Сети, часть 2. Домашнее задание

1. Что будет, если удалить /etc/hosts?
   Ответ: В Linux существует файл /etc/nsswitch.conf, строка hosts, которая определяет, где ОС будет запрашивать ip адрес нужного ресурса по доменному имени при необходимости.

```
➜ ~  cat /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         files systemd
group:          files systemd
shadow:         files
gshadow:        files

hosts:          files mdns4_minimal [NOTFOUND=return] dns mymachines
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files
```

   В моем случае первым делом система пойдет в **files**, в /etc/hosts. Если там нет нужной записи, то далее идет **mdns4_minimal**, который пытается разрешить имя с использованием параллельного (multicast) DNS. **[NOTFOUND=return]** означает, что любой ответ notfound, предшествующий процессу mdns4_minimal, должен считаться значимым (авторитетным) и что система не будет пытаться продолжать искать ответ. **dns** запись означает запрос имён у DNS серверов(адреса dns серверов лежат в /etc/resolv.conf). **Mymachines** означает, что если домен совпадает с именем хоста, с которого идет запрос, то сразу же вернется ip адрес машины.
   Таким образом, если мы удалим файл /etc/hosts, то ОС пойдет искать записи дальше по цепочке.

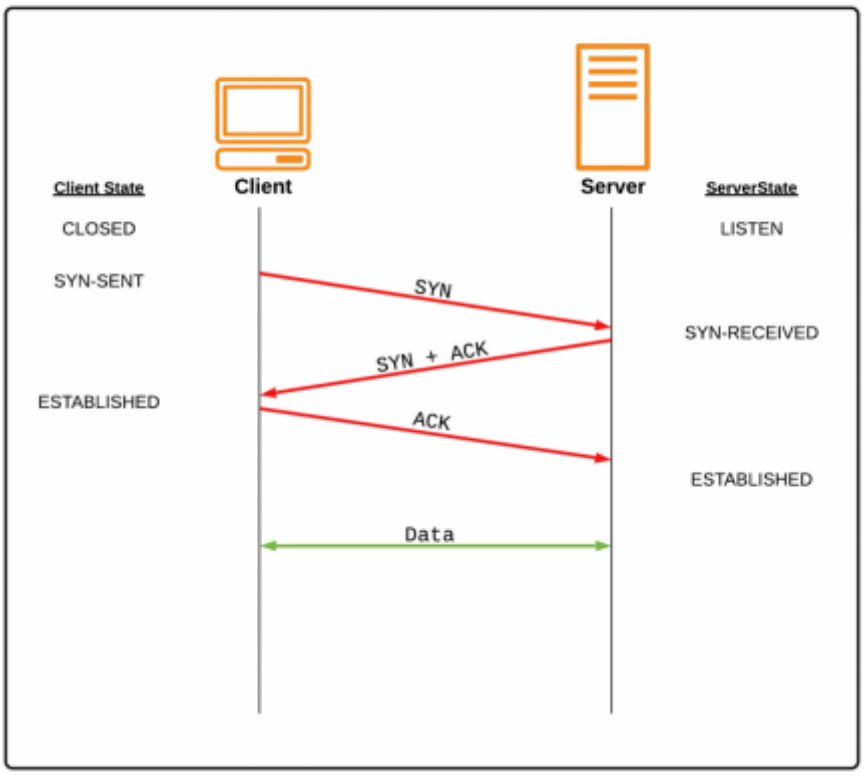
2. Сколько запросов делает ваш DNS resolver, чтобы определить адрес www.google.co.jp (http://www.google.co.jp)?
   Ответ:4 запроса

```
➜  ~  dig www.google.co.jp -4 +trace +nodnssec

; <<>> DiG 9.16.1-Ubuntu <<>> www.google.co.jp -4 +trace +nodnssec
;; global options: +cmd
.                       9228    IN      NS      h.root-servers.net.
.                       9228    IN      NS      e.root-servers.net.
.                       9228    IN      NS      c.root-servers.net.
.                       9228    IN      NS      g.root-servers.net.
.                       9228    IN      NS      k.root-servers.net.
.                       9228    IN      NS      i.root-servers.net.
.                       9228    IN      NS      j.root-servers.net.
.                       9228    IN      NS      m.root-servers.net.
.                       9228    IN      NS      l.root-servers.net.
.                       9228    IN      NS      d.root-servers.net.
.                       9228    IN      NS      a.root-servers.net.
.                       9228    IN      NS      b.root-servers.net.
.                       9228    IN      NS      f.root-servers.net.
;; Received 239 bytes from 192.168.1.1#53(192.168.1.1) in 24 ms

jp.                     172800  IN      NS      e.dns.jp.
jp.                     172800  IN      NS      a.dns.jp.
jp.                     172800  IN      NS      h.dns.jp.
jp.                     172800  IN      NS      f.dns.jp.
jp.                     172800  IN      NS      c.dns.jp.
jp.                     172800  IN      NS      d.dns.jp.
jp.                     172800  IN      NS      b.dns.jp.
jp.                     172800  IN      NS      g.dns.jp.
;; Received 501 bytes from 202.12.27.33#53(m.root-servers.net) in 72 ms

google.co.jp.           86400   IN      NS      ns1.google.com.
google.co.jp.           86400   IN      NS      ns2.google.com.
google.co.jp.           86400   IN      NS      ns3.google.com.
google.co.jp.           86400   IN      NS      ns4.google.com.
;; Received 155 bytes from 150.100.6.8#53(f.dns.jp) in 308 ms

www.google.co.jp.       300     IN      A       74.125.131.94
;; Received 61 bytes from 216.239.34.10#53(ns2.google.com) in 76 ms
```

