МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информатики и прикладной математики

Кафедра прикладной математики и экономико-математических методов

ОТЧЁТ

по дисциплине:

«Сети передачи данных и информационная безопасность»

на тему:

«Перехват ответов хостов Wireshark»

Направление (специальность)_____01.03.02_____
(код, наименование)

Обучающийся _____Бронников Егор Игоревич_____
(Ф.И.О. полностью)

Группа___ПМ-1901___
(номер группы)

Санкт-Петербург
2021

Задание

Приложить скриншот tracert и файл Wireshark. Дать текстовое пояснение по одному из пакетов.

С помощью утилиты «*traceroute*» можно просмотреть сколько хостов прошёл пакет который мы отправляем с нашего хоста до конечного хоста получателя.

```
[~]
λ traceroute ya.ru
traceroute to ya.ru (87.250.250.242), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  0.418 ms  0.390 ms  0.407 ms
 2  91.201.231.181 (91.201.231.181)  1.857 ms  1.952 ms  1.931 ms
 3  core-v625.xtrim.ru (91.201.231.234)  1.973 ms  2.173 ms  1.929 ms
 4  nat2-c1.xtrim.ru (91.201.230.169)  2.396 ms  2.131 ms  2.043 ms
 5  nat2-j-45-gw.xtrim.ru (91.201.230.173)  2.563 ms  2.479 ms  2.386 ms
 6  spb.piter-ix.yandex.ru (185.1.152.57)  3.104 ms  2.831 ms  2.633 ms
 7  * 10.4.8.1 (10.4.8.1)  16.165 ms 10.3.3.1 (10.3.3.1)  18.307 ms
 8  ya.ru (87.250.250.242)  13.230 ms  12.545 ms  12.583 ms
```

Рисунок 1. Результат работы утилиты traceroute на примере ya.ru

Из результата работы утилиты «traceroute» видно, что пакет проходит через 8 хостов прежде чем достигнет итогового хоста получателя.

Далее при помощи фильтра Wireshark перехватим ответы хостов.

Рисунок 2. Фильтр захвата Wireshark

Таким образом, после запуска захвата, мы получили, следующие записи:

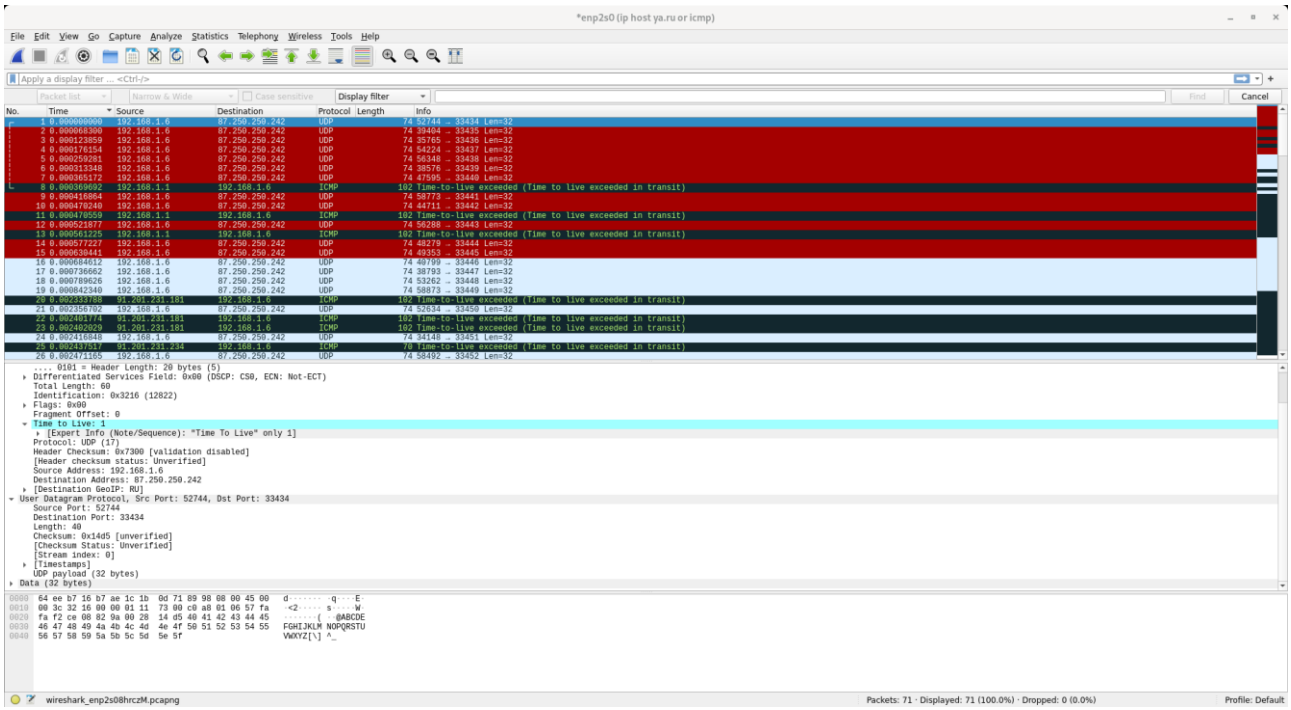
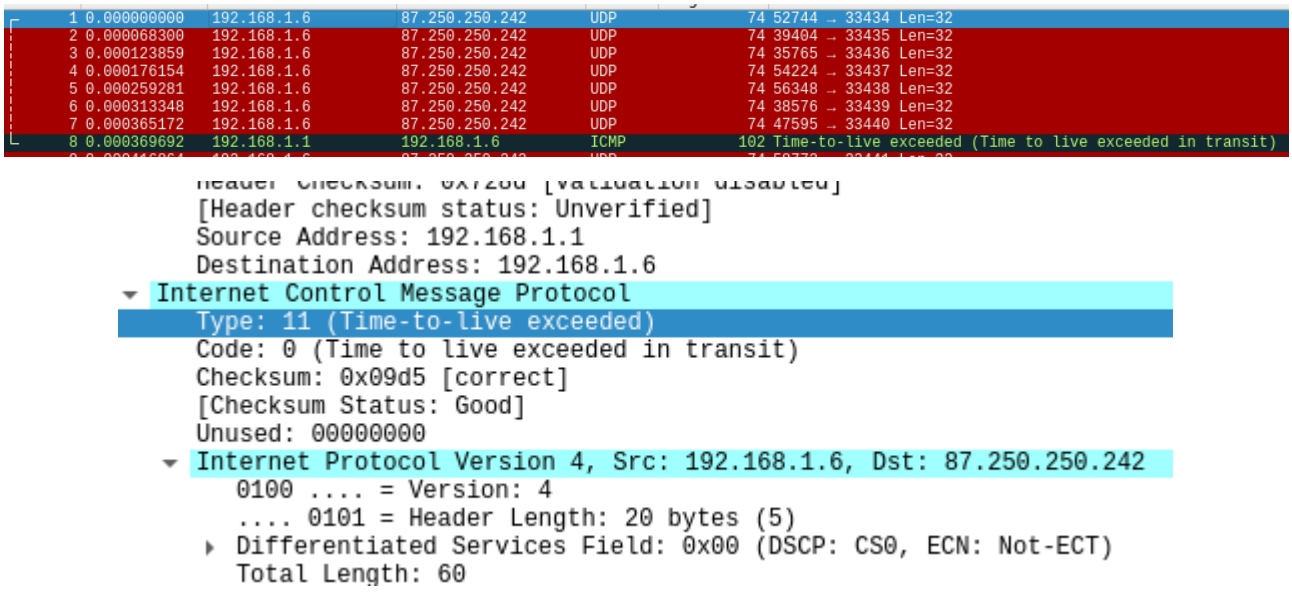


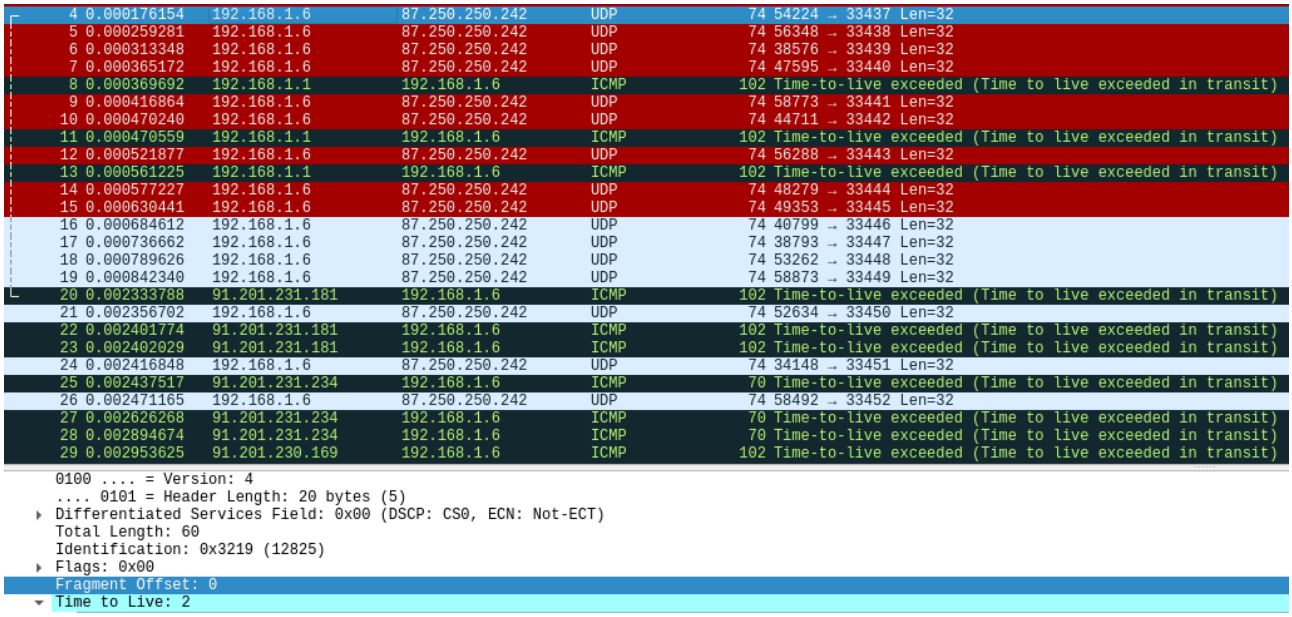
Рисунок 3. Результат захвата

Сначала мы отправляем UDP пакет от нашего хоста 192.168.1.6 до первого роутера 192.168.1.1 с TTL=1. Роутер дропает пакет и сообщает нам о том, что “Time to live exceeded in transit” (Type=11).

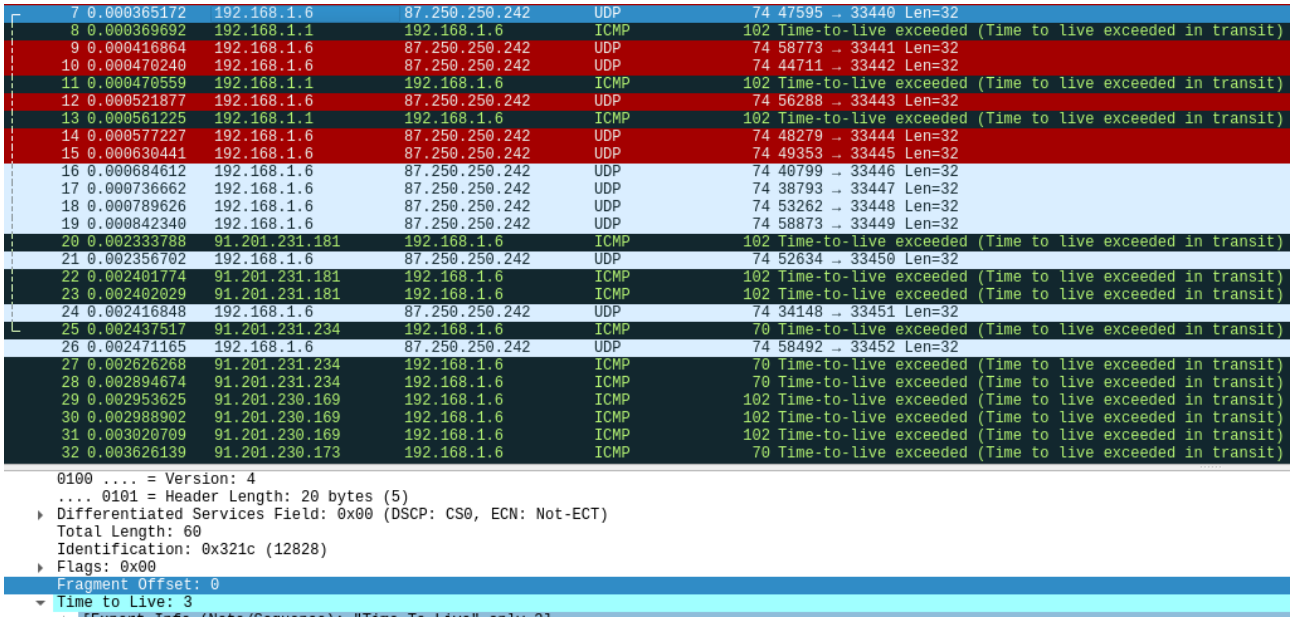


Всё это происходит 3 раза до того, как источник отправит следующий пакет с увеличением значения TTL на 1, то есть TTL=2.

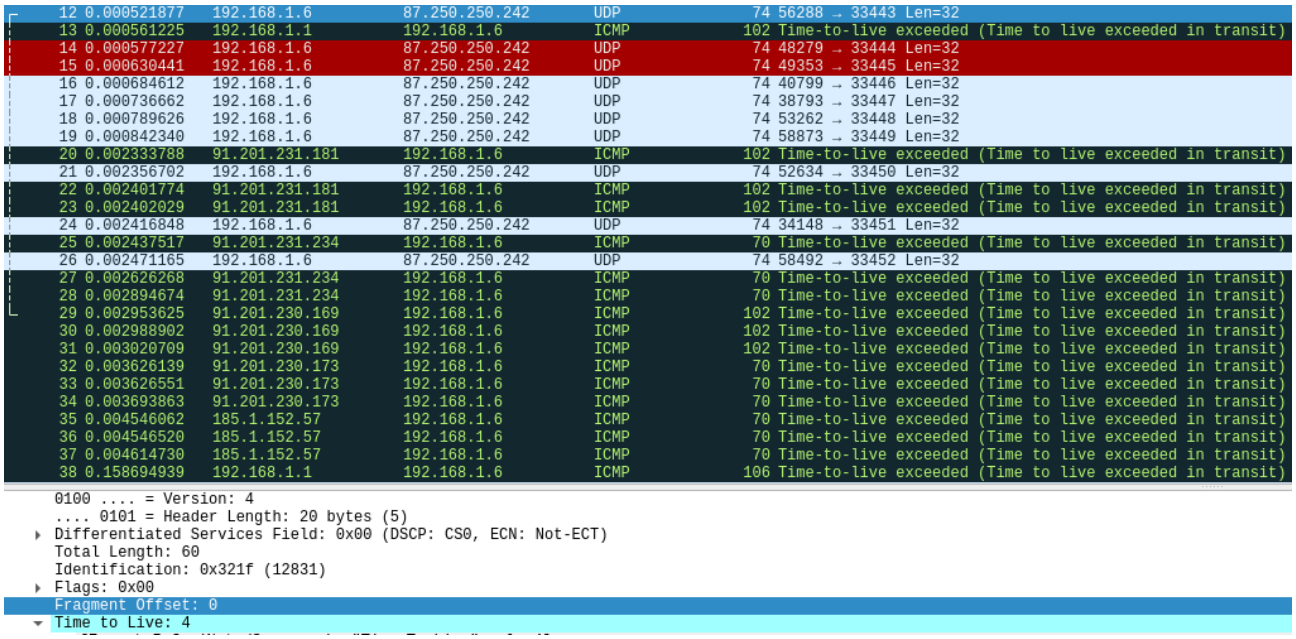
Снова отправляем UDP пакет, но уже с TTL=2. В результате уже от 2 хоста – 91.201.231.181, мы получили ICMP ответ, что опять нам не хватило TTL – “Time to live exceeded in transit” (Type 11).



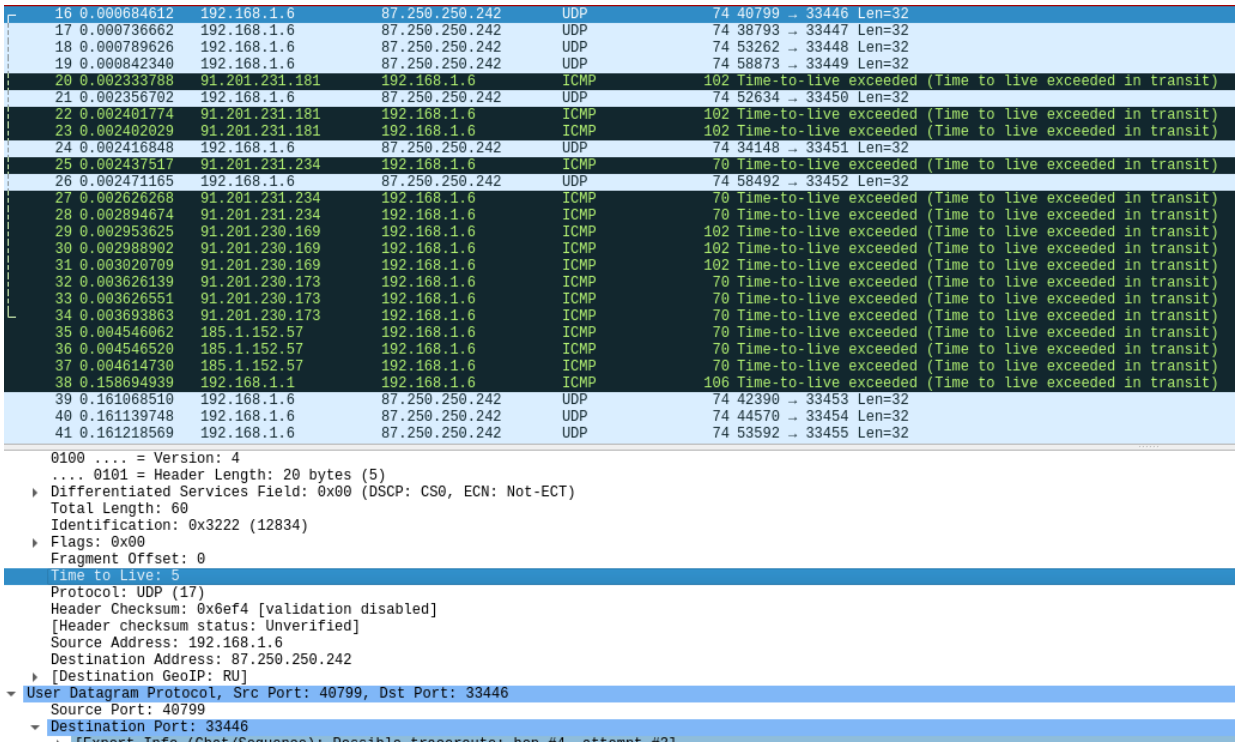
Опять-таки проделываем это 3 раза, после чего увеличиваем TTL на 1, то есть TTL=3. Снова отправляем UDP пакет, но уже с TTL=3. В результате уже от 3 хоста – 91.201.231.234, мы получили ICMP ответ, что опять нам не хватило TTL – “Time to live exceeded in transit” (Type 11).



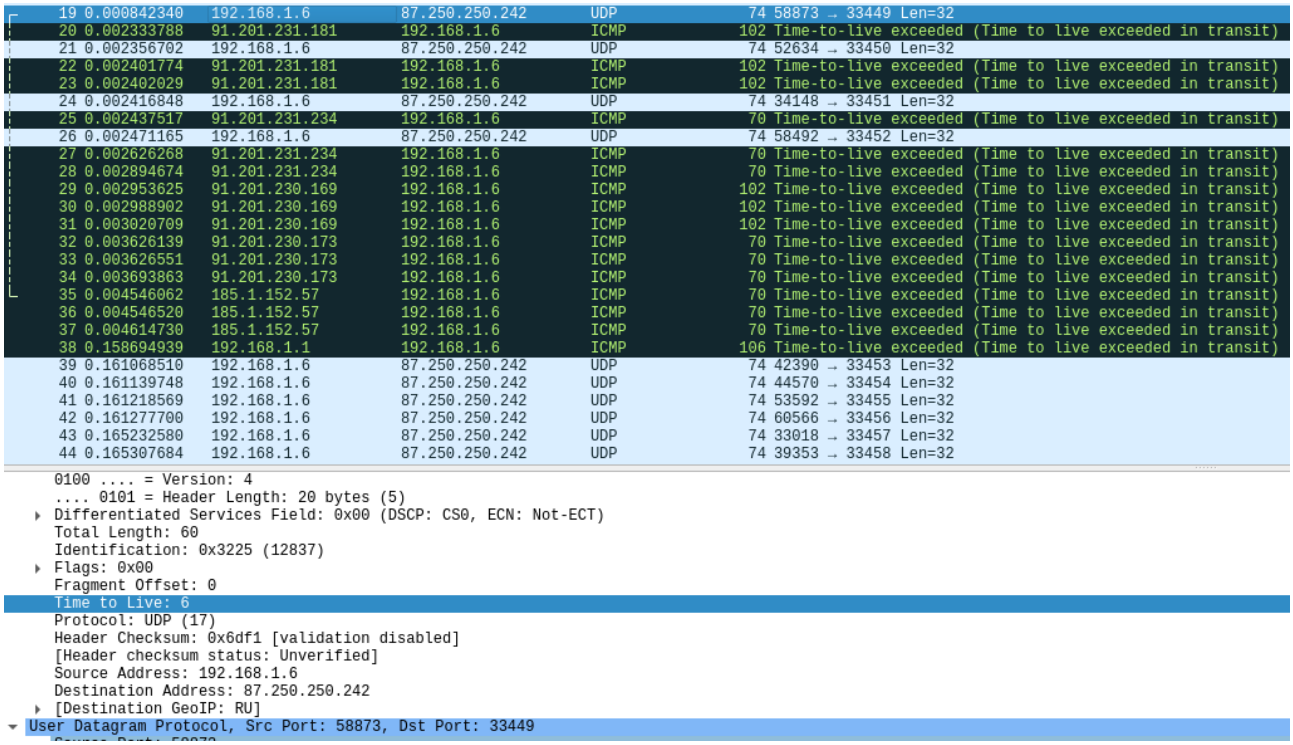
Проделываем это 3 раза. Увеличиваем TTL на 1, то есть TTL=4. Снова отправляем UDP пакет, но уже с TTL=4. В результате уже от 4 хоста – 91.201.230.169, мы получили ICMP ответ, что опять нам не хватило TTL – “Time to live exceeded in transit” (Type 11).



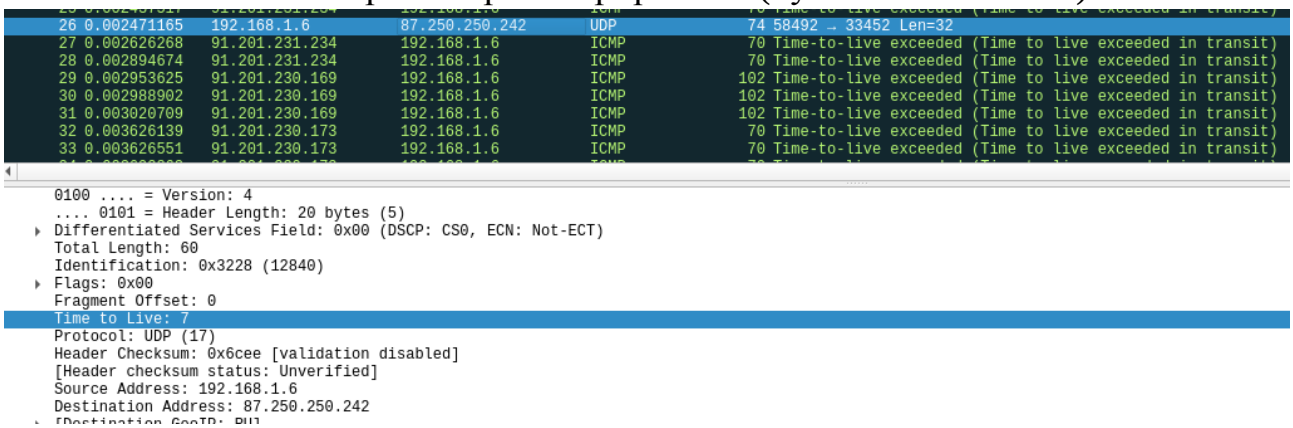
Проделываем это 3 раза. Увеличиваем TTL на 1, то есть TTL=5. Снова отправляем UDP пакет, но уже с TTL=5. В результате уже от 5 хоста – 91.201.230.173, мы получили ICMP ответ, что опять нам не хватило TTL – “Time to live exceeded in transit” (Type 11).



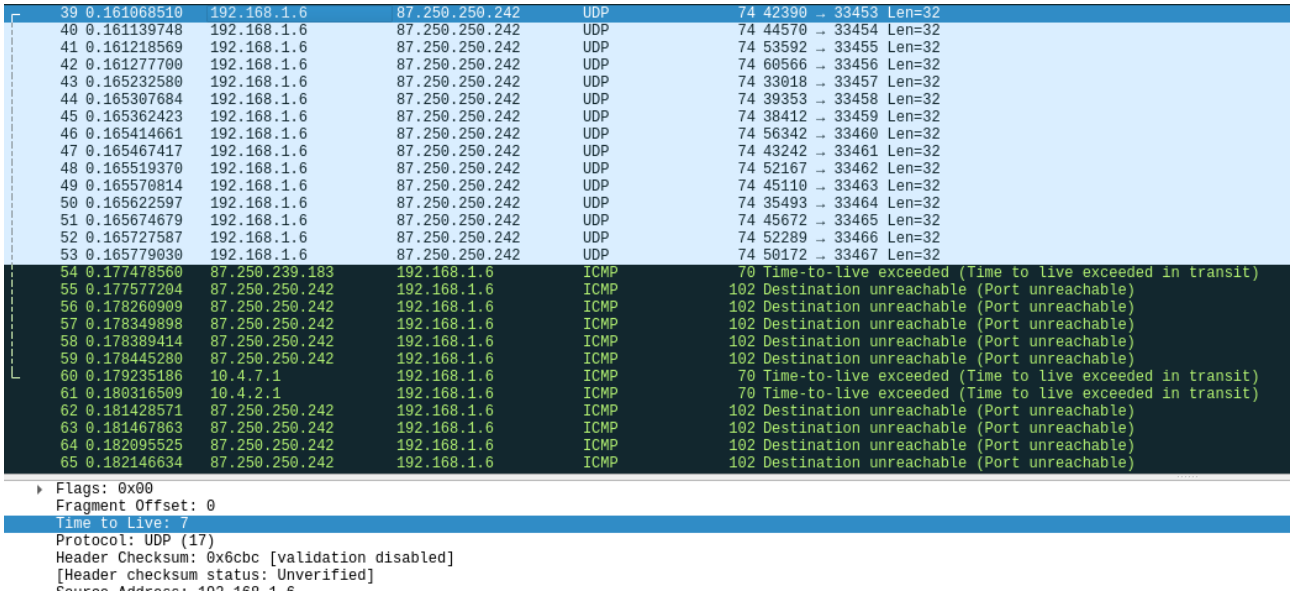
Проделываем это 3 раза. Увеличиваем TTL на 1, то есть TTL=6. Снова отправляем UDP пакет, но уже с TTL=6. В результате уже от 6 хоста – 185.1.152.57, мы получили ICMP ответ, что опять нам не хватило TTL – “Time to live exceeded in transit” (Type 11).



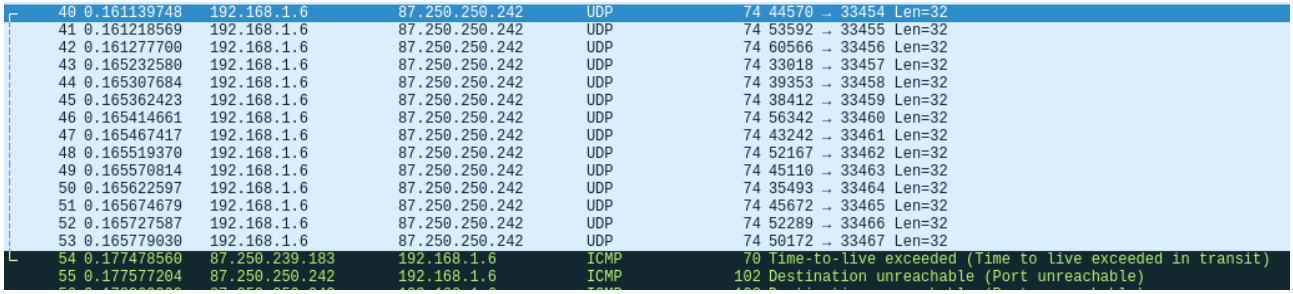
Проделываем это 3 раза. Увеличиваем TTL на 1, то есть TTL=7. Снова отправляем UDP пакет, но уже с TTL=7. В результате этот товарищ нам решил ничего не отвечать и просто проигнорировать. (ну и не хотелось ☹)



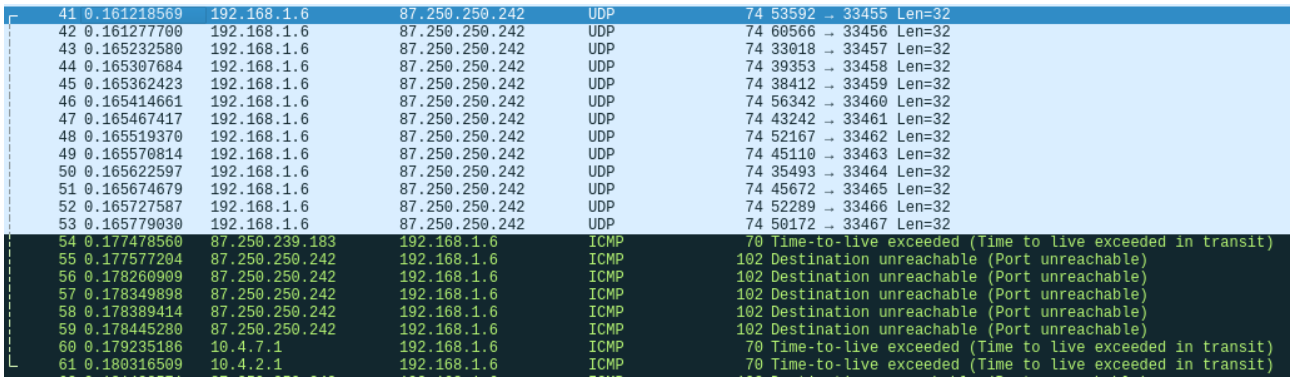
Отправляем ещё раз UDP пакет с TTL=7 и всё-таки уже от 7 хоста – 10.4.7.1, мы получили ICMP ответ, что опять нам не хватило TTL – “Time to live exceeded in transit” (Type 11).



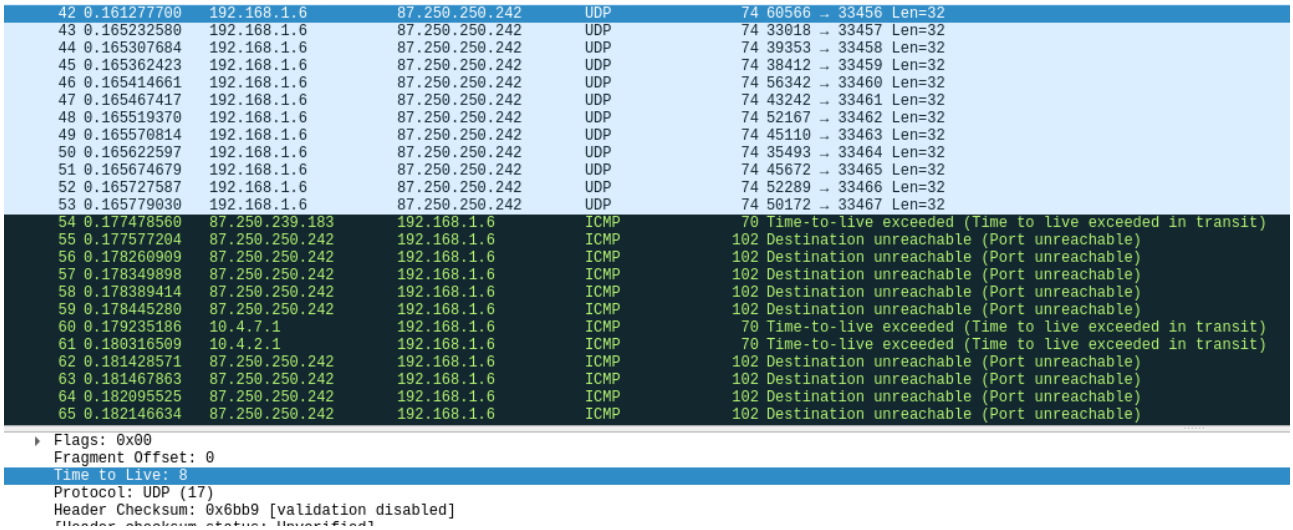
Отправляем ещё раз UDP пакет с TTL=7 и уже от другого хоста – 87.250.239.183, мы получили ICMP ответ, что опять нам не хватило TTL – “Time to live exceeded in transit” (Type 11).



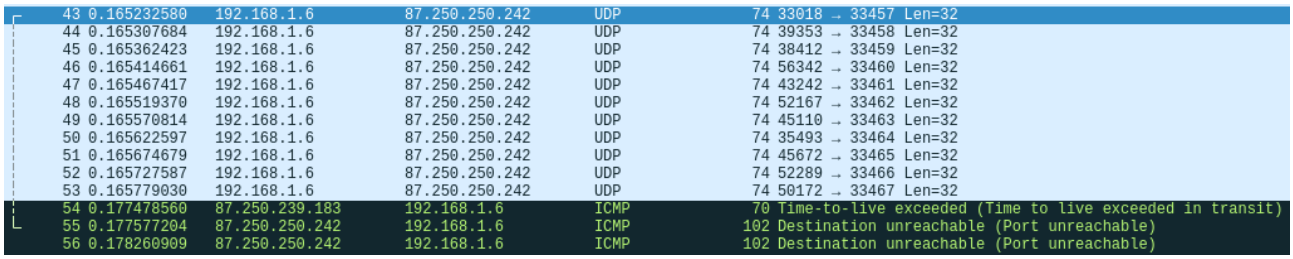
Отправляем ещё раз UDP пакет с TTL=7 и уже от другого хоста – 10.4.2.1, мы получили ICMP ответ, что опять нам не хватило TTL – “Time to live exceeded in transit” (Type 11).



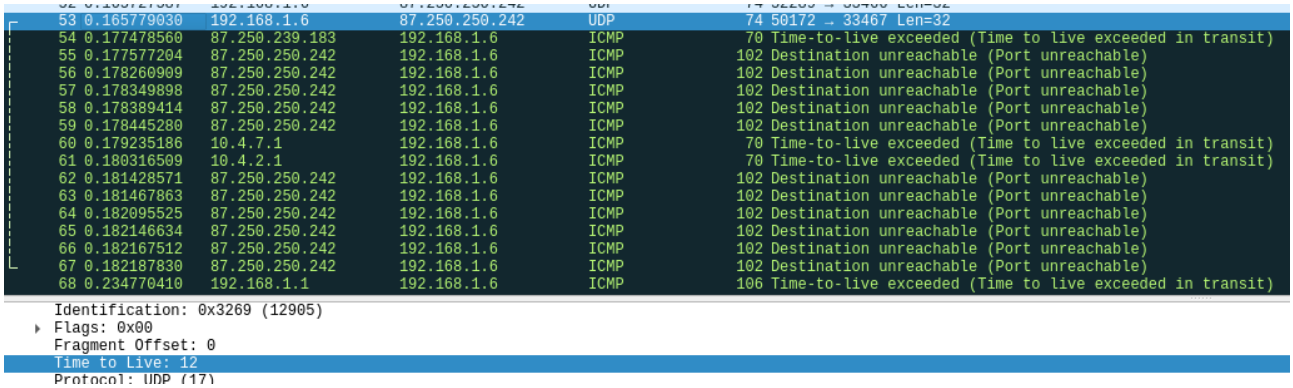
Увеличиваем TTL на 1, то есть TTL=8. Снова отправляем UDP пакет, но уже с TTL=8. В результате этот товарищ нам решил ничего не отвечать и просто проигнорировать. (ну и не хотелось ☹)



Отправляем ещё раз UDP пакет с TTL=8 и уже от другого хоста – 87.250.239.183, мы получили ICMP ответ – “Destination unreachable” (Type 3). (правда непонятно почему)



Далее мы наращиваем TTL последовательно до 12, то есть TTL=12, но каждый раз получаем получили ICMP ответ – “Destination unreachable” (Type 3). (правда непонятно почему)



Получилось немного странно, не то что я ожидал, но я пытался несколько раз перезапускать *«traceroute ya.ru»*, но получал всегда один и тот же ответ +-.