Домашняя работа 10

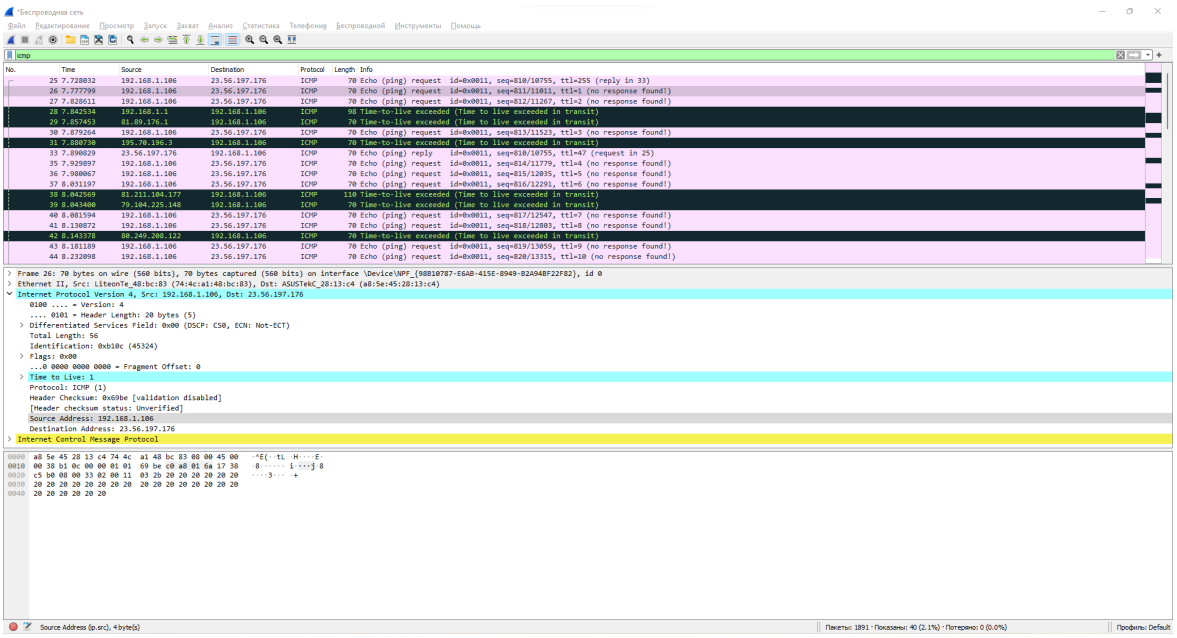
Задание 1:

1. Выберите первое ICMP-сообщение эхо-запроса, отправленное вашим компьютером, и раскройте часть информации о пакете Internet Protocol в окне подробной информации. Каков IP-адрес вашего компьютера?

IP-адрес моего компьютера 192.168.1.106.

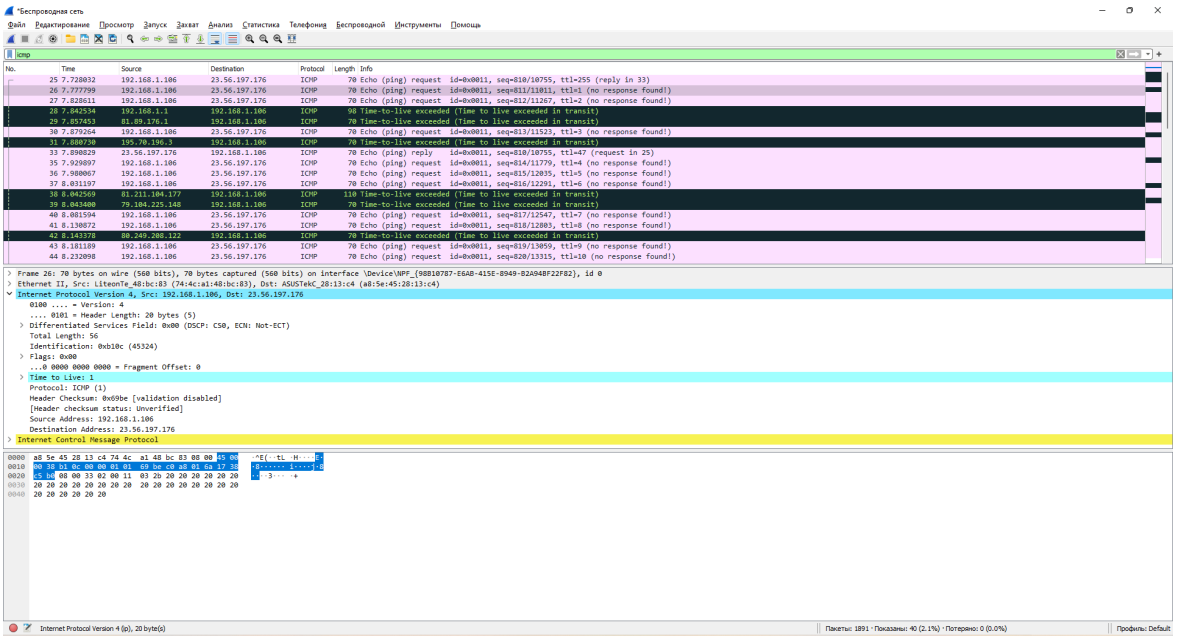
2. Найдите заголовок IP-пакета. Какое значение указано здесь в поле протокола верхнего уровня?

В поле протокола верхнего уровня здесь указано значение ICMP (1).



3. Сколько байт в IP-заголовке? Сколько байт приходится на полезную нагрузку IP-дейтаграммы?

В IP-заголовке 20 байт (Header Length). На полезную нагрузку IP-дейтаграммы приходится 36 байт (56 (Total Length) - 20).



4. Отсортируйте отслеженные пакеты по их исходному IP-адресу; для этого щелкните по заголовку столбца Source. Выберите первое сообщение эхо-запроса, отосланное вашим компьютером по протоколу ICMP, и раскройте раздел Internet Protocol.

a. Какие поля IP-дейтаграммы всегда изменяются от одной дейтаграммы к следующей в рамках одной последовательности ICMP-сообщений, отсылаемых компьютером?

Всегда изменяются поля Identification, Time to Live, Checksum (хотя в теории Checksum может и совпасть).

b. Какие поля не меняются? Какие поля должны оставаться неизменными? Какие поля должны изменяться?

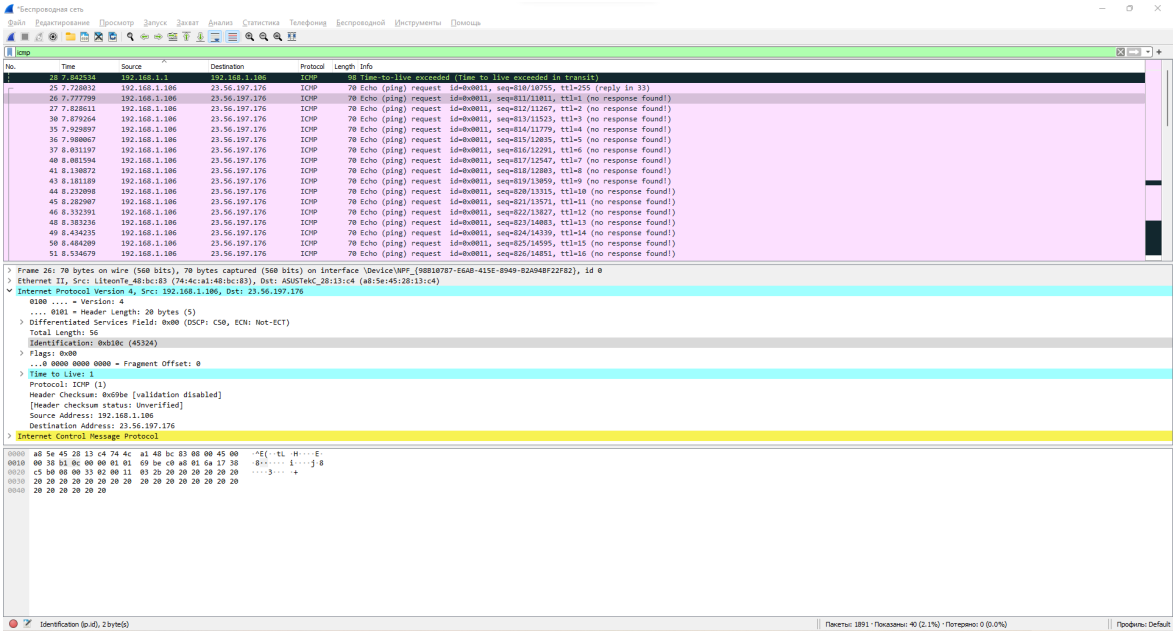
Не меняются поля Version, Header Length, Differentiated Services Field, Total Length, Flags, Fragment Offset, Protocol, Source Address и Destination Address.

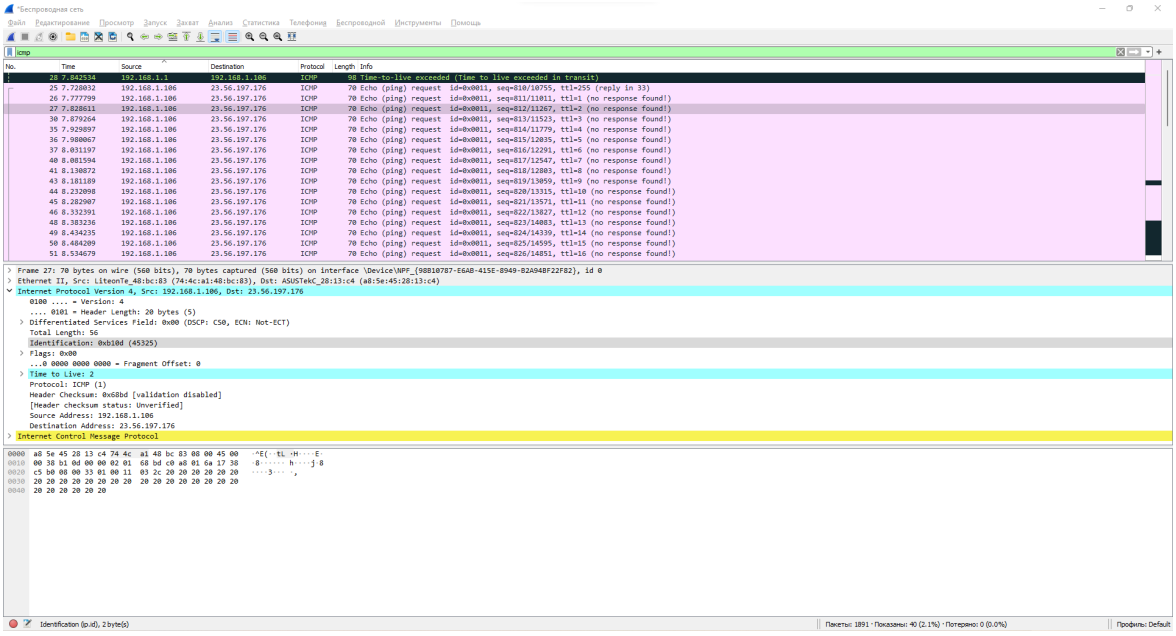
Должны оставаться неизменными поля Version (т.к. для IPv6 используется другой протокол ICMPv6), Protocol (т.к. traceroute использует ICMP), Source Address и Destination Address.

Должны изменяться поля Time to Live (т.к. так устроен traceroute), Identification и Checksum (если только не совпадет случайно).

c. Как изменяется значение поля Identification IP-дейтаграммы с каждым последующим эхо-запросом? Есть ли какая-либо закономерность?