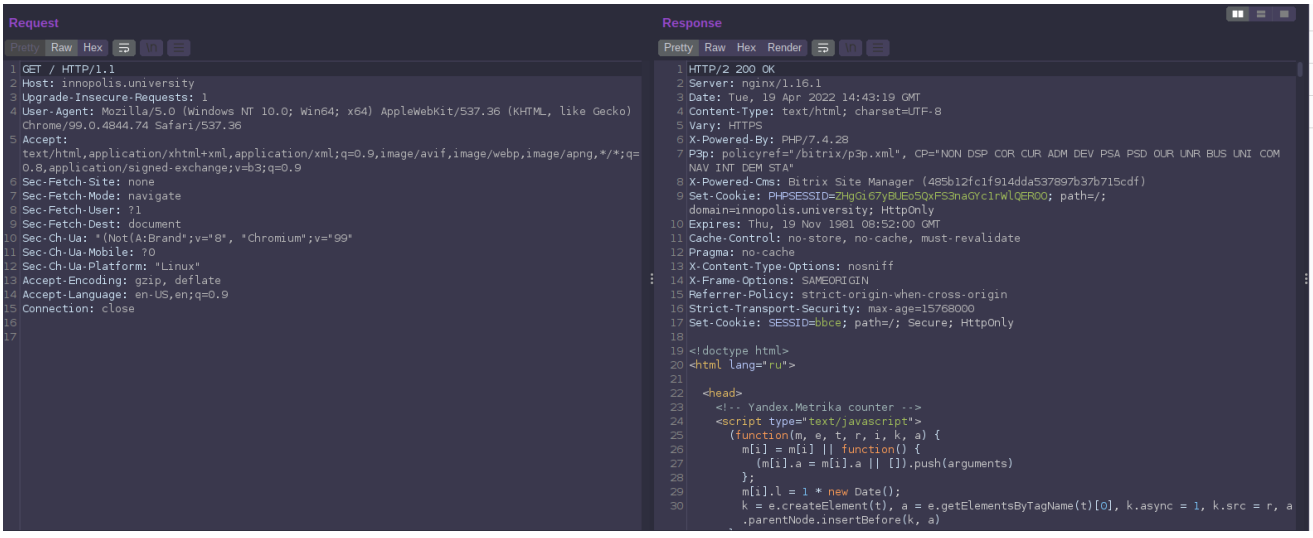
3. Какая SPF запись нужна для моего почтового сервера, чтобы его письма не заблокировали другие почтовые серверы?
   Ответ: Запись в DNS у нашего домена в записи TXT: v=spf1 +all"
   v=spf1 - версия spf, +all - означает, что письма от отправителя в нашем домене не должны блокироваться.

4. Применительно к протоколу http опишите что происходит при открытии в браузере http://innopolis.university (http://innopolis.university). Опишите со всеми подробностями
   Ответ:
   Первым делом ОС должна найти ip адрес сервера через протокол DNS. Порядок поиска описан в первом вопросе.
   Далее, как только браузер знает IP адрес сервера, клиент пытается установить TCP соединение. Все начинается с рукопожатия:

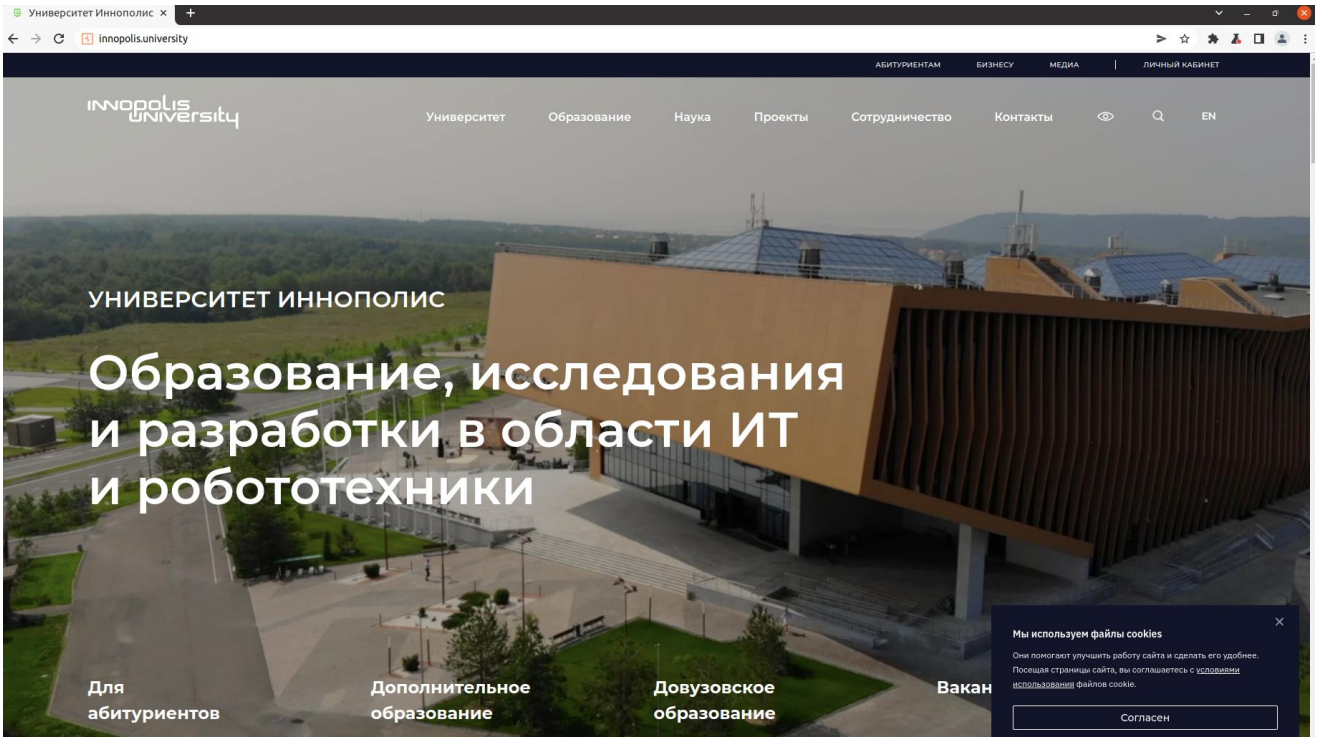
Модель OSI. TCP-handshake



Далее клиент отправляет запрос, в нашем случае метод будет GET со всеми необходимыми заголовками, чтобы сервер мог понять как нужно взаимодействовать с клиентом, в ответ сервер присылает html файл, который уже содержит шрифты, скрипты, картинки и прочий контент, который соответственно подгрузуится через другие запросы.



Ну и в конце само собой, браузер получив весь необходимый контент, отрисовывает страницу сайта Университета Иннополис.



5. Как заблокировать исходящий почтовый трафик со своего компьютера чтобы предотвратить рассылку спама с машины?
   Ответ: Чтобы блокировать весь исходящий траффик, который будет передаваться по протоколу smtp, для этого заблокируем дефолтный порт получателя для smtp, это порт 25, добавим запись в файерволл

```
sudo iptables -A OUTPUT -p tcp --dport 25 -j DROP
```

6. Разверните сервер vsftpd, подробности в практическом задании в секции ftp. Можно приложить лог процесса передачи файла по ftp
   Ответ:
   Все проделал, развернул, перекинул файл на удаленный ftp сервер через put:

```
└─# ftp 192.168.1.18
Connected to 192.168.1.18.
220 (vsFTPd 3.0.3)
Name (192.168.1.18:xokage):
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put Bez_Imeni-1_Kopia.png
local: Bez_Imeni-1_Kopia.png remote: Bez_Imeni-1_Kopia.png
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
202198 bytes sent in 0.02 secs (8.0628 MB/s)
ftp>
```