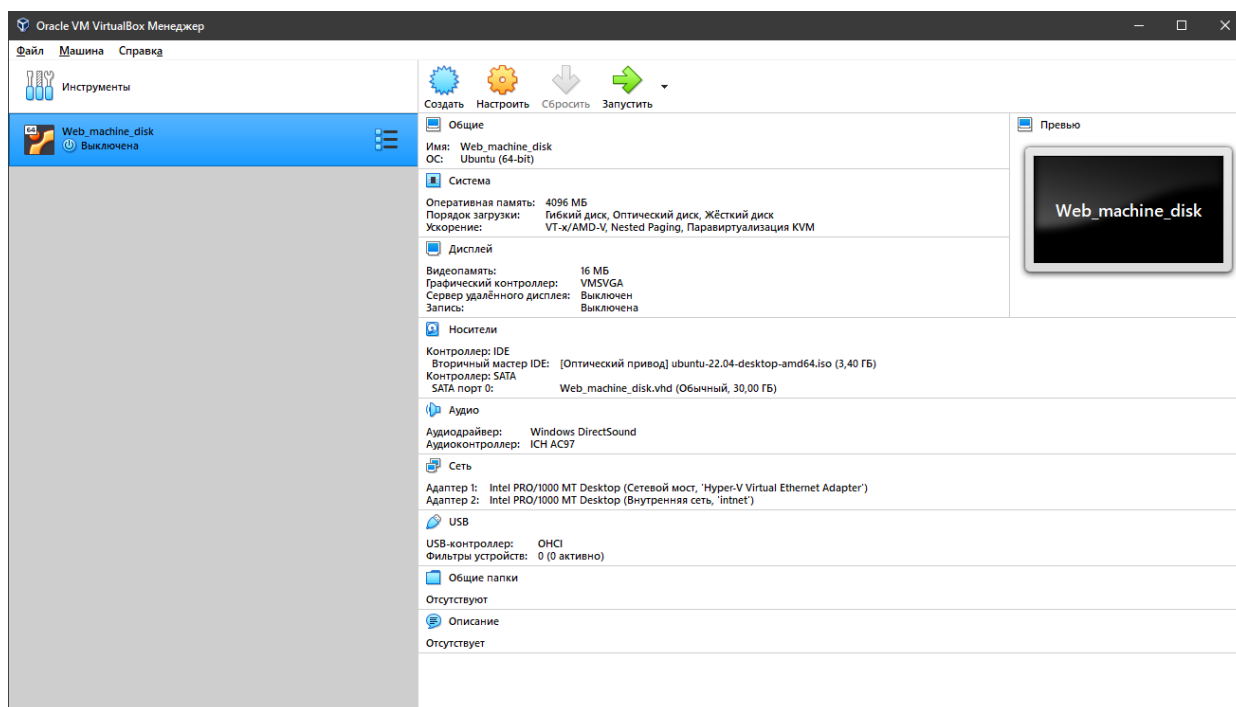
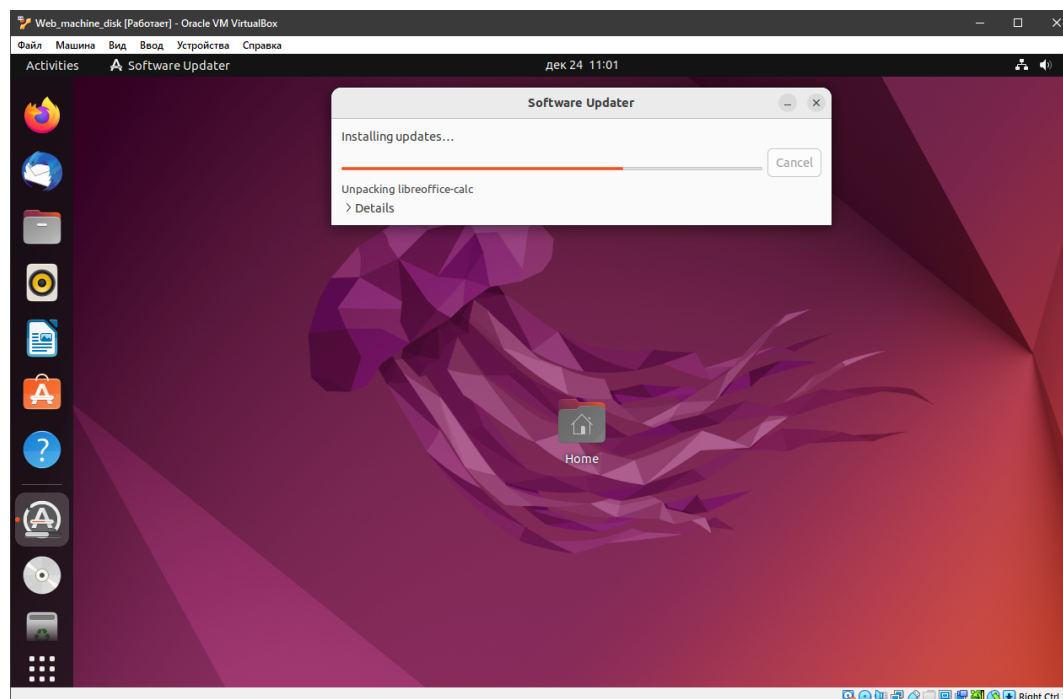


Задание 1: 1. Установите VirtualBox и виртуальную машину с Ubuntu. Все дальнейшие задания рекомендуется делать на Ubuntu.



Предустановки выбранные для Ubuntu. Использовался образ 22.04LTS, ранее используемый для знакомства с unix семейством.

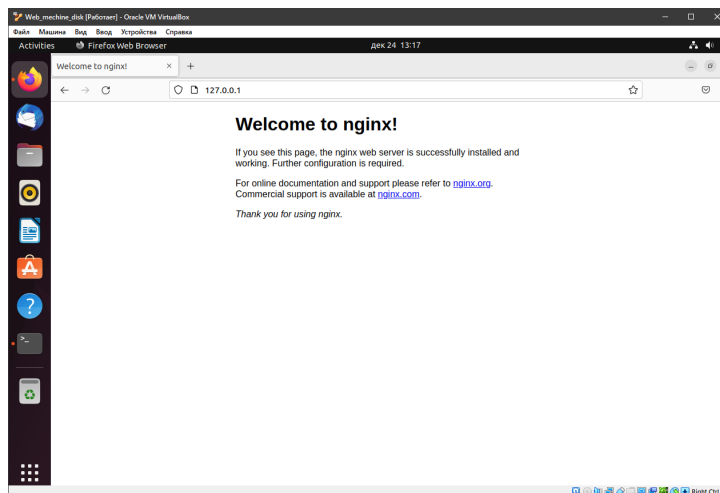


Установка прошла успешно, далее пошло автоматическое обновление, (музыка ожидания), после можно приступать к следующему заданию. Дополнительно для своего спокойствия и удобства был засунут в виртуальную машину диск для "двустороннего обмена адекватными способами drug`n`drop и копи-паст".

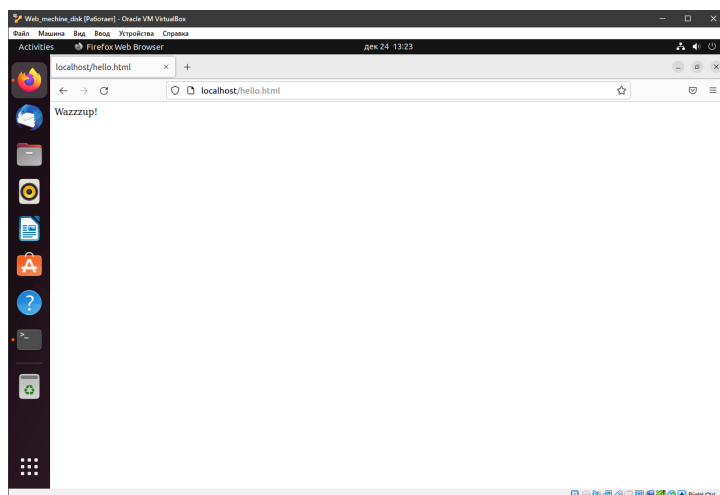
Задание 2: Установите и запустите nginx. Введите в адресной строке браузера `http://localhost` и убедитесь, что nginx показывает приветственную страницу. Найдите ваш запрос к домашней странице в логах nginx.

`sudo apt-get install nginx` #в терминале вводится команда для установки nginx

После установки проверю, что nginx запустился, работает и функционирует по `127.0.0.1` (localhost).

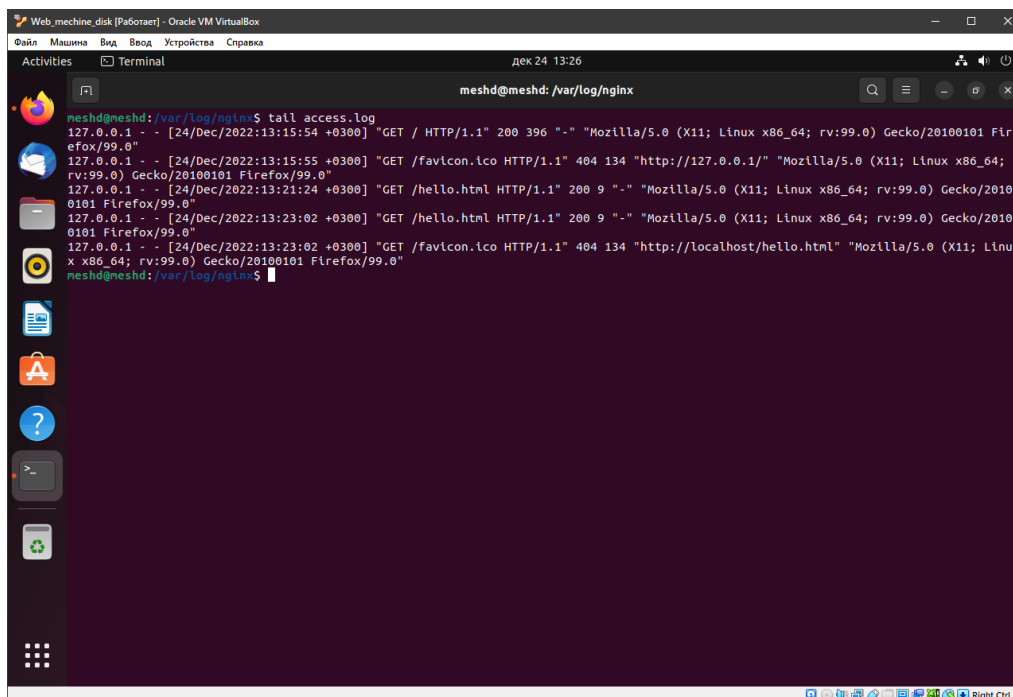


Дополнительно в директории nginx **`/var/www/html`** был создан файл `hello.html` наполнение файла:



Для просмотра логов nginx необходимо перейти в директорию логов:
`cd /var/log/nginx/` #команда для перехода в директорию логов nginx
`tail access.log` #вывод последних 10 строк файла лога.

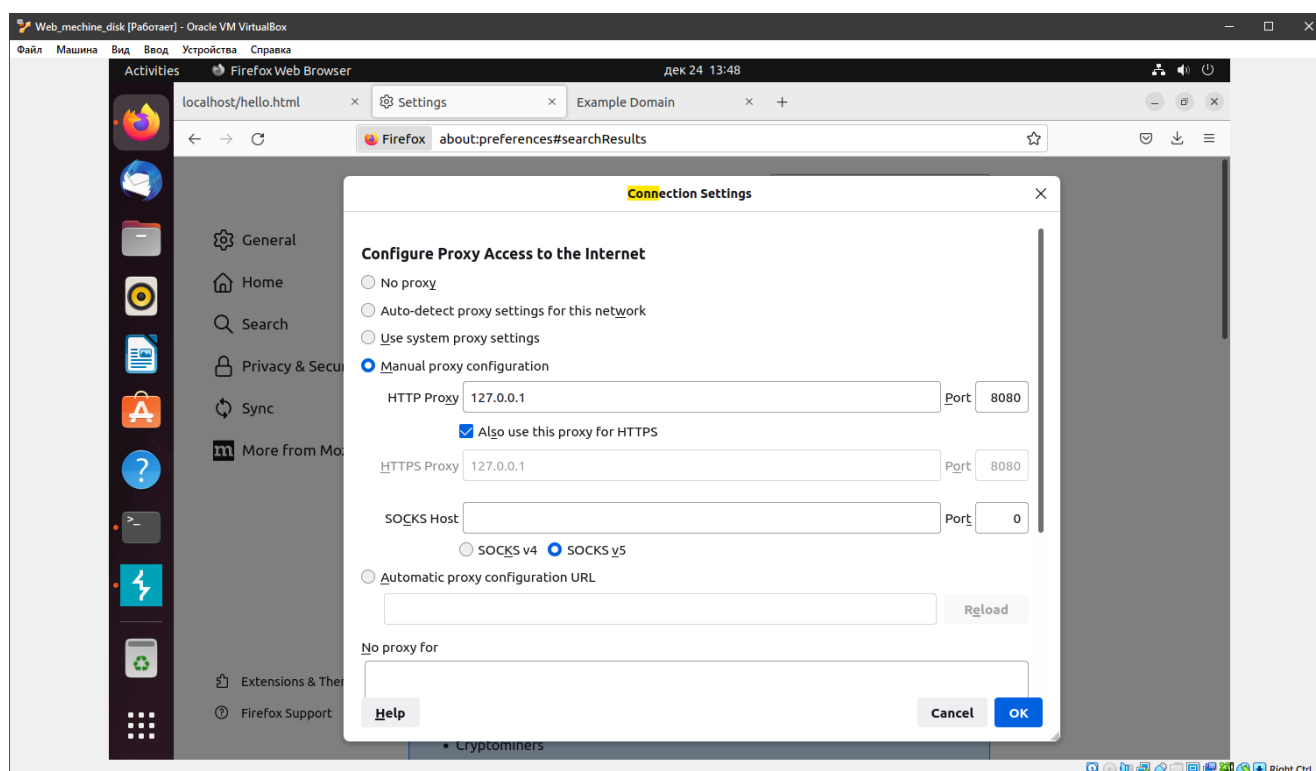
В данном запросе видны строки запросов как по `127.0.0.1` на "главную страницу nginx", так и по `localhost/hello.html`, созданную для тестов и дополнительная информация по данным запросам.



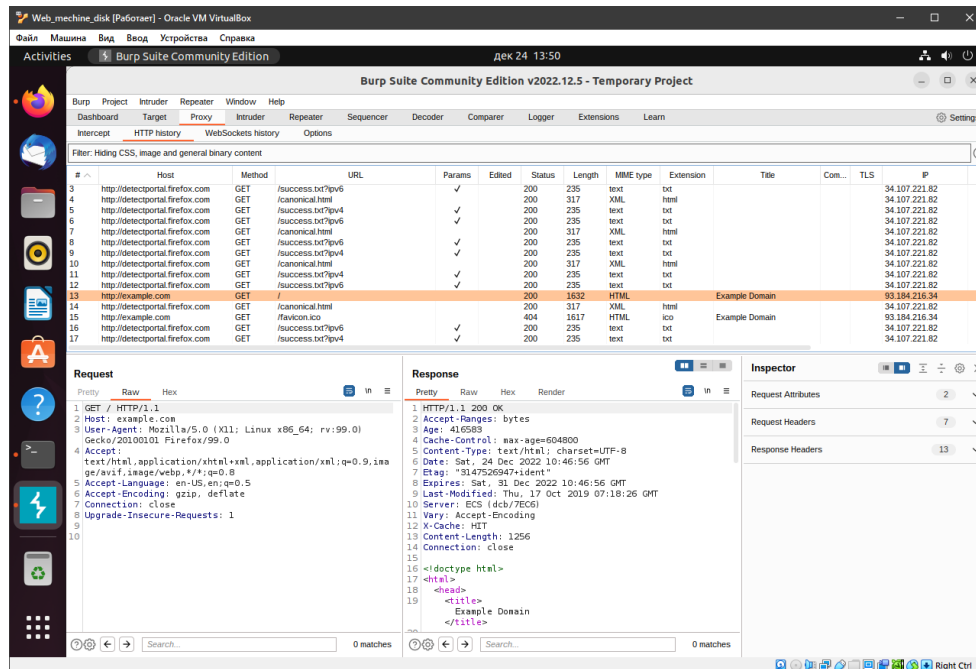
Задание 3*: Установите Burp Suite в качестве прокси. Попробовать основные функции: history, interception, sitemap, repeater.

Устанавливается Burp Suite Community Edition, читается лицензионное соглашение, в данной ситуации можно определёнными репозиториями "расширить" комьюнити версию до энтерпрайза, но нет, далее настраивается браузер для использования бурпа в качестве прокси.

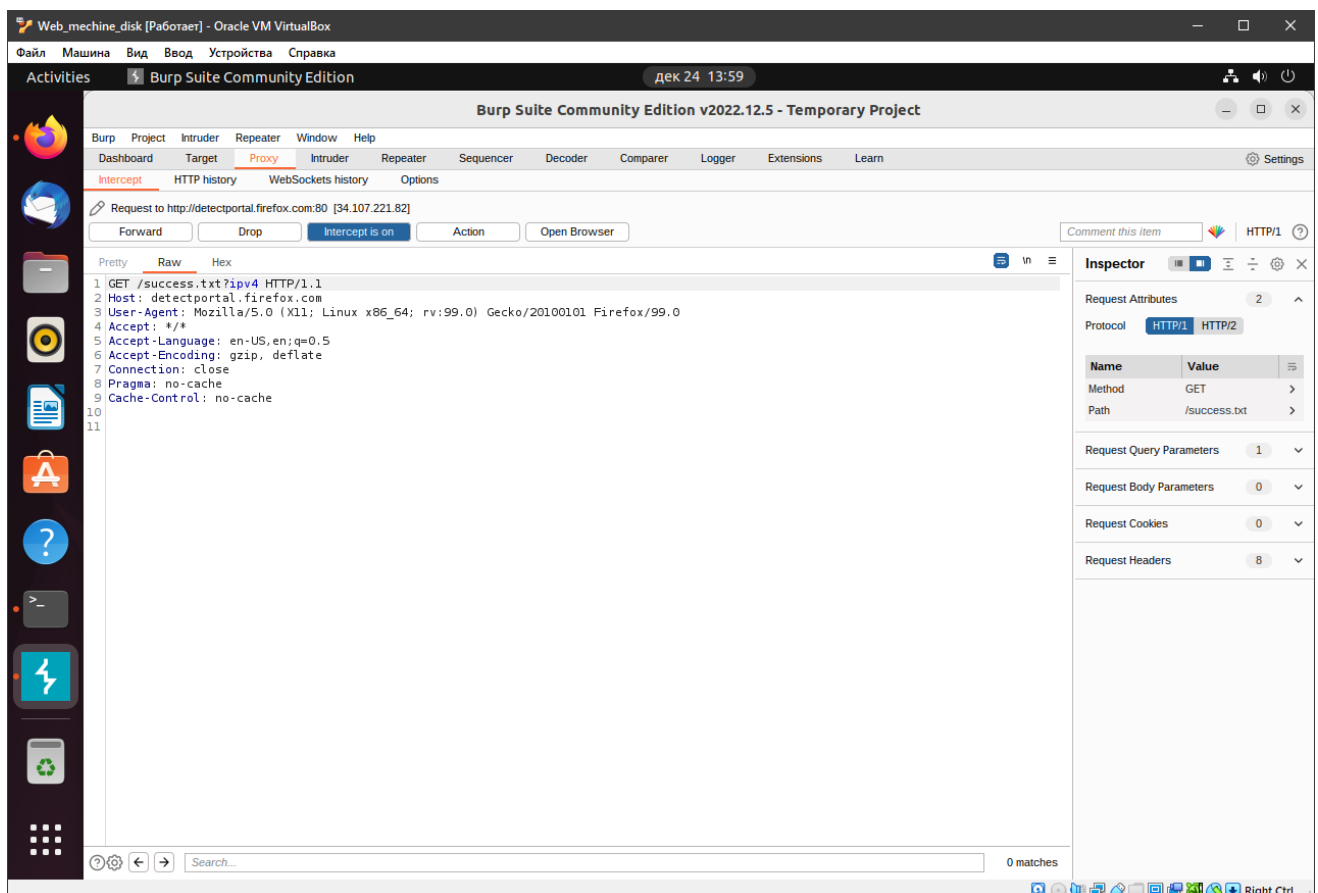
В бурпе создаётся дефолтный временный проект. Далее в браузере по умолчанию Firefox: Settings -> Connection settings -> в открывшемся окне выбирается Manual proxy configuration.



Проверю созданные прокси настройки через открытие сайта **example.com**, данный запрос должен будет отображаться в Burp -> Proxy -> HTTP History. Номер запроса #13 соответствует запросу на **example.com**.

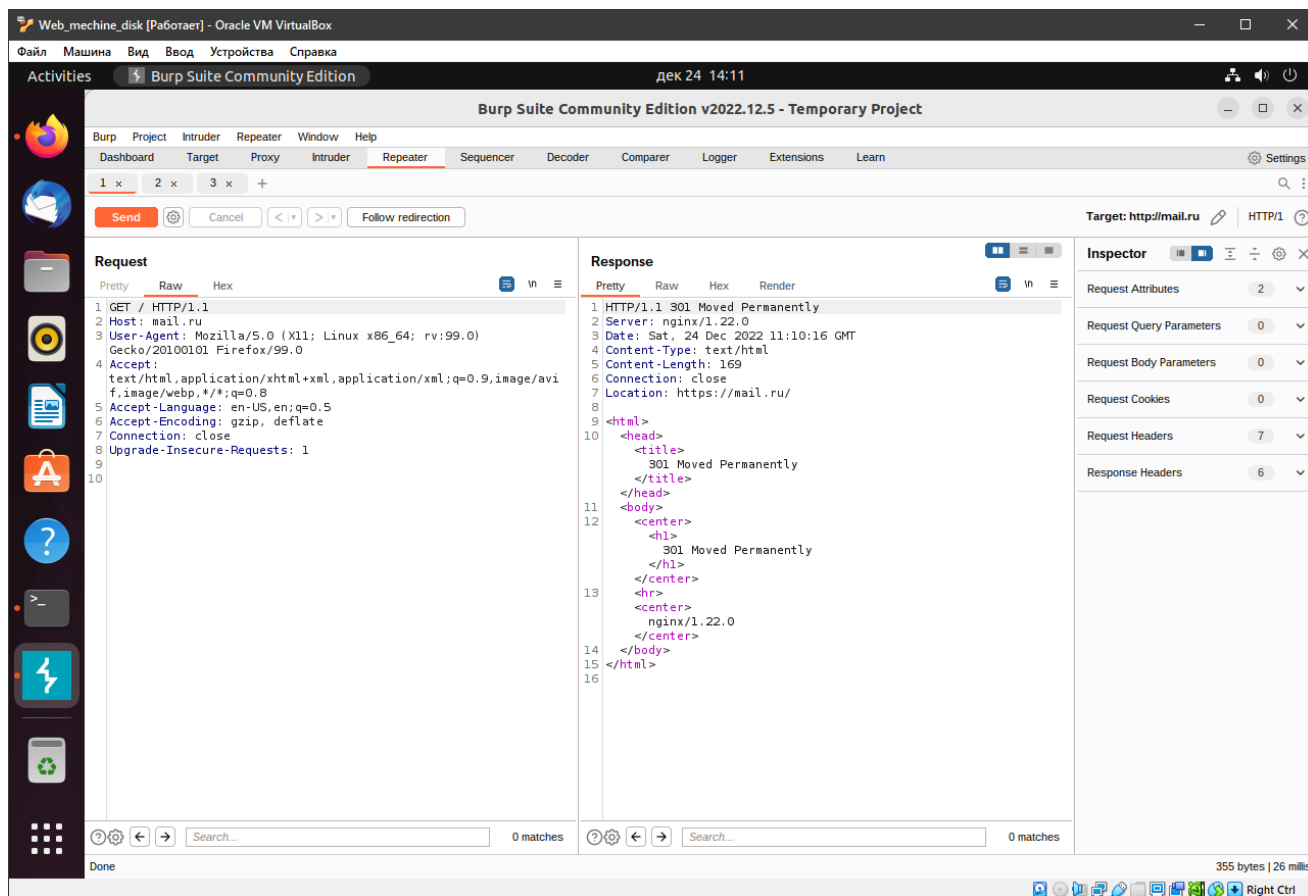


Далее перехват (Интерсер) в бурпе для модификации запроса. В бурпе изначально необходимо включить перехват в прокси: после чего можно попробовать зайти на сайт, например **mail.ru**, сайт с "ходу" не открывается, бурп тормозит пакет от браузера к серверу. Одновременно с этим в бурпе происходит "анализ" исходящего пакета на адрес mail.ru

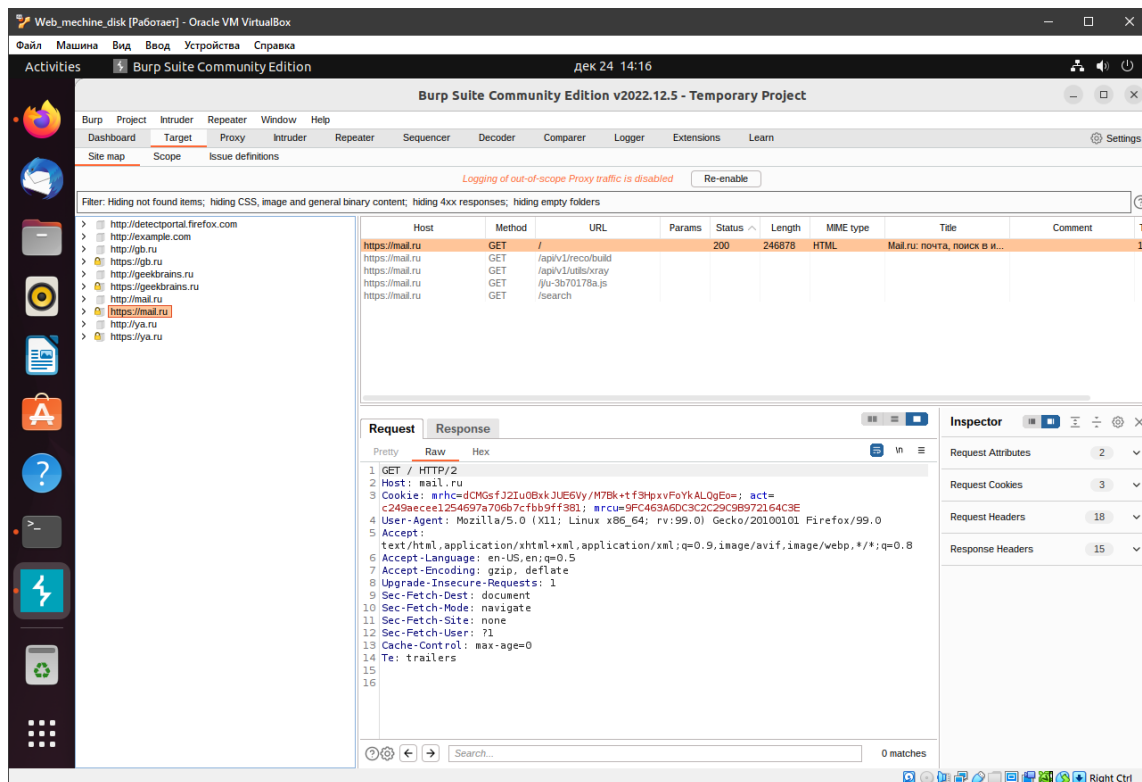


Для отправки пакета можно нажать Forward, что непосредственно отправит пакет, но не пример ответ от сервера, также начав его анализ в бурпе. В данной ситуации mail.ru является весьма нагруженным сайтом, что достаточно тормозит загрузку с перехватом.

Repeater. Ручное изменение и повторение отправки запроса. Для начала отключу перехват и в истории запроса через ПКМ по запросу выберу "Send to Repeater" таким образом можно уже изменённый запрос отправить на сайт и получить ответ. Само изменение запроса происходит в разделе "Repeater" в бурпе. Там же и можно рассмотреть ответ на запрос.



Далее Target. При открытии этого раздела можно видеть запросы, прошедшие через Spider - утилиту бурпа, отображает данный раздел "карту сайта", ссылки с которых собирет информацию запрос.



С помощью этой утилиты/раздела Target можно добавлять определённые сайты, и уже в Score выбирать, включать/отключать определённые условия для отслеживания бурпом.