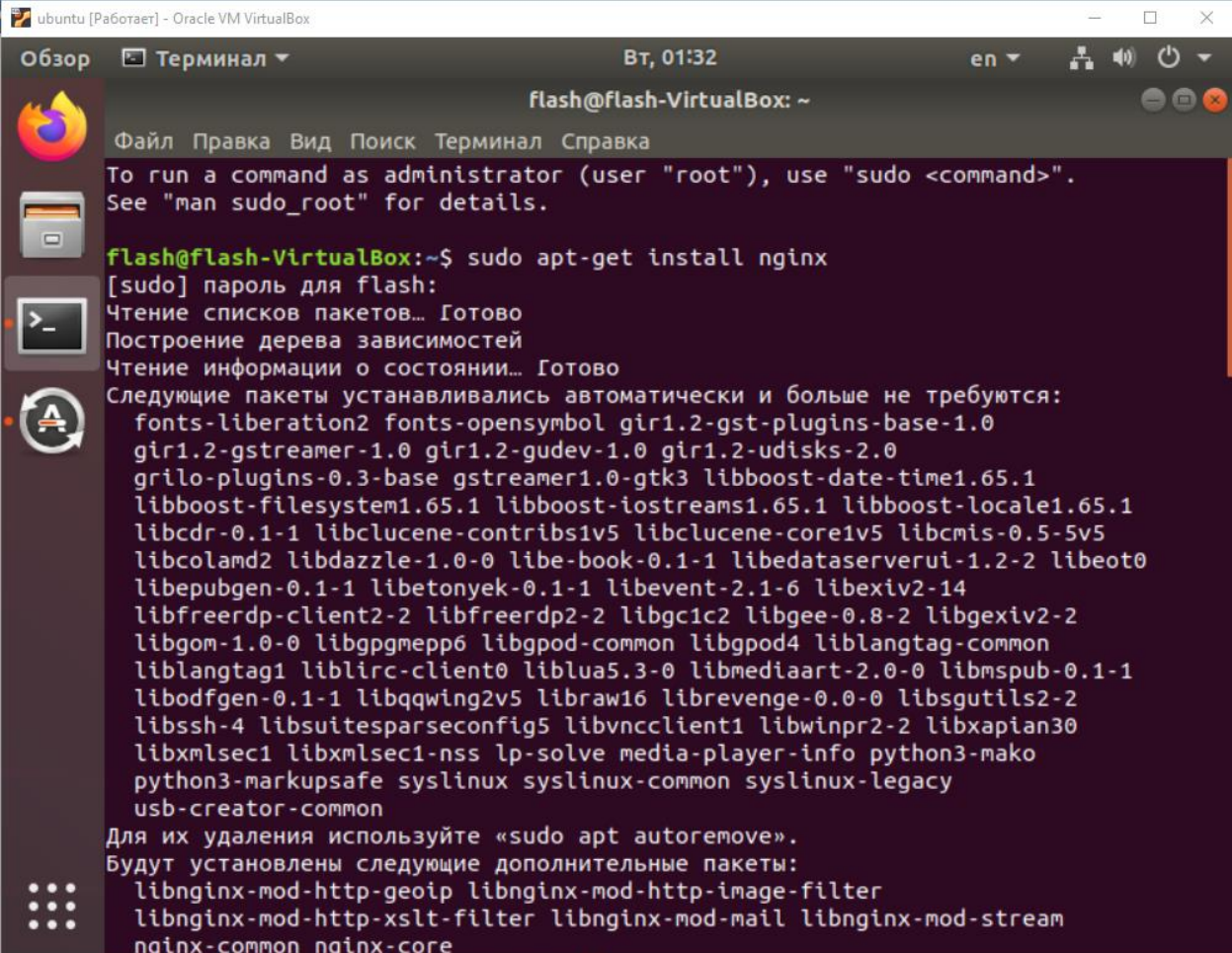
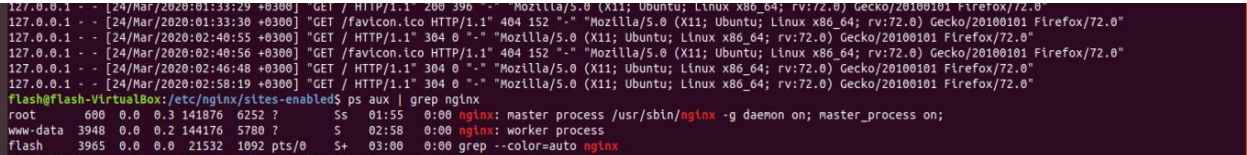


1. VirtualBox и Ubuntu установлены



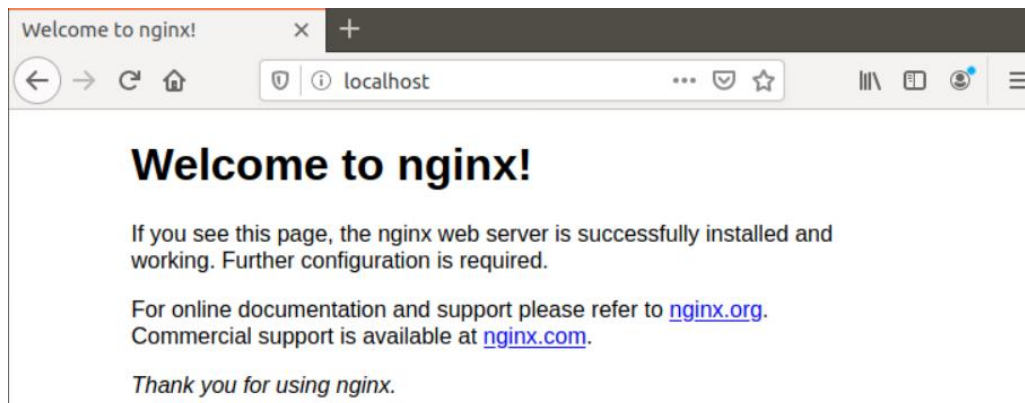
```
flash@flash-VirtualBox: ~  
Файл Правка Вид Поиск Терминал Справка  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
flash@flash-VirtualBox:~$ sudo apt-get install nginx  
[sudo] пароль для flash:  
Чтение списков пакетов... Готово  
Построение дерева зависимостей  
Чтение информации о состоянии... Готово  
Следующие пакеты устанавливались автоматически и больше не требуются:  
fonts-liberation2 fonts-opensymbol gir1.2-gst-plugins-base-1.0  
gir1.2-gstreamer-1.0 gir1.2-gudev-1.0 gir1.2-udisks-2.0  
grilo-plugins-0.3-base gstreamer1.0-gtk3 libboost-date-time1.65.1  
libboost-filesystem1.65.1 libboost-iostreams1.65.1 libboost-locale1.65.1  
libcdr-0.1-1 libclucene-contribs1v5 libclucene-core1v5 libcmis-0.5-5v5  
libcolamd2 libdazzle-1.0-0 libe-book-0.1-1 libdataserverui-1.2-2 libeat0  
libepubgen-0.1-1 libetonyek-0.1-1 libevent-2.1-6 libexiv2-14  
libfreerdp-client2-2 libfreerdp2-2 libgc1c2 libgee-0.8-2 libgexiv2-2  
libgom-1.0-0 libgpgmepp6 libgpod-common libgpod4 liblangtag-common  
liblangtag1 liblirc-client0 liblua5.3-0 libmediaart-2.0-0 libmspub-0.1-1  
libodfgen-0.1-1 libqwing2v5 libraw16 librevenge-0.0-0 libsgutils2-2  
libssh-4 libsuitesparseconfig5 libvncclient1 libwinpr2-2 libxapian30  
libxmlsec1 libxmlsec1-nss lp-solve media-player-info python3-mako  
python3-markupsafe syslinux syslinux-common syslinux-legacy  
usb-creator-common  
Для их удаления используйте «sudo apt autoremove».  
Будут установлены следующие дополнительные пакеты:  
libnginx-mod-http-geoip libnginx-mod-http-image-filter  
libnginx-mod-http-xslt-filter libnginx-mod-mail libnginx-mod-stream  
nginx-common nginx-core
```

2. Сервер Nginx установлен и запущен, на что указывает вывод команды ps aux | grep nginx



```
flash@flash-VirtualBox:~$ ps aux | grep nginx  
root      680  0.0  0.3 141876 6252 ?        Ss   01:55   0:00 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;  
www-data 3948  0.0  0.2 144176 5780 ?        S    02:58   0:00 nginx: worker process  
flash    3965  0.0  0.0 21532 1892 pts/0    S+   03:00   0:00 grep --color=auto nginx
```

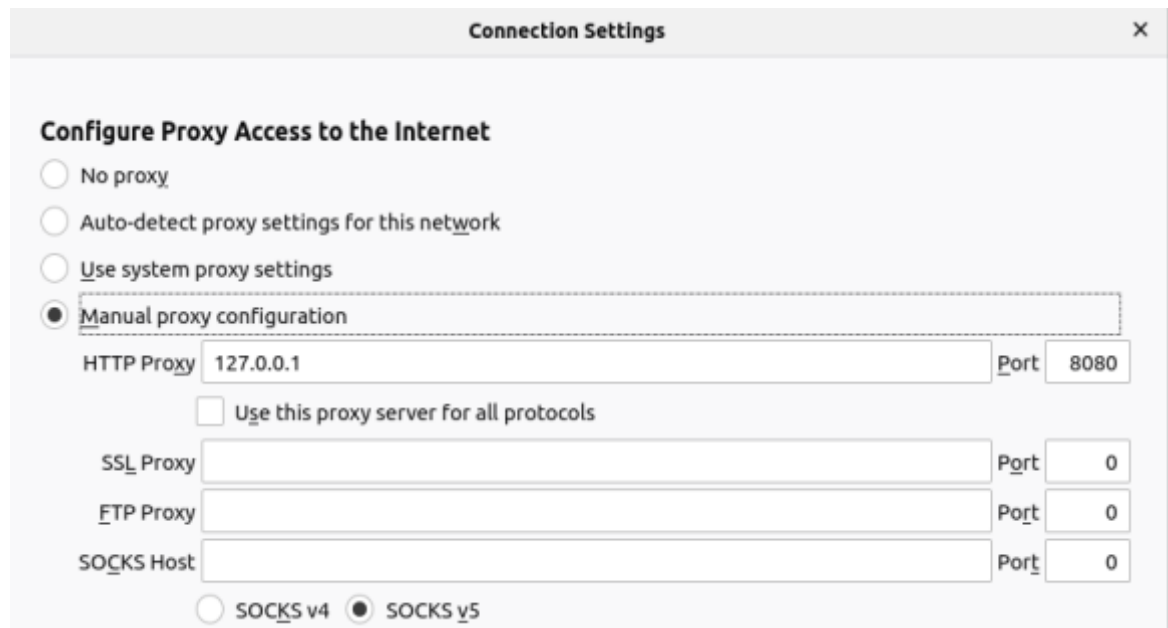
А также ответ браузера после ввода в адресной строке <http://localhost>, показывается домашняя страница Nginx



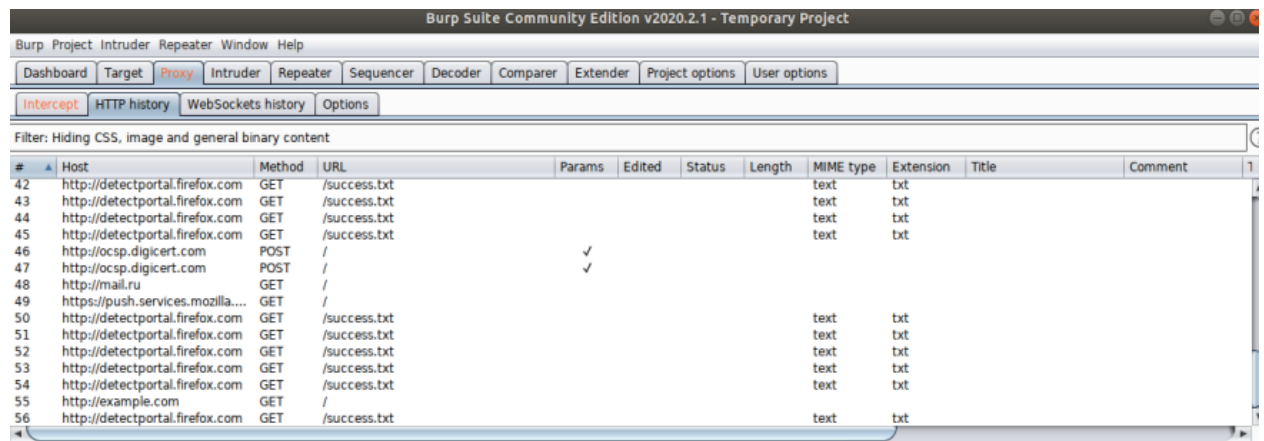
Последние записи в файле access.log показывают, что мы обращались к серверу с запросом домашней страницы

```
127.0.0.1 - [24/Mar/2020:02:40:55 +0300] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0"
127.0.0.1 - [24/Mar/2020:02:40:56 +0300] "GET /favicon.ico HTTP/1.1" 404 152 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0"
127.0.0.1 - [24/Mar/2020:02:46:48 +0300] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0"
127.0.0.1 - [24/Mar/2020:02:58:19 +0300] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0"
Flash@Flash-VirtualBox: /etc/nginx/sites-enabled$ tail /var/log/nginx/access.log
127.0.0.1 - [24/Mar/2020:01:33:29 +0300] "GET / HTTP/1.1" 200 396 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0"
127.0.0.1 - [24/Mar/2020:01:33:30 +0300] "GET /favicon.ico HTTP/1.1" 404 152 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0"
127.0.0.1 - [24/Mar/2020:02:40:55 +0300] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0"
127.0.0.1 - [24/Mar/2020:02:40:56 +0300] "GET /favicon.ico HTTP/1.1" 404 152 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0"
127.0.0.1 - [24/Mar/2020:02:46:48 +0300] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0"
127.0.0.1 - [24/Mar/2020:02:58:19 +0300] "GET / HTTP/1.1" 304 0 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101 Firefox/72.0"
Flash@Flash-VirtualBox: /etc/nginx/sites-enabled$
```

