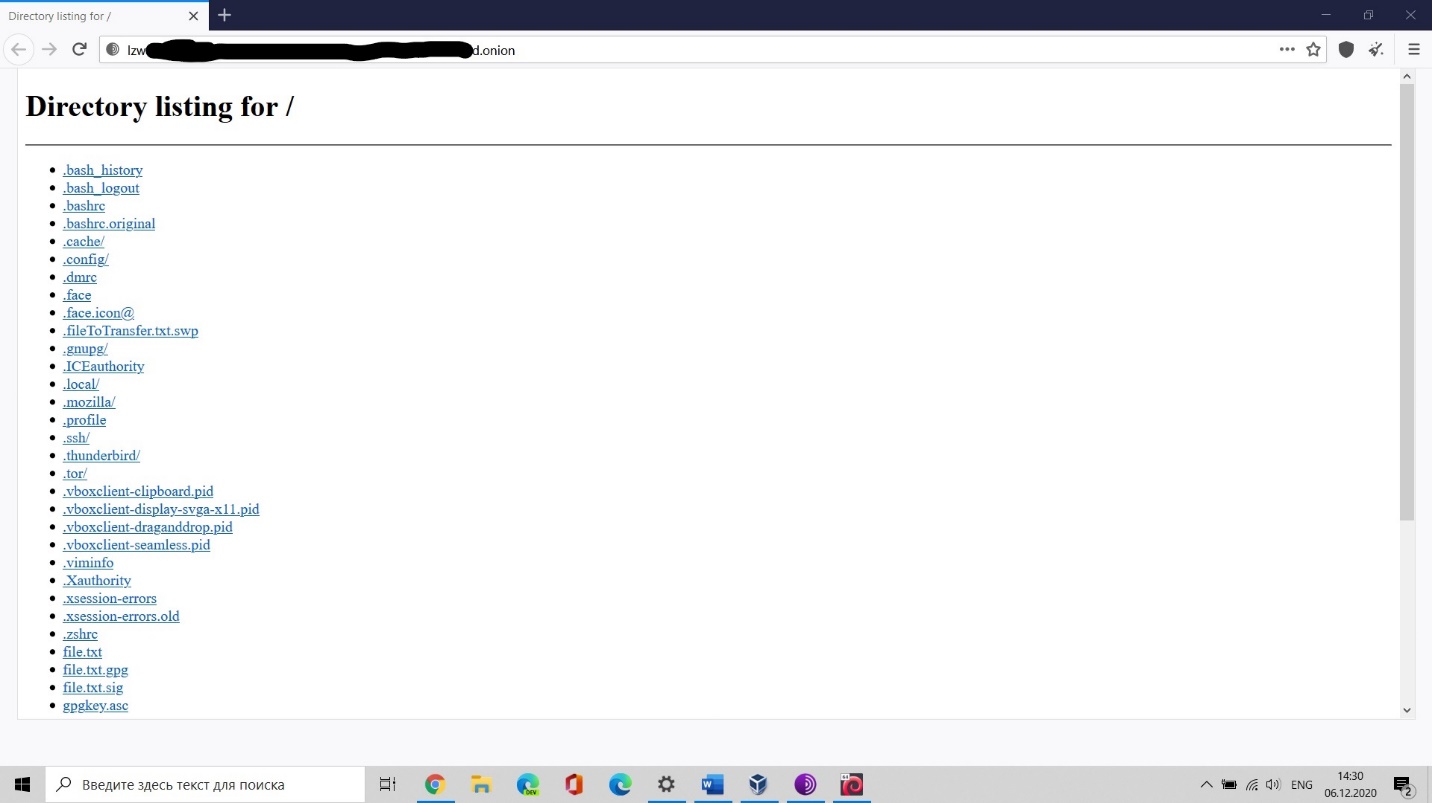
Перейдём в папку hidden\_service и убедимся что там находятся файлы “hostname” и “secret\_key”, а после получим сгенерированный адрес:



Снова запустим сервер:

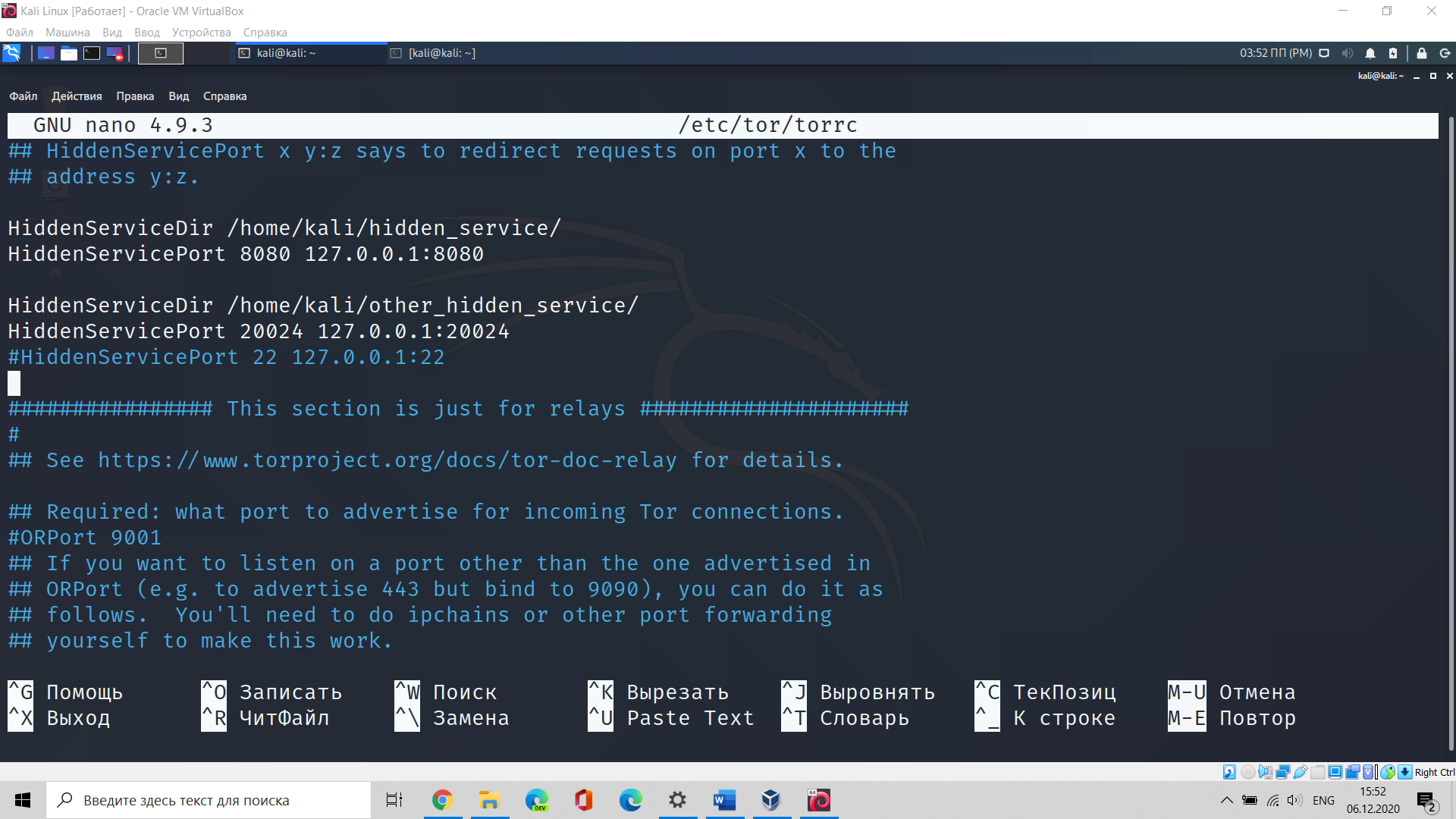


Проверим сайт в TOR на Windows:

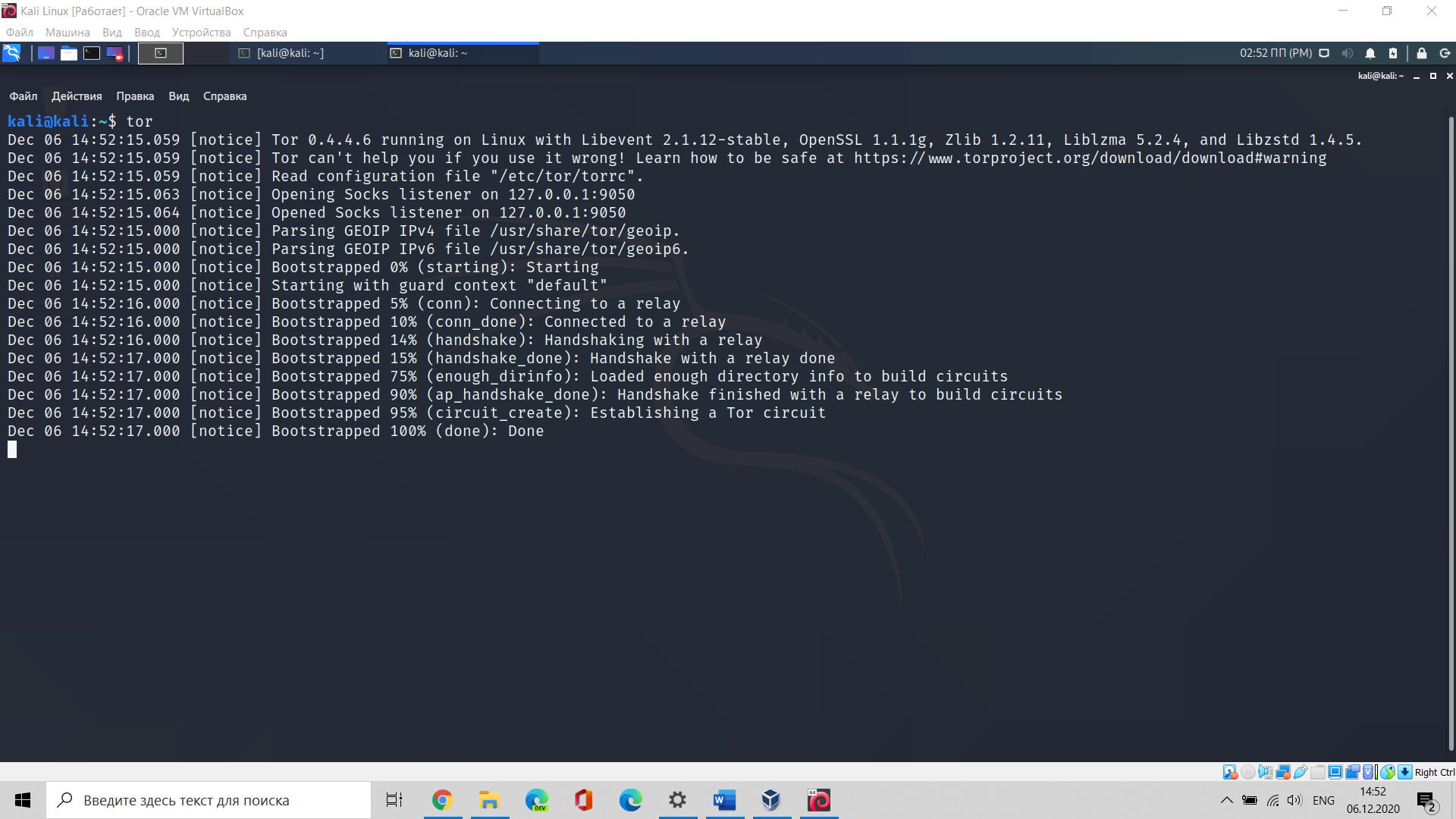


SSH – сервер

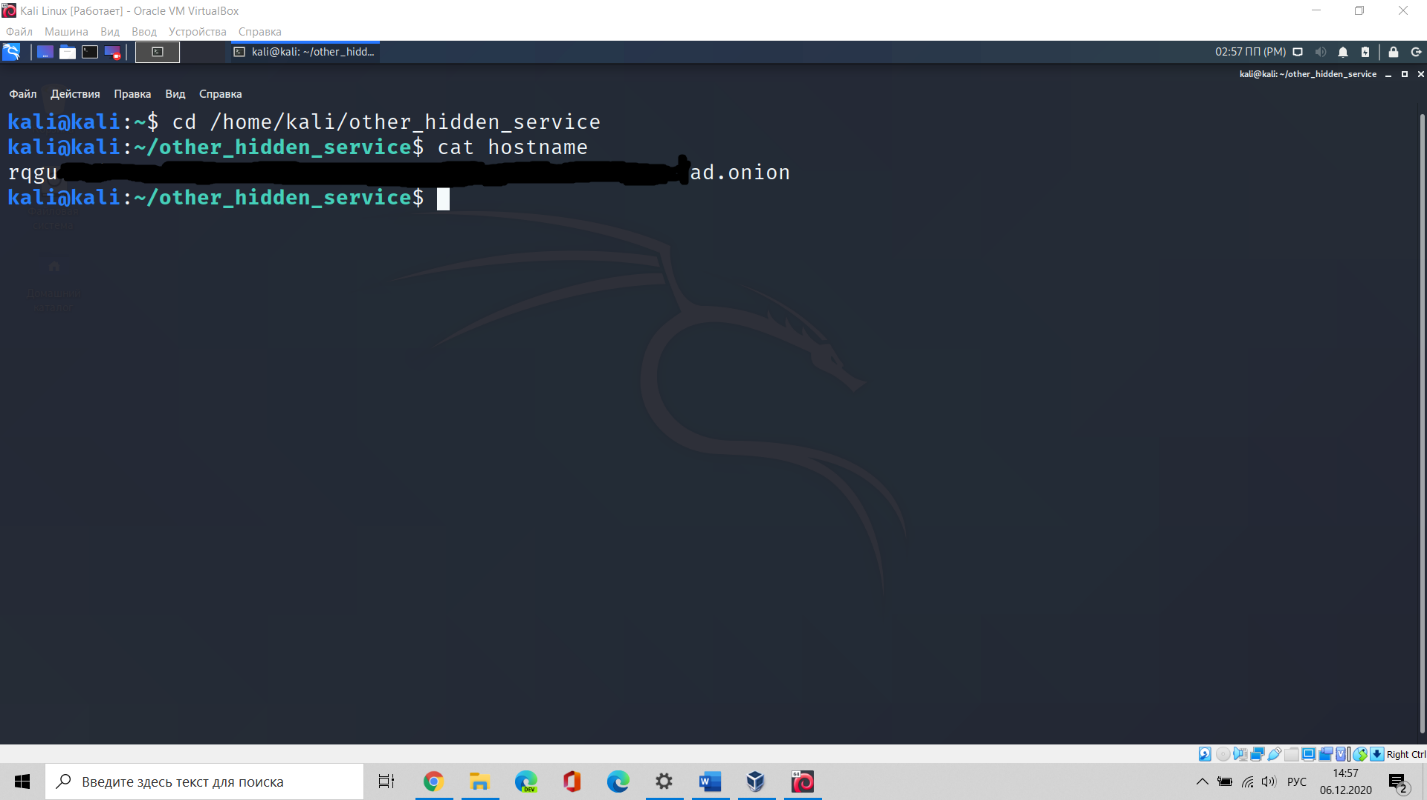
Раскомментируем и модифицируем строки в файле torrc:



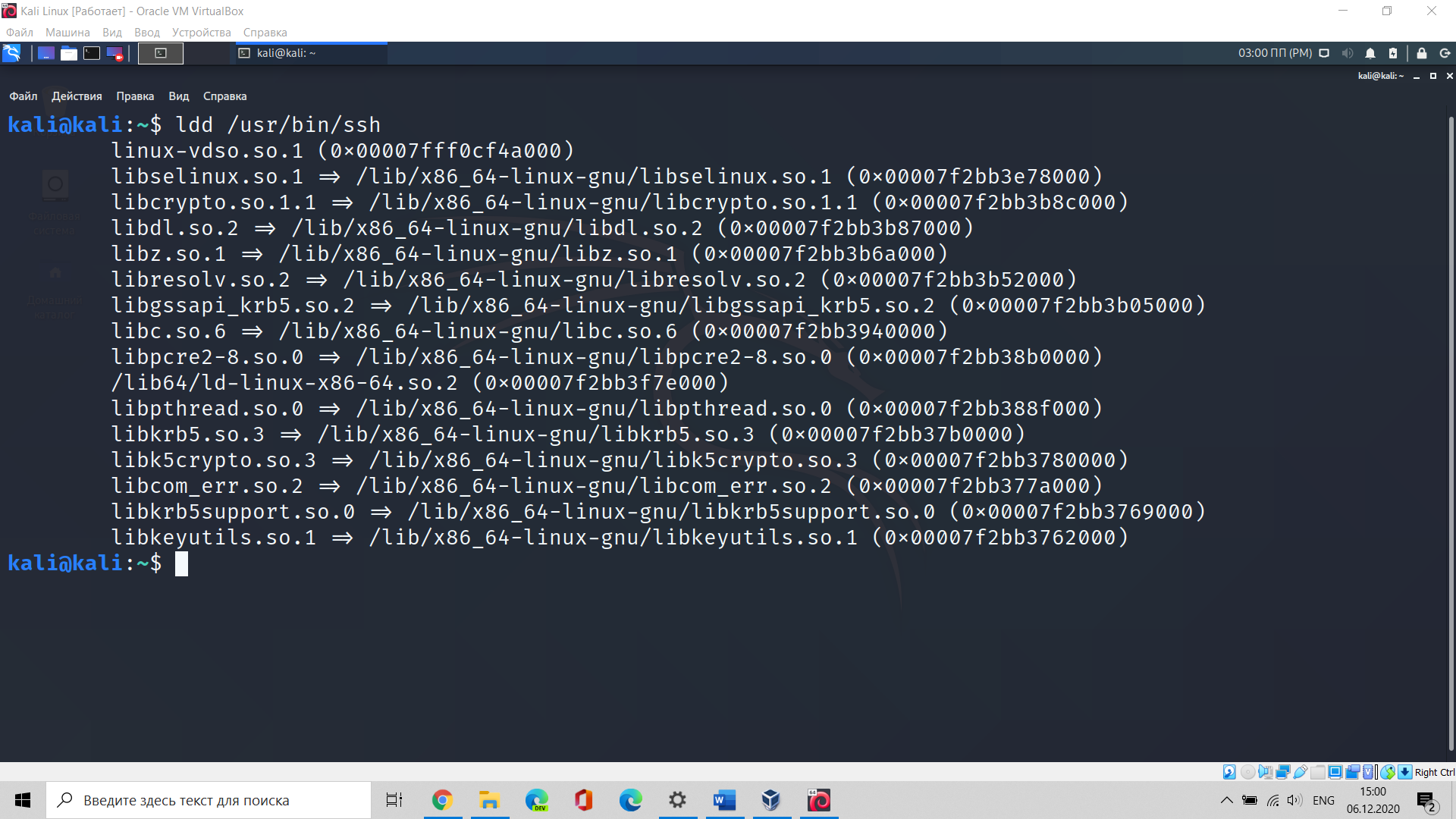
Перезапустим TOR:



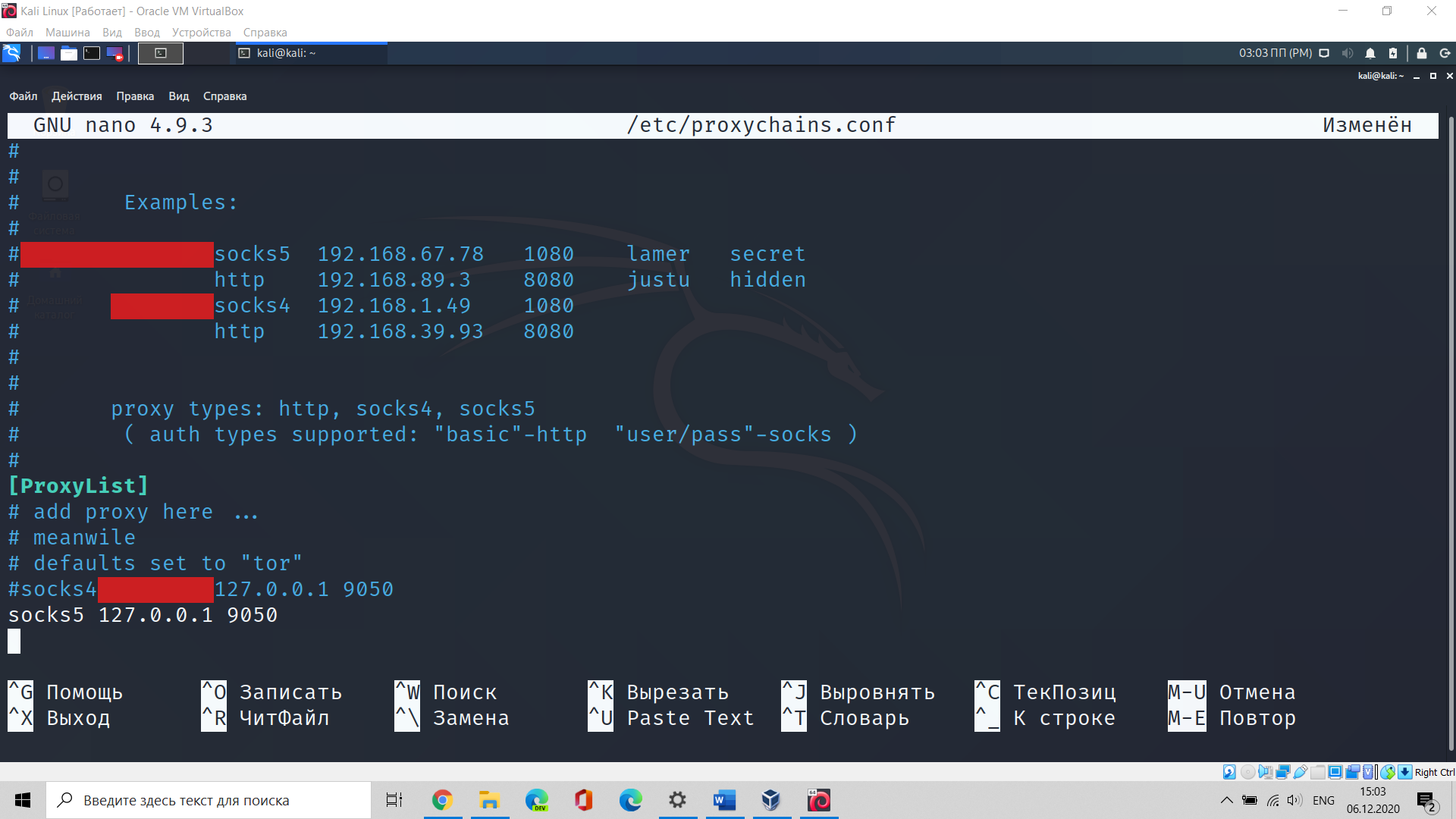
Отобразим значение “.onion” из “other\_hidden\_service”:



Выведем список разделяемых библиотек:



Изменим данные в файле proxychains.conf:



Установим connect-proxy:

