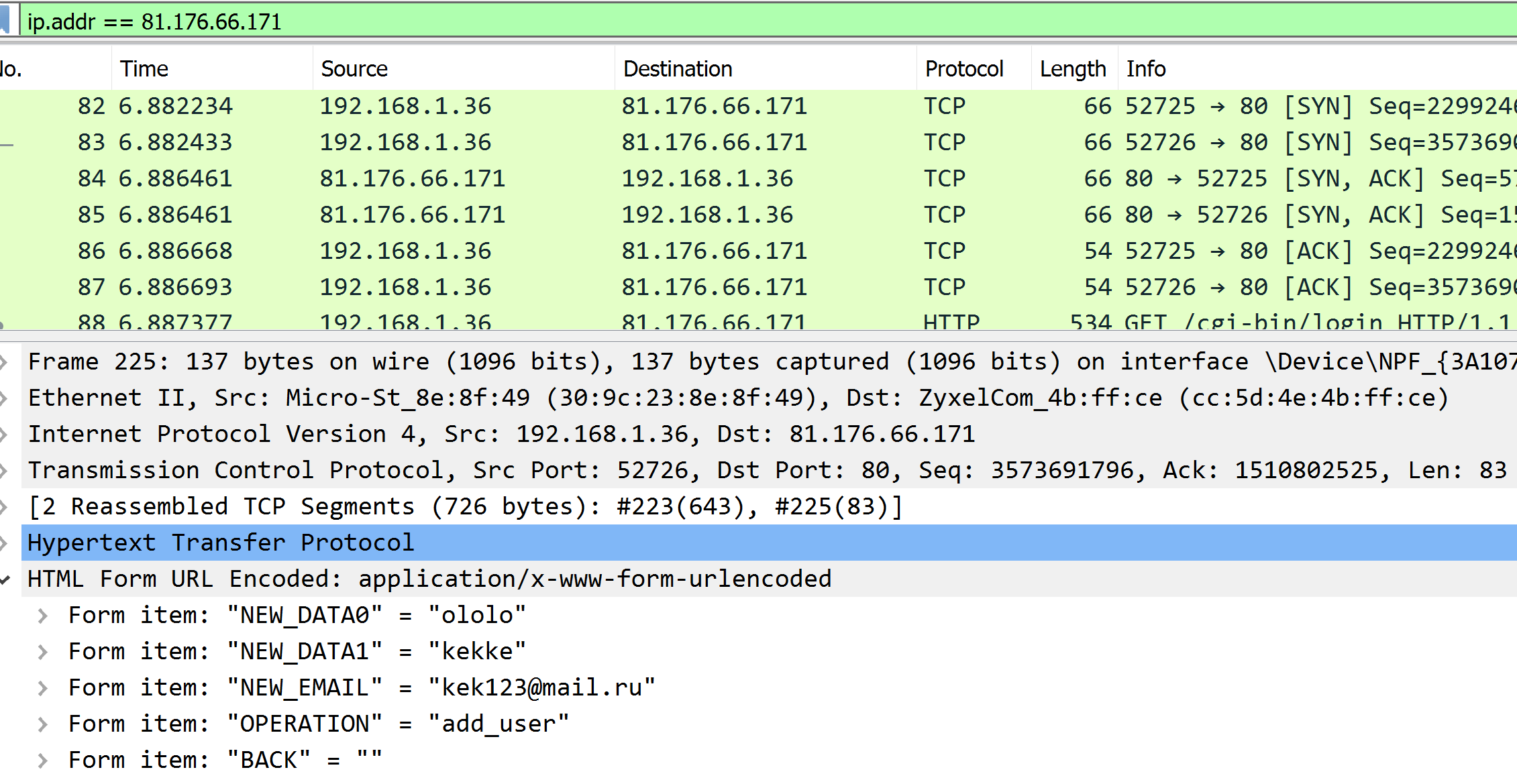
1)Задание 1:

Запустить Wireshark, выбрать любой веб-сайт по HTTP, где требуется вход или регистрация по паролю, например зайти на http://samlib.ru (или другой нешифрованный Http),ввести тут http://samlib.ru/cgi-bin/login любой пароль. Какую информацию можно узнать с помощью Wireshark?

Решение:

Данные по http передаются в открытом виде, в случае прослушивания канала связи, передаваемые данные будут получены 3 стороной в “читабельном” виде. Можно узнать логин/пароль и остальную информацию при регистрации.



2)Задание 2:

С помощью Wireshark или Cisco Packet Tracer отследить трафик, идущий по протоколу HTTP и HTTPS. В чем разница? Попробовать отследить трафик в Wireshark, подключаясь к сервисам Google (например, youtube.com) с помощью браузера Google Chrome. Какой протокол используется для доступа к веб-сервисам?

Решение:

HTTPS в отличие от HTTP передаваемую информацию шифрует (как правило используются коммерческие сертификаты), соответственно даже если данные и будут перехвачены они не смогут быть прочитаны. Подключаясь к сервисам Google через Google Chrome использовался протокол шифрования TLSv1.2/1.3. Также есть экспериментальный интернет-протокол, разработанный Google QUIC, но не смотря на включенный “тумблер” в браузере, он так и не показался в wireshark.

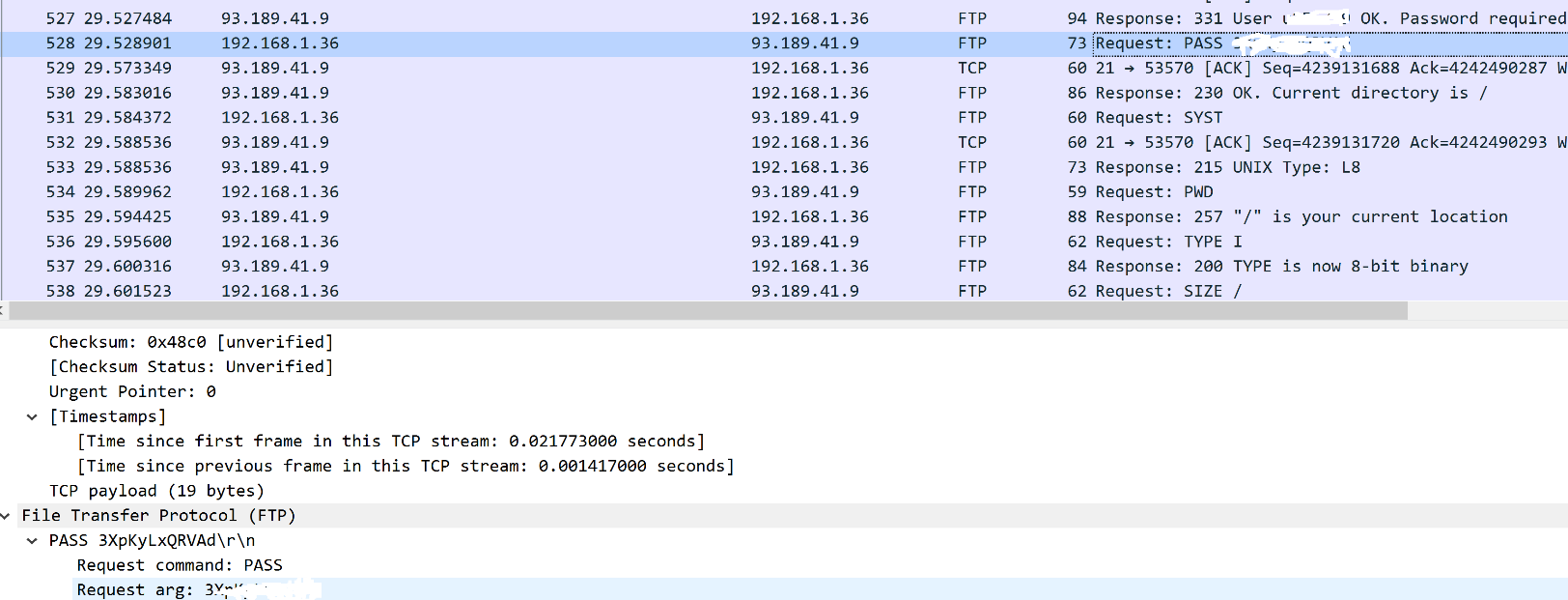
3) Задание 3:

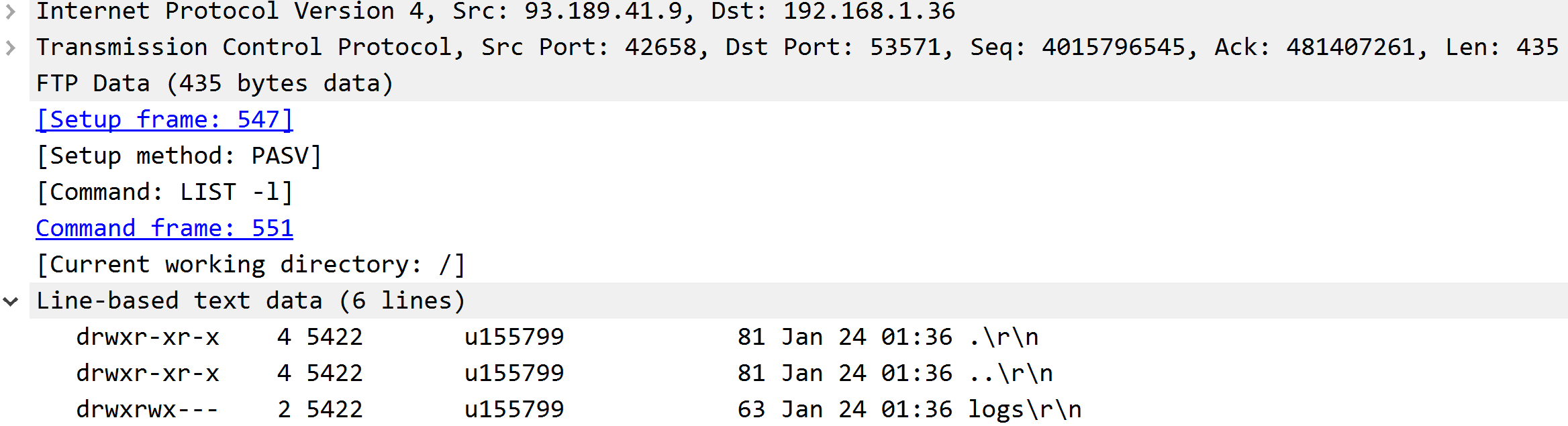
С помощью Wireshark отследить трафик при работе с обычным ftp (найти любой ftp-ресурс и подключиться к нему, через браузер). Можно ли через ftp передавать данные на

сервер, как предлагают некоторые хостеры?

Решение:

Передавать информацию по ftp на публичные сервера не безопасно, т.к. информация так же передается в открытом виде как и http.



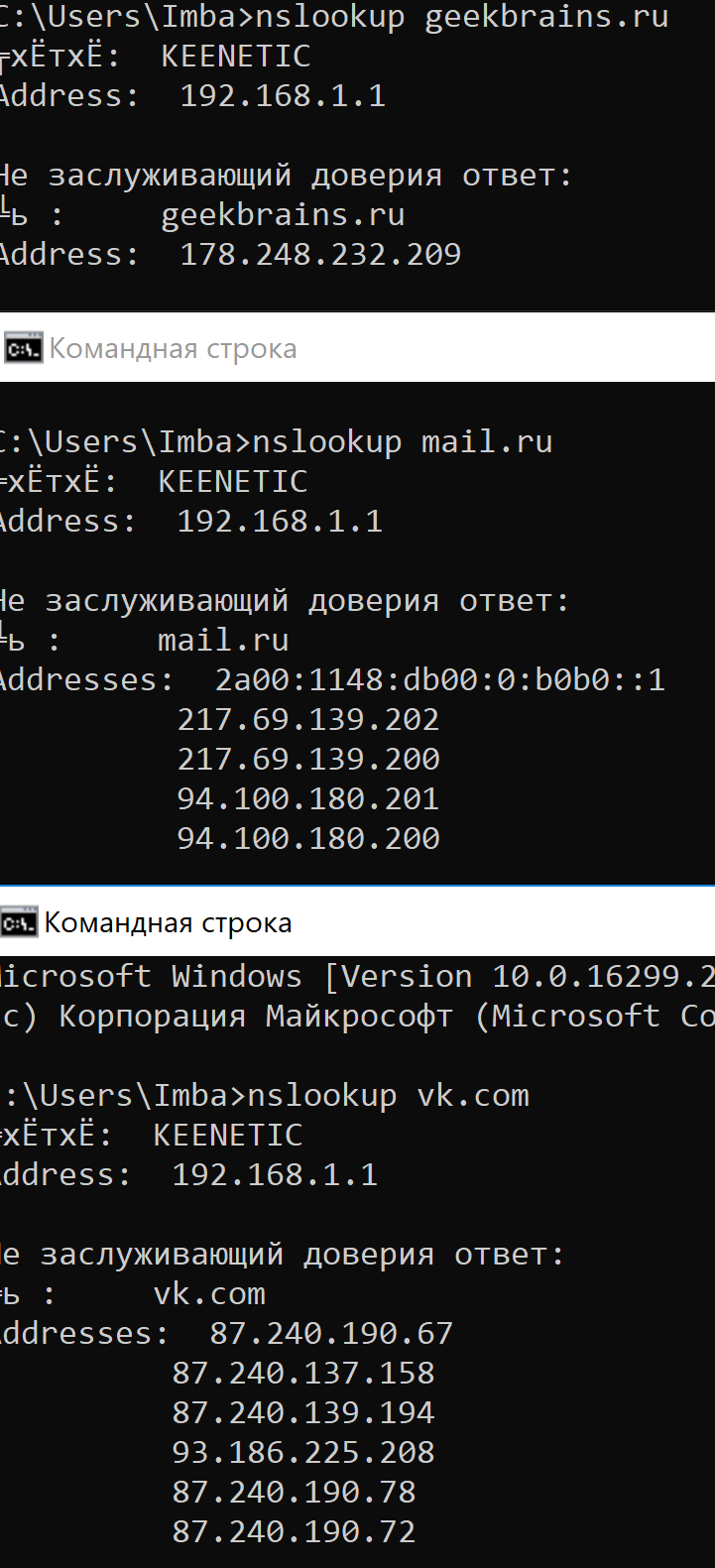


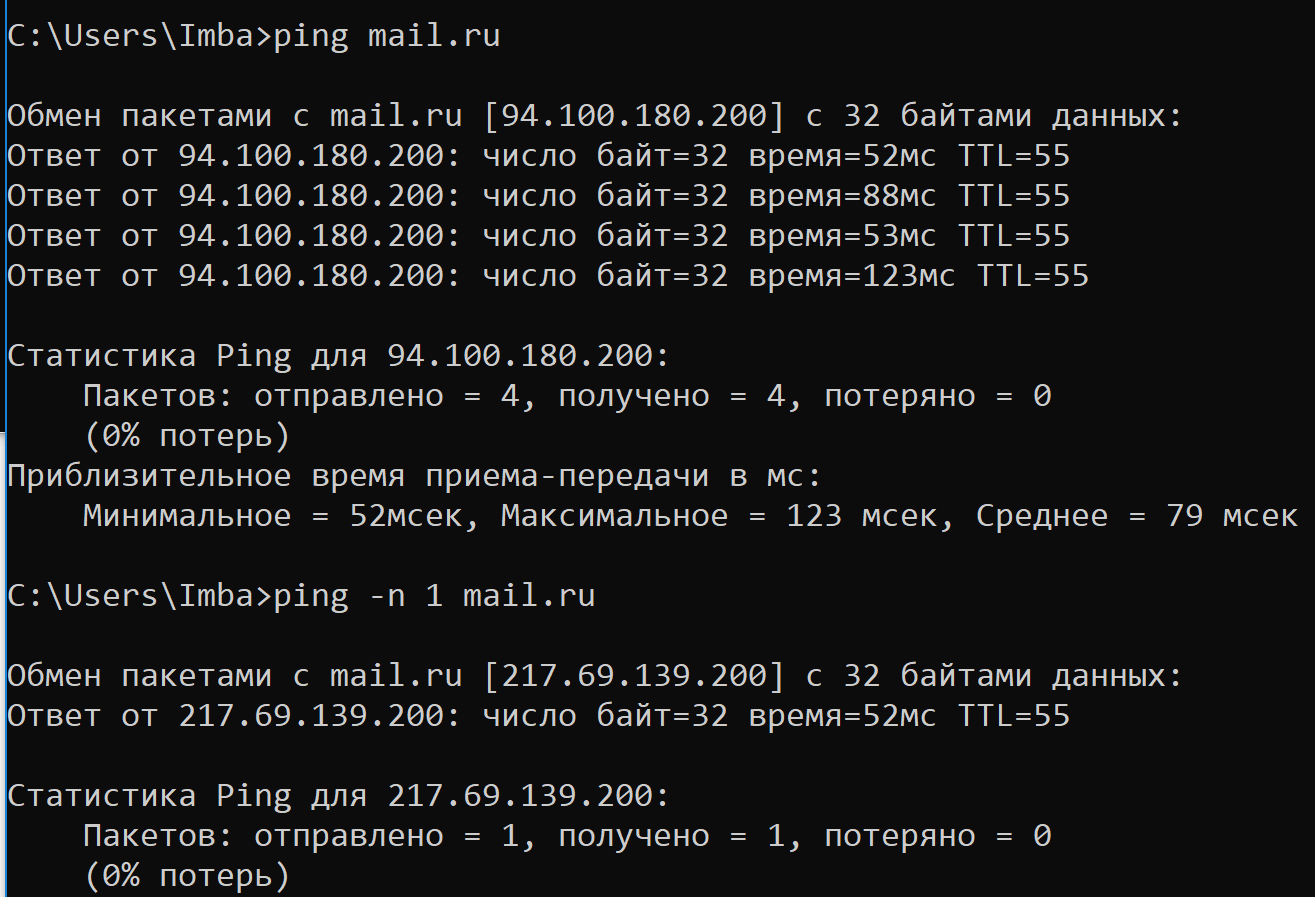
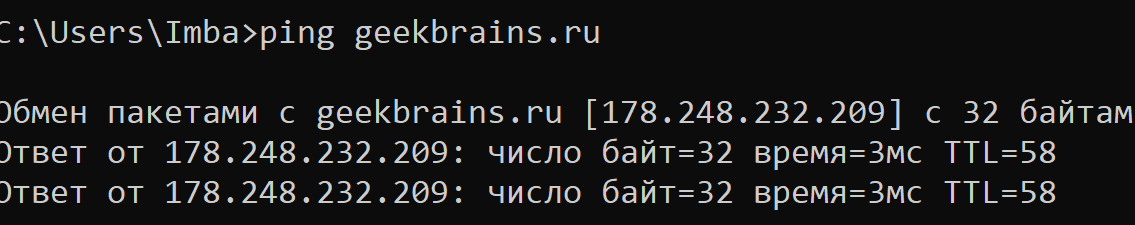
4) Задание 4:

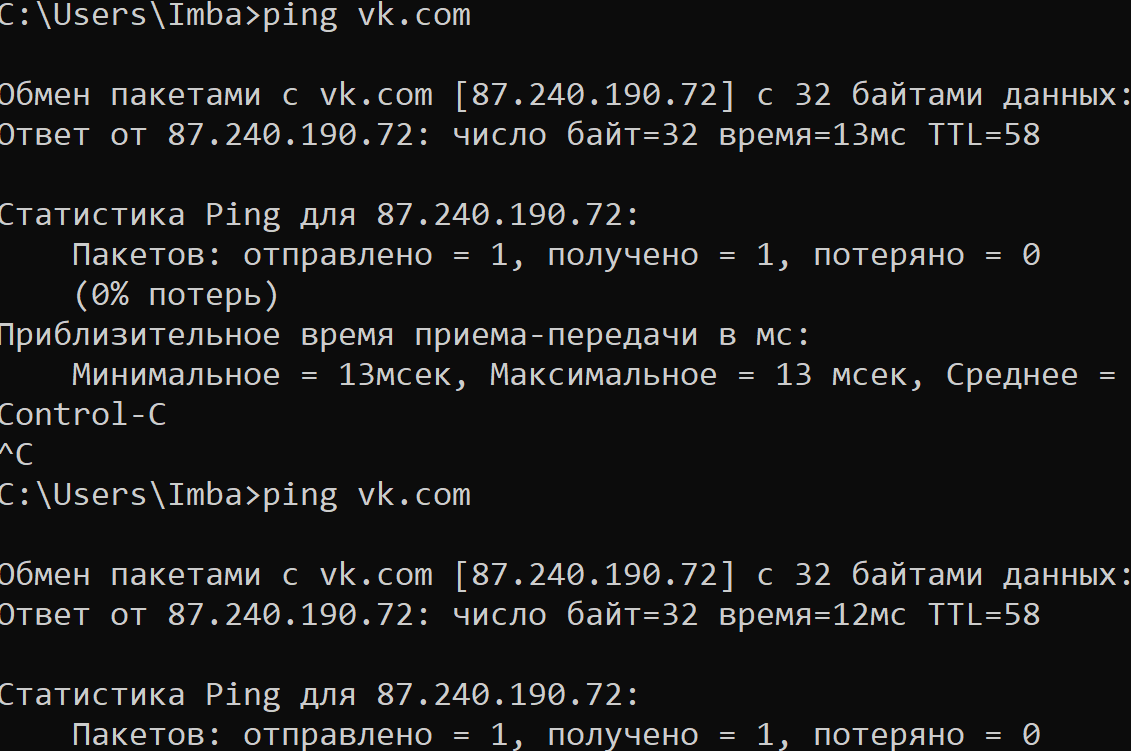
Просмотреть А-записи для доменов mail.ru, geekbrains.ru, vk.com. Сколько IP адресов серверов у этих ресурсов? Какой из них отвечает при выполнении команды ping на mail.ru, geekbrains.ru, vk.com соответственно?

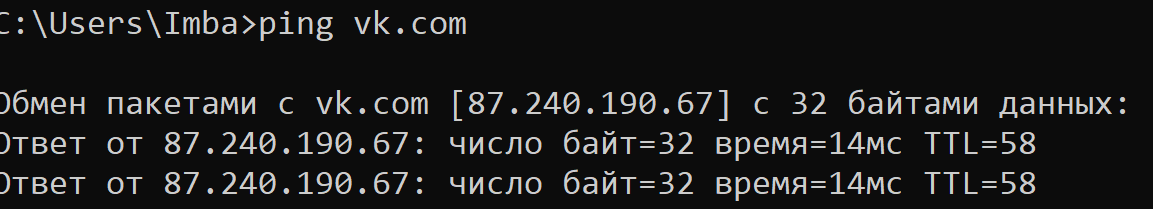
Решение:

У всех сайтов по не несколько IP адресов кроме geekbrains. Соответственно у mail.ru и vk.com ответы на ping менялись после истечения ttl записи.







5) Задание 5:

Просмотреть NS-записи для доменов google.com и youtube.com. Какой можно сделать вывод по результатам вывода этих двух команд? ДЗ сдать в виде текстового отчета в Word или PDF со скриншотами и описанием (сами дампы из WireShark прикладывать не надо).

Решение:

DNS зоны google.com и youtube.com хранятся и обслуживаются одними и теми же серверами, в количестве 4 шт.

