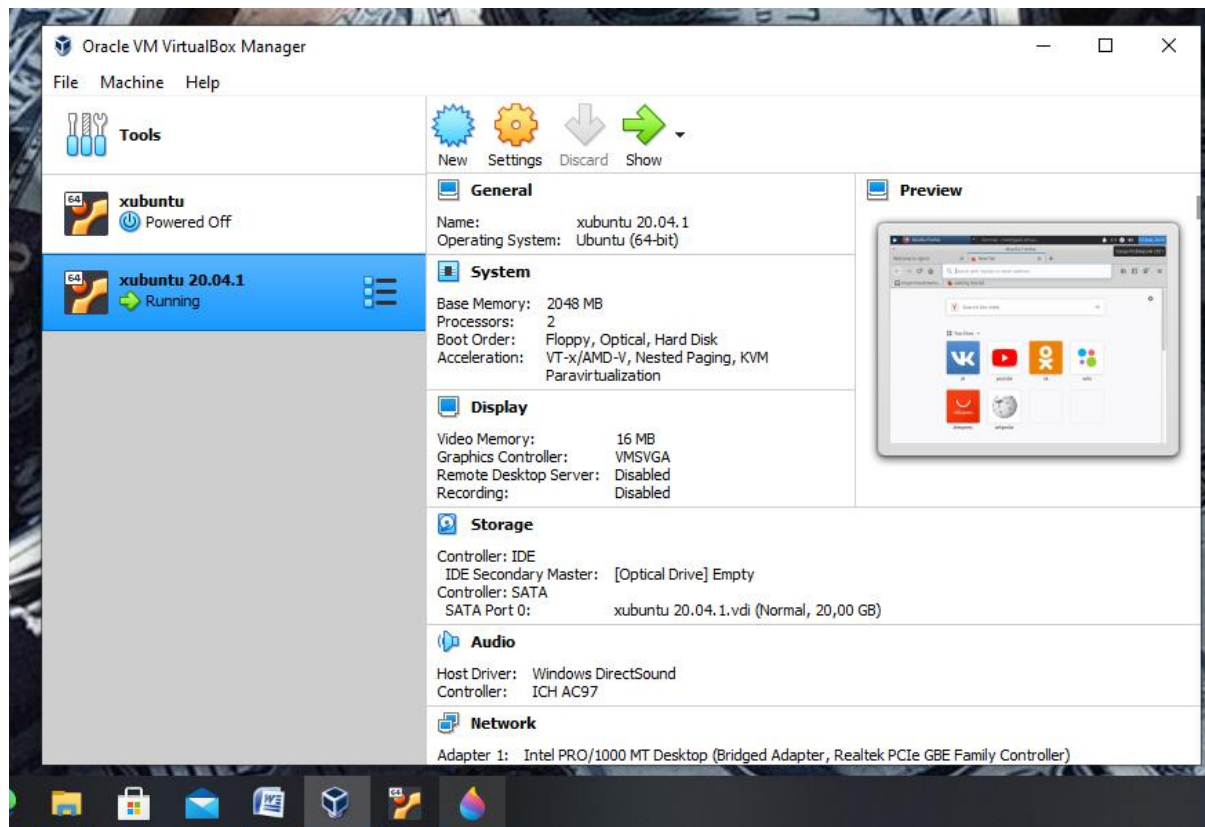


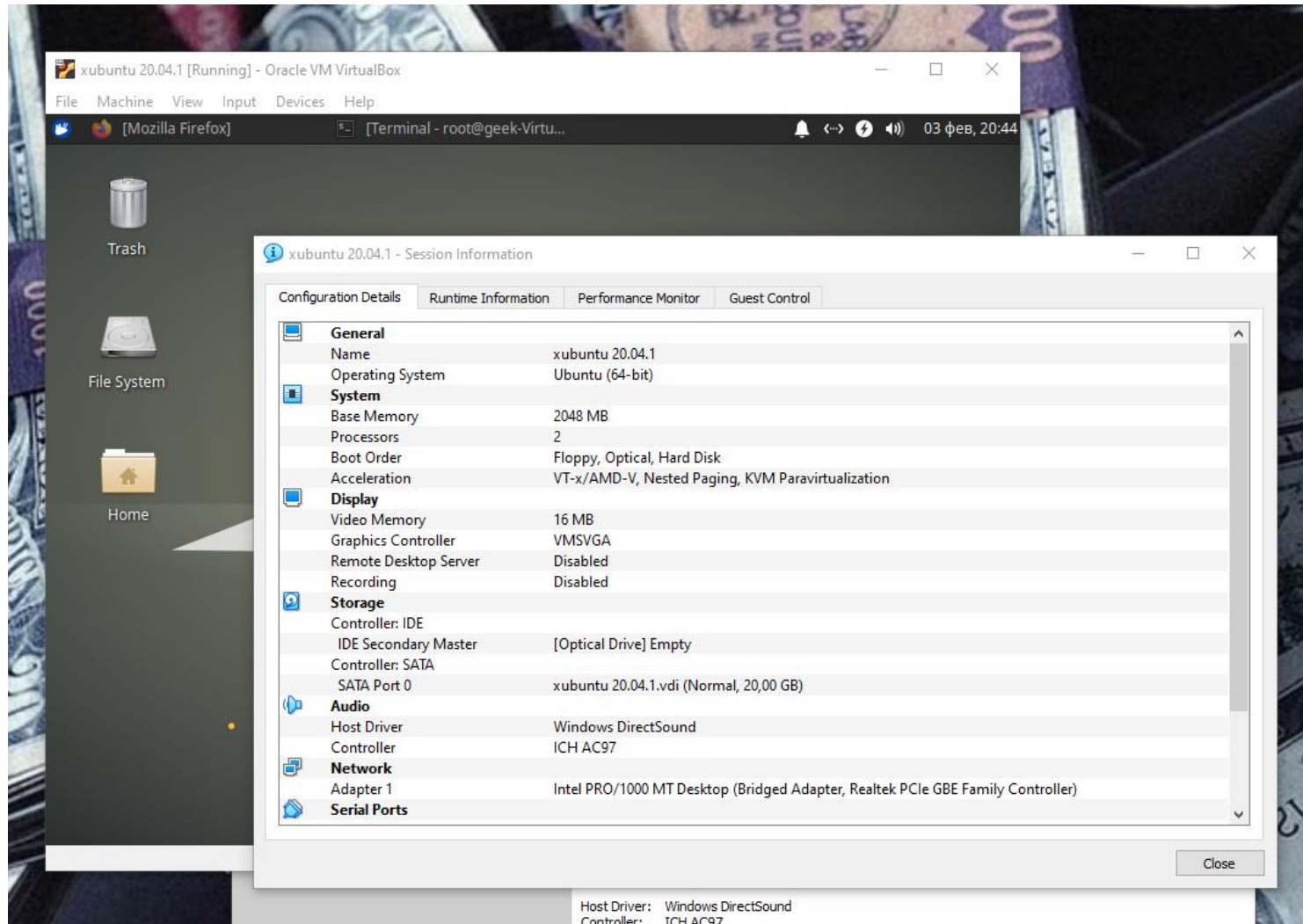
Урок 1.

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

1. Установлен Oracle VM VirtualBox Manager:

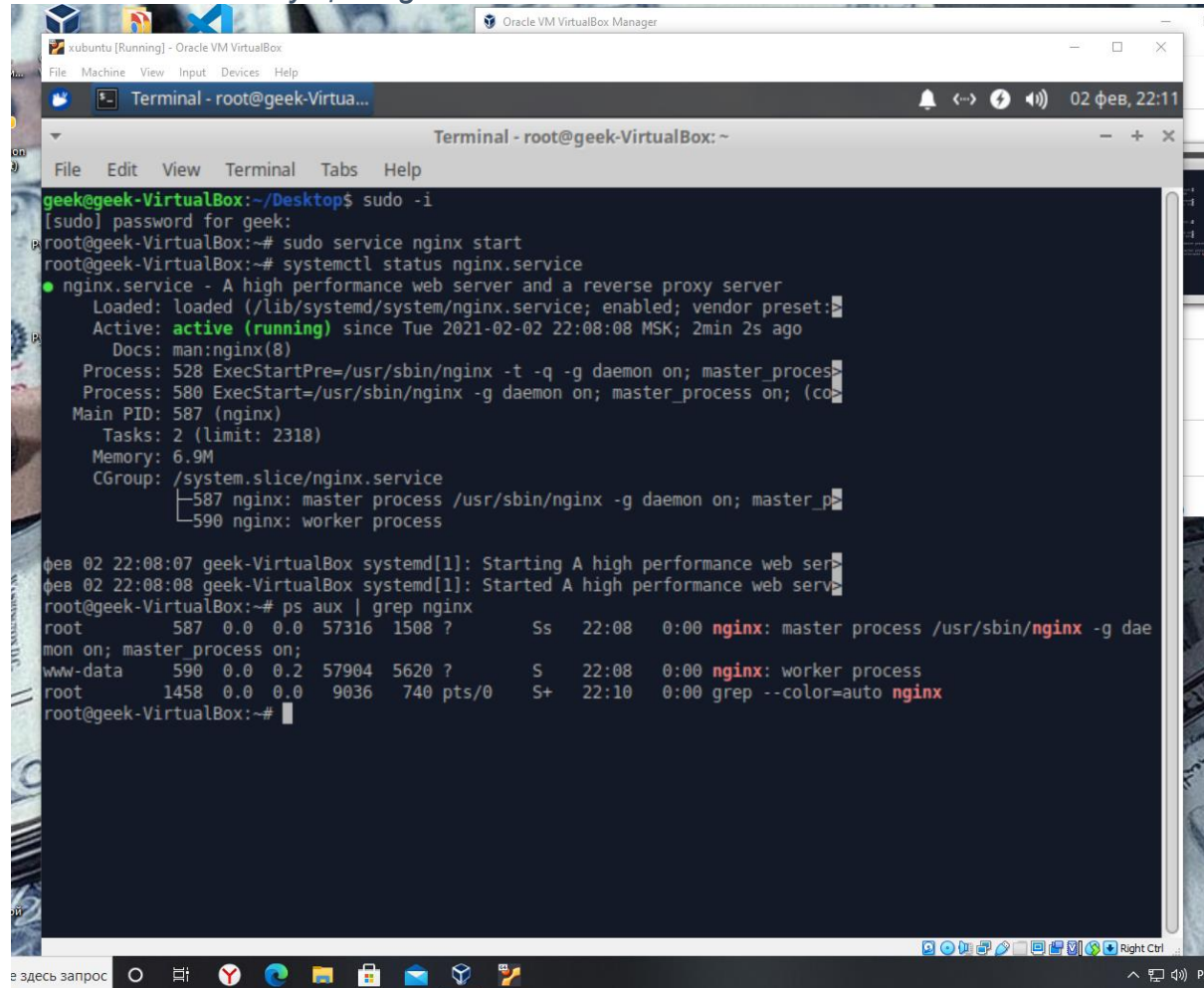


## 2. Установлена виртуальная машина: xubuntu-20.04.1



**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.**

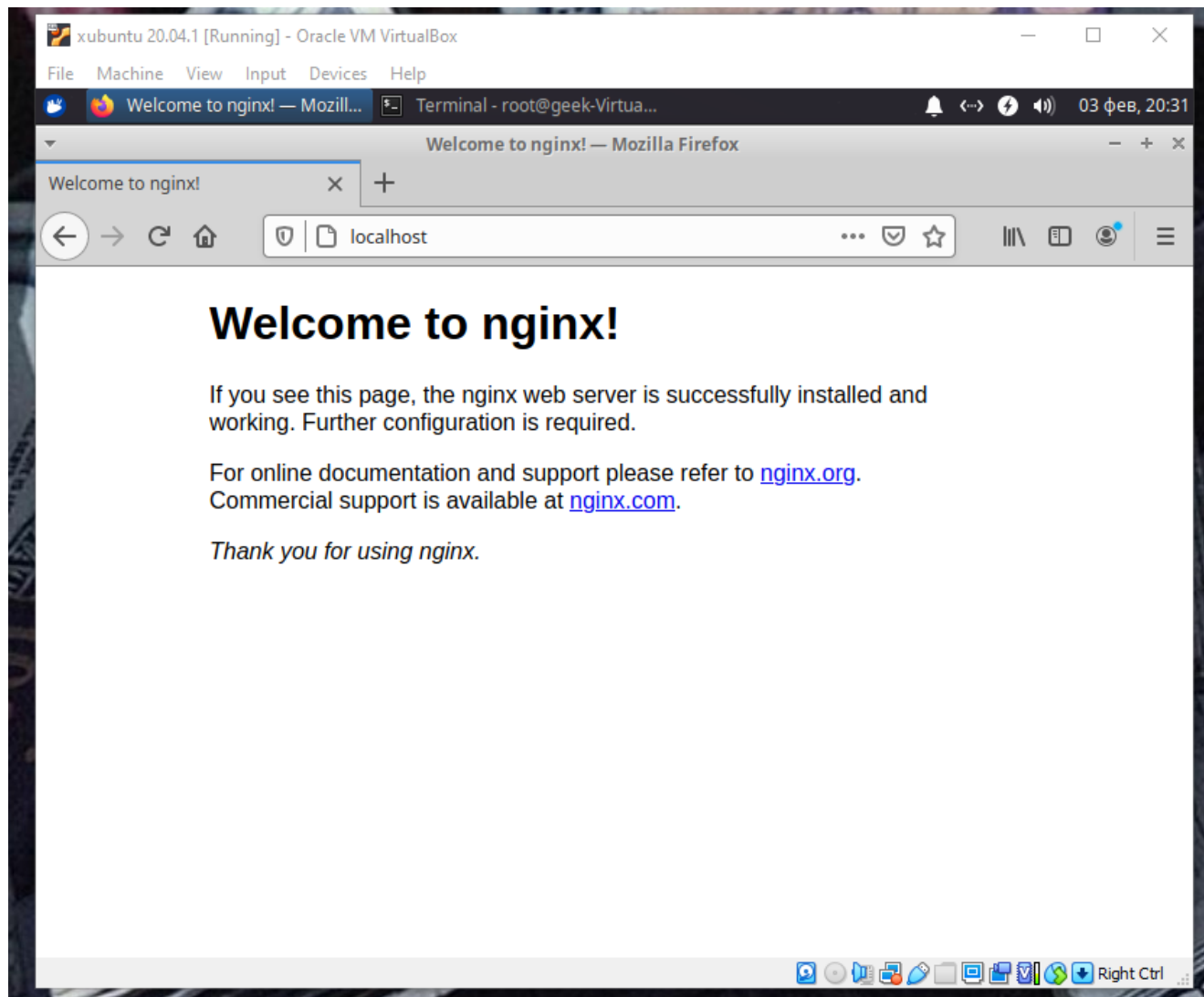
**1. Установлен и запущен nginx:**



```
geek@geek-VirtualBox:~/Desktop$ sudo -i
[sudo] password for geek:
root@geek-VirtualBox:~# sudo service nginx start
root@geek-VirtualBox:~# systemctl status nginx.service
● nginx.service - A high performance web server and a reverse proxy server
   Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2021-02-02 22:08:08 MSK; 2min 2s ago
     Docs: man:nginx(8)
   Process: 528 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=0)
   Process: 580 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=0)
   Main PID: 587 (nginx)
    Tasks: 2 (limit: 2318)
   Memory: 6.9M
   CGroup: /system.slice/nginx.service
           └─587 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
             └─590 nginx: worker process

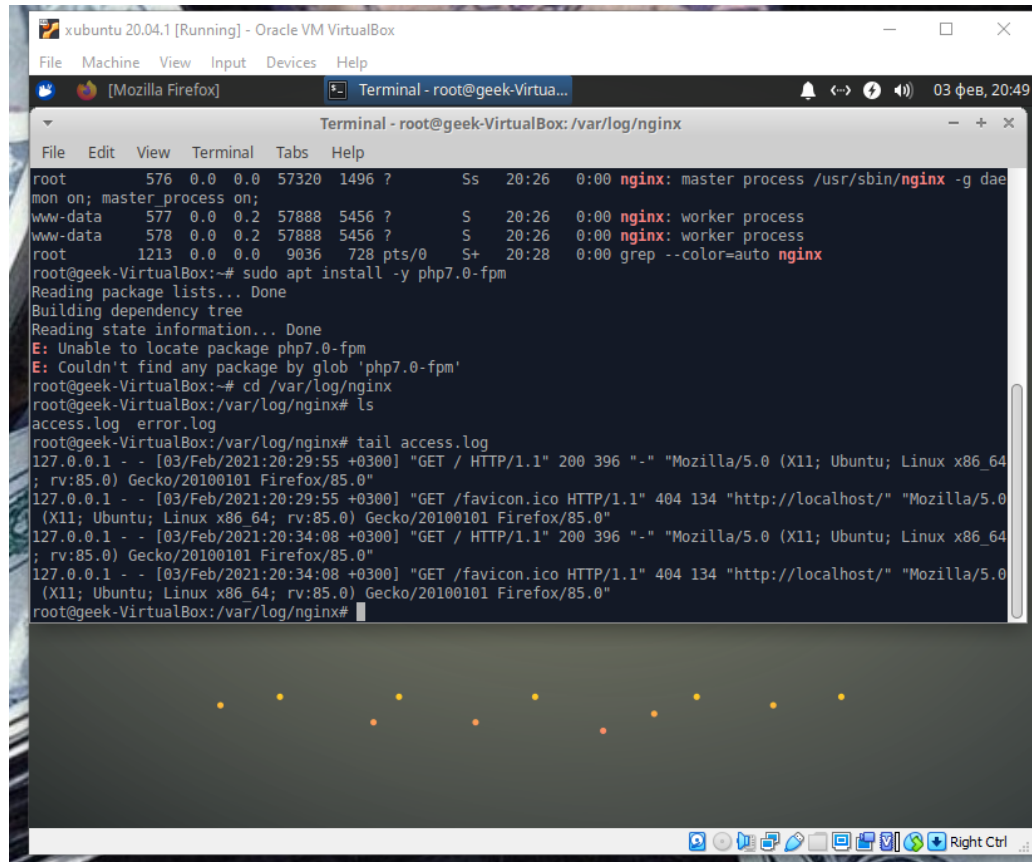
feb 02 22:08:07 geek-VirtualBox systemd[1]: Starting A high performance web server: nginx.
feb 02 22:08:08 geek-VirtualBox systemd[1]: Started A high performance web server: nginx.
root@geek-VirtualBox:~# ps aux | grep nginx
root      587  0.0  0.0  57316  1508 ?        Ss   22:08   0:00 nginx: master process /usr/sbin/nginx -g dae
mon on; master_process on;
www-data  590  0.0  0.2  57904  5620 ?        S    22:08   0:00 nginx: worker process
root     1458  0.0  0.0   9036   740 pts/0    S+   22:10   0:00 grep --color=auto nginx
root@geek-VirtualBox:~#
```

2. Введён в адресной строке браузера <http://localhost> , можно ввести IP-адрес: 127.0.0.1. nginx показывает приветственную страницу.



### 3. Найден наш запрос к домашней странице в логах nginx.

```
127.0.0.1 - - [03/Feb/2021:20:34:08 +0300] "GET /favicon.ico HTTP/1.1" 404 134 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0"
```



The screenshot shows a terminal window titled "Terminal - root@geek-Virtua..." with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal output includes:

```
root@geek-VirtualBox:~# ps -ef | grep nginx
root      576  0.0  0.0  57320 1496 ?        Ss   20:26   0:00 nginx: master process /usr/sbin/nginx -g daem
mon on; master process on;
www-data  577  0.0  0.2  57888 5456 ?        S    20:26   0:00 nginx: worker process
www-data  578  0.0  0.2  57888 5456 ?        S    20:26   0:00 nginx: worker process
root     1213  0.0  0.0   9036  728 pts/0    S+   20:28   0:00 grep --color=auto nginx

root@geek-VirtualBox:~# sudo apt install -y php7.0-fpm
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package php7.0-fpm
E: Couldn't find any package by glob 'php7.0-fpm'

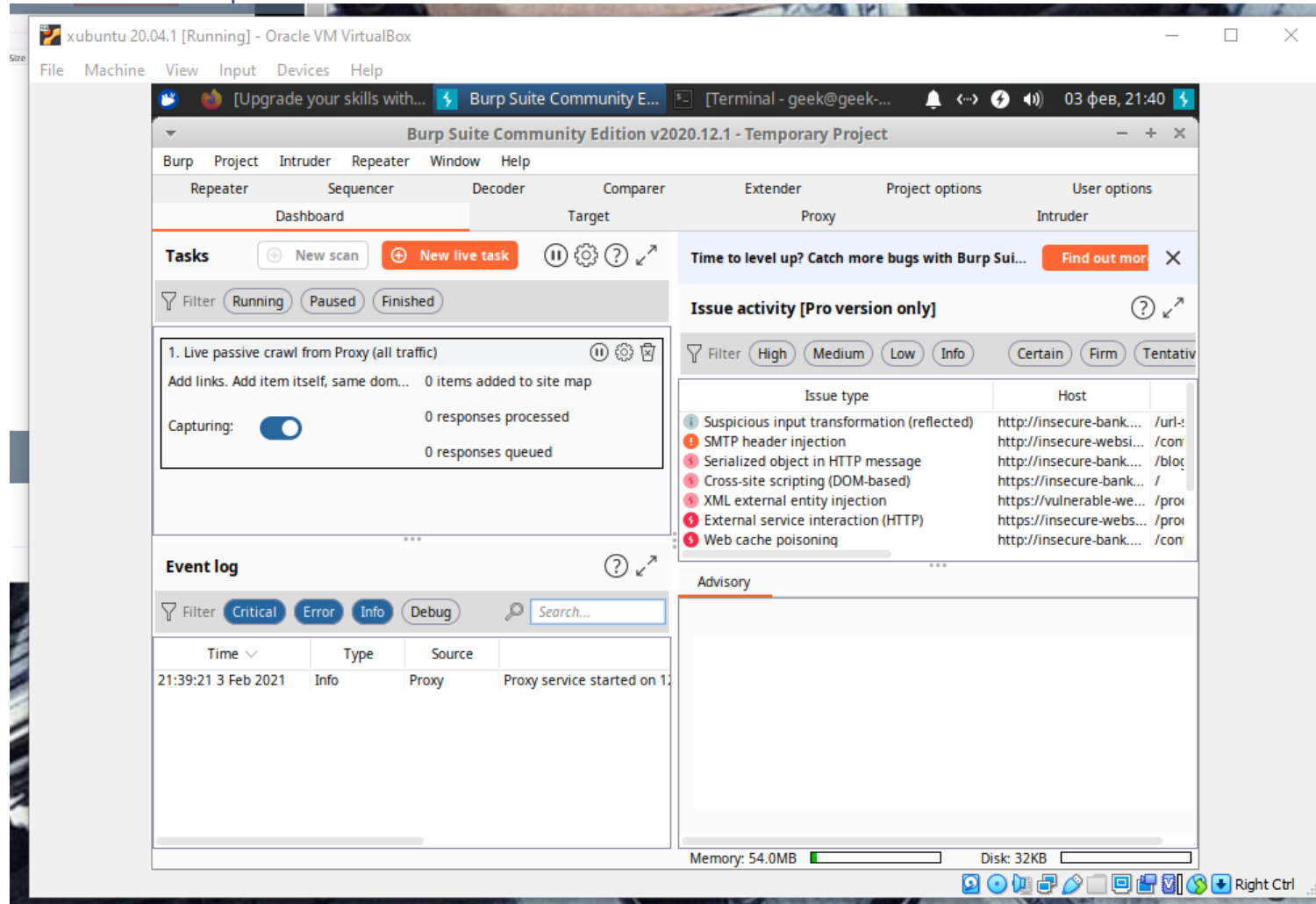
root@geek-VirtualBox:~# cd /var/log/nginx
root@geek-VirtualBox:/var/log/nginx# ls
access.log  error.log

root@geek-VirtualBox:/var/log/nginx# tail access.log
127.0.0.1 - - [03/Feb/2021:20:29:55 +0300] "GET / HTTP/1.1" 200 396 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0"
127.0.0.1 - - [03/Feb/2021:20:29:55 +0300] "GET /favicon.ico HTTP/1.1" 404 134 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0"
127.0.0.1 - - [03/Feb/2021:20:34:08 +0300] "GET / HTTP/1.1" 200 396 "-" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0"
127.0.0.1 - - [03/Feb/2021:20:34:08 +0300] "GET /favicon.ico HTTP/1.1" 404 134 "http://localhost/" "Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:85.0) Gecko/20100101 Firefox/85.0"

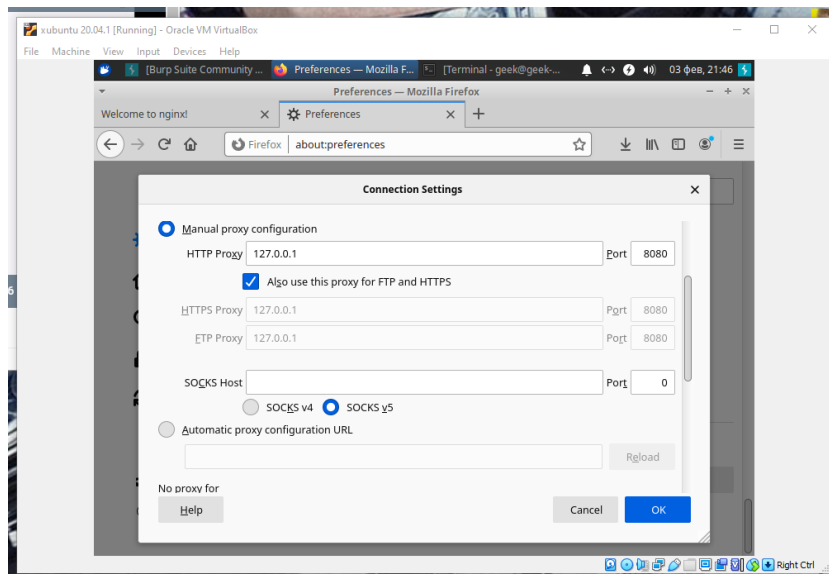
root@geek-VirtualBox:/var/log/nginx#
```

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

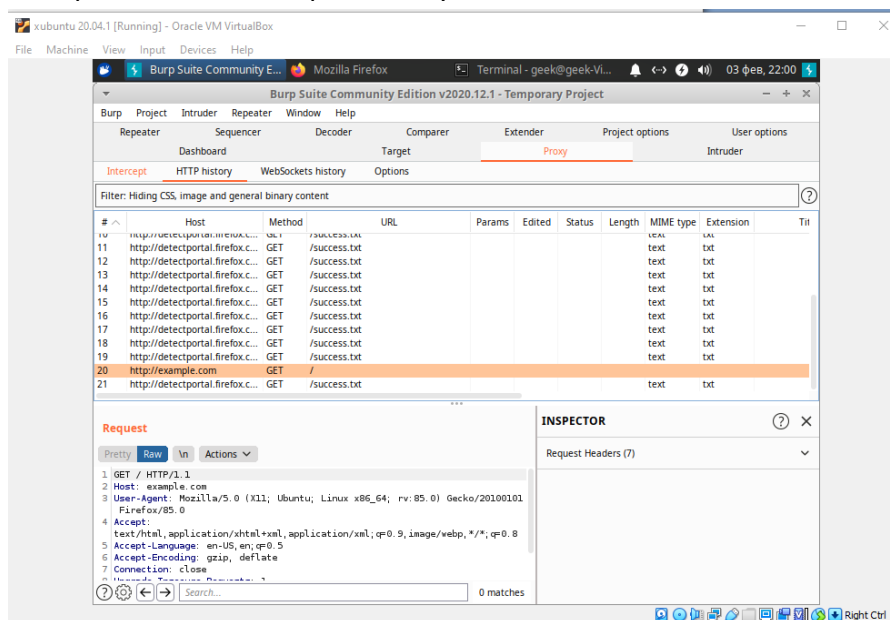
1. Установлен Burp Suite:



2. Открыл Firefox и настроил его так, что бы он использовал Вурп в качестве прокси.

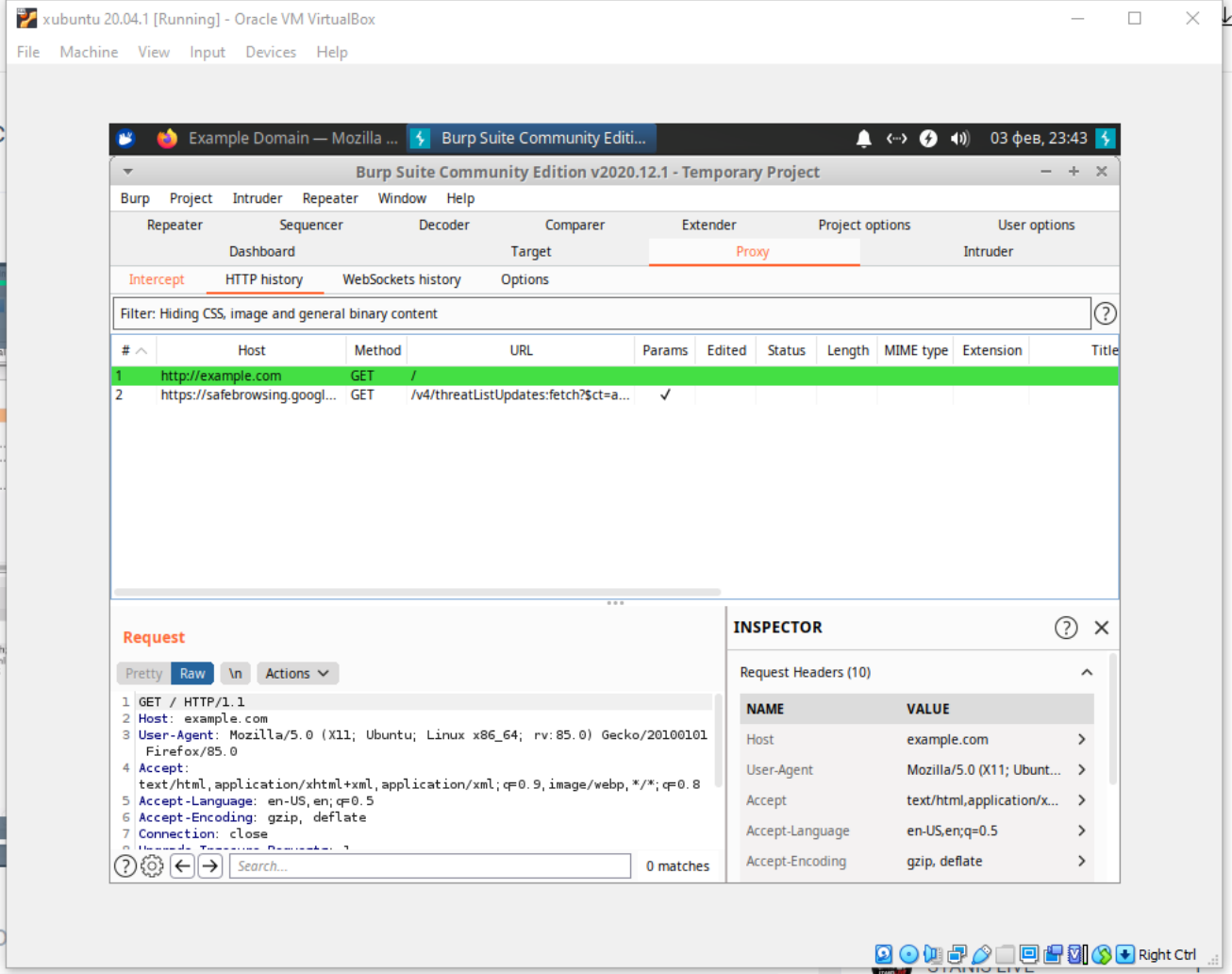


3. В Вурп был сделан запрос и получен ответ:





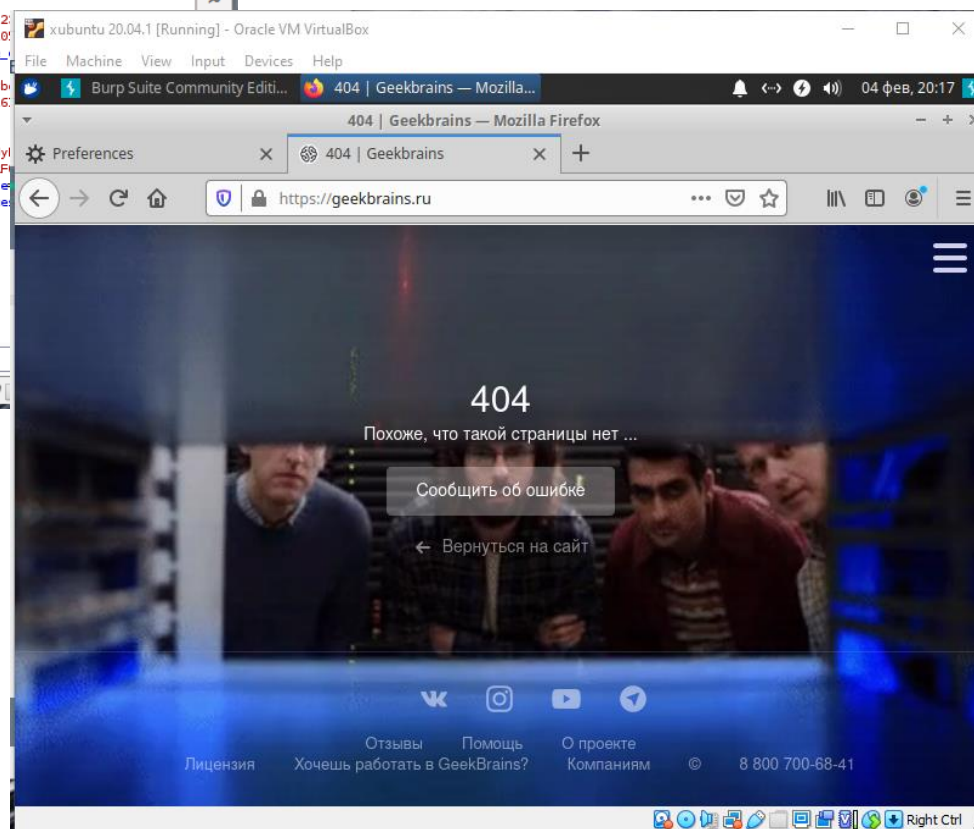
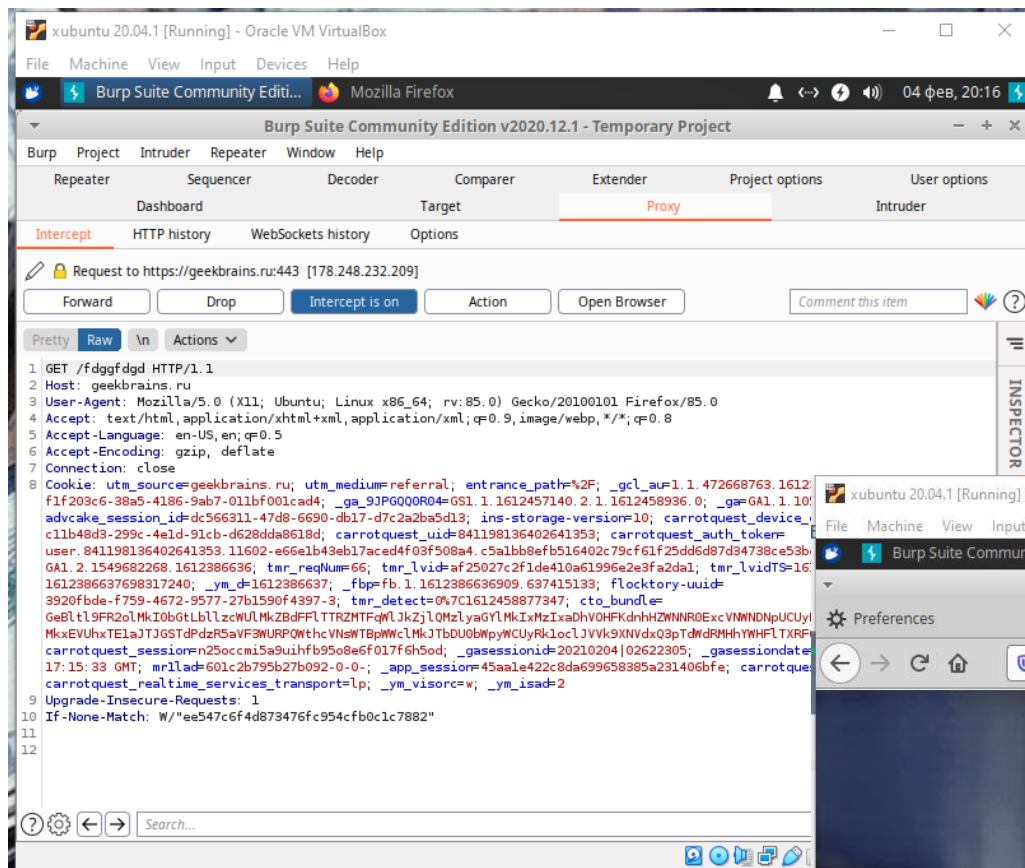
4. Функция: **history.**





## 5. Функция: **interception**.

Модифицирован запрос (дописан набор букв) и перенаправлен этот запрос. Такой страницы нет, введен не валидный URL и GeekBrains его не смог найти.



## 6. Функция: sitemap.

xubuntu 20.04.1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Burp Suite Community Edition v2020.12.1 - Temporary Project

Repeater Sequencer Decoder Comparer Extender Project options User options

Dashboard Target Proxy Intruder

Site map Scope Issue definitions

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Stat...	Length	MIME type
https://googleads.g.doubleclick.net						
https://gum.criteo.com						
https://hit.api.useinsider.com						
https://ib.adnxs.com						
https://incoming.telemetry.mozilla.org						
https://mc.admetrica.ru						
https://mc.yandex.ru						
https://portal-xiva.yandex.net						
https://push.services.mozilla.com						
https://realtime-services-chat-1.carrotquest.a						
https://recommender-eu.scarabresearch.com						
https://redirect.frontend.weborama.fr						
https://sslwidget.criteo.com						
https://static.ads-twitter.com						
https://stats.g.doubleclick.net						
https://strm.yandex.ru						
https://suggest.yandex.com						
https://sync.1dmp.io						
https://top-fwz1.mail.ru						
https://vertis-frontent.s3.yandex.net						
https://webchannel-content.eservice.emarsys						
https://www.google-analytics.com						
https://www.googleadservices.com						
https://www.googletagmanager.com						
https://www.yandex.ru						
https://yabs.yandex.ru						
http://yandex.ru						
chat						

Request

1 GET / HTTP/1.1

2 Host: yandex.ru

3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:85.0) Gecko/20100101 Firefox/85.0

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

Response

евралья, четверг 21:26 Сделать стартов

Санкт-Петербург Коронавирус

снятие ограничений по COVID-19 в М

беспечит иммунитет от коронавируса

итерии оценки эффективности работы

акционированной акции арестован муж

INSPECTOR

0 matches

Right Ctrl

## 7. Функция: repeater.

xubuntu 20.04.1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 x ...

Send Cancel < >

Target: <https://geekbrains.ru>

**Request**

Pretty Raw \n Actions

```
1 GET /ghsvg-defs.svg HTTP/1.1
2 Host: geekbrains.ru
3 User-Agent: Mozilla/5.0 (X11;
  Ubuntu; Linux x86_64; rv:85.0)
  Gecko/20100101 Firefox/85.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: https://geekbrains.ru/
9 Cookie: utm_source=geekbrains.ru;
  utm_medium=referral; entrance_path
  =%2F; _gcl_auf
  1.1.472668763.1612386530; gbwsuid=
  f1f203c6-38a5-4186-9ab7-011bf001ca
  d4; _ga_9JPGQQ0R04=
  GS1.1.1612457140.2.1.1612458872.0;
  _ga=GA1.1.1056870094.1612386634;
  advcake_session_id=
  dc566311-47d8-6690-db17-d7c2a2ba5d
  13; ins-storage-version=9;
  carrotquest_device_guid=
  c11b48d3-299c-4e1d-91cb-d628dda861
  d;
```

**Response**

Pretty Raw Render \n Actions

```
1 HTTP/1.1 404 Not Found
2 Server: QRATOR
3 Date: Thu, 04 Feb 2021 17:31:04
  GMT
4 Content-Type: text/html
5 Connection: close
6 Vary: Accept-Encoding
7 ETag: W/"5f318221-7da7"
8 Strict-Transport-Security:
  max-age=15724800
9 Content-Length: 32167
10
11 <!doctype html>
12 <html lang="">
13 <head>
14 <!-- Google Tag Manager -->
15 <script>
16 (function(w, d, s, l, i) {
17   w[l] = w[l] || [];
18   w[l].push({
19     'gtm.start': new Date().
  getTime(),
20     event: 'gtm.js'
21   });
22 })
```

**INSPECTOR**

NAME VALUE

Remove ^ v Add...

Request Cookies (31)

NAME	VALUE
utm_source	geekbrains.ru
utm_medium	referral
entrance_path	/
_gcl_auf	1.1.472668763.161238...
gbwsuid	f1f203c6-38a5-4186-9a...
_ga_9JPGQQ0R04	GS1.1.1612457140.2.1....
_ga	GA1.1.1056870094.161...
advcake_session_id	dc566311-47d8-6690-d...
ins-storage-version	9
carrotquest_device_guid	c11b48d3-299c-4e1d-9...

32,406 bytes | 44 millis

Done

Right Ctrl