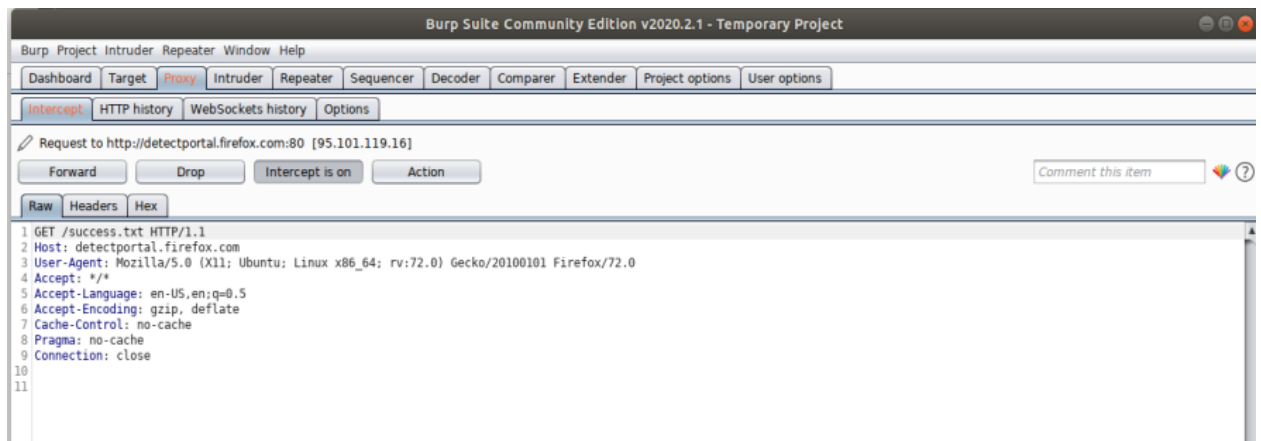
3. Burp Suite установлен и в настройках браузера указаны адрес и порт прокси-сервера



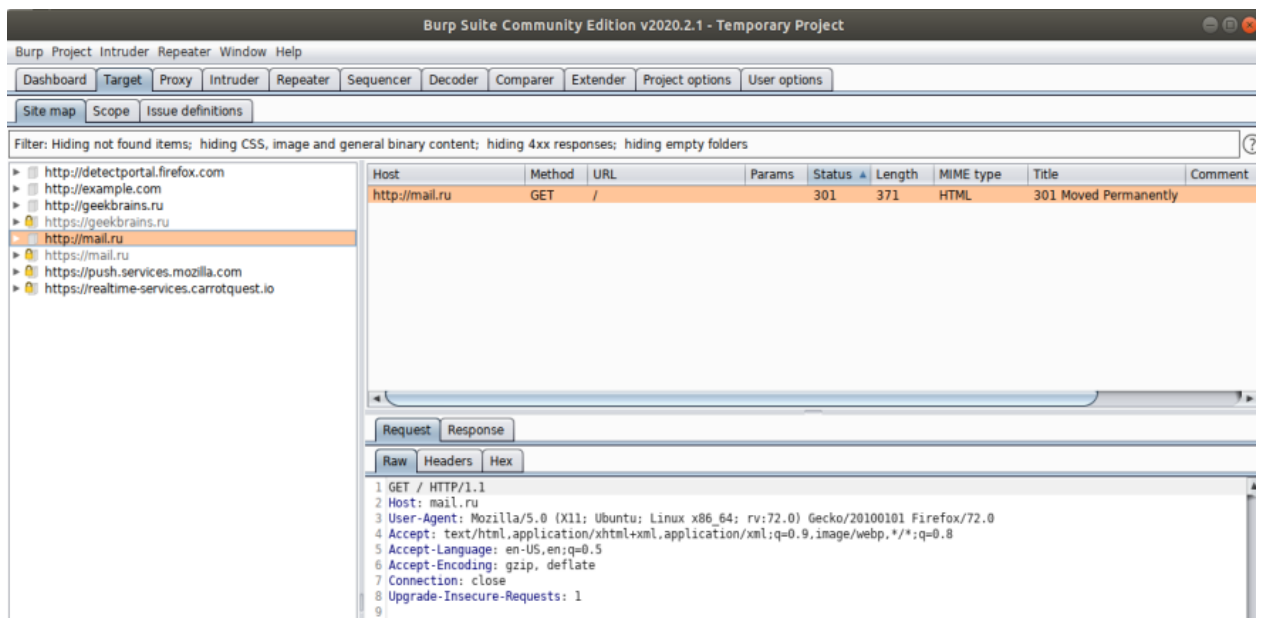
Функция history показывает историю HTTP запросов



Функция interception перехватывает запрос и ждет дальнейших указаний пользователя, что с этим запросом делать (отправить как есть, модифицировать и отправить, либо не отправлять)



Функция sitemap отображает посещенные страницы, позволяет добавить в score и в дальнейшем выставлять фильтр по интересующим нас сайтам



Функция repeater позволяет многократно отправлять запросы и тут же наблюдать ответ сервера, скопировать заголовки можно из истории путем нажатия правой клавишей и выбора пункта Send to Repeater

The screenshot displays the Burp Suite Community Edition v2020.2.1 interface, specifically the Repeater tab. The top menu bar includes options like Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, and User options. The Repeater tab is active, showing a list of requests and responses. The left pane displays the 'Request' tab with a raw HTTP GET request to example.com. The right pane displays the 'Response' tab with a raw HTTP 200 OK response from example.com. The response includes various headers and an HTML body with CSS styles.

Request

```
1 GET / HTTP/1.1
2 Host: example.com
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:72.0) Gecko/20100101
  Firefox/72.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Response

```
1 HTTP/1.1 200 OK
2 Accept-Ranges: bytes
3 Age: 375227
4 Cache-Control: max-age=604800
5 Content-Type: text/html; charset=UTF-8
6 Date: Mon, 23 Mar 2020 23:21:22 GMT
7 Etag: "3147526947"
8 Expires: Mon, 30 Mar 2020 23:21:22 GMT
9 Last-Modified: Thu, 17 Oct 2019 07:18:26 GMT
10 Server: ECS (nyb/ID2C)
11 Vary: Accept-Encoding
12 X-Cache: HIT
13 Content-Length: 1256
14 Connection: close
15
16 <!doctype html>
17 <html>
18 <head>
19   <title>Example Domain</title>
20
21   <meta charset="utf-8" />
22   <meta http-equiv="Content-type" content="text/html; charset=utf-8" />
23   <meta name="viewport" content="width=device-width, initial-scale=1" />
24   <style type="text/css">
25     body {
26       background-color: #f0f0f2;
27       margin: 0;
28       padding: 0;
29       font-family: -apple-system, system-ui, BlinkMacSystemFont, "Segoe UI",
  "Open Sans", "Helvetica Neue", Helvetica, Arial, sans-serif;
30     }
31   }
32   div {
33     width: 600px;
34     margin: 5em auto;
35     padding: 2em;
36     background-color: #fdfdff;
37     border-radius: 0.5em;
38     box-shadow: 2px 3px 7px rgba(0,0,0,0.02);
39   }
40   a:link, a:visited {
41     color: #38488f;
42     text-decoration: none;
43   }
44   @media (max-width: 700px) {
45     div {
46       margin: 0 auto;
47       width: auto;
48     }
49   }
50
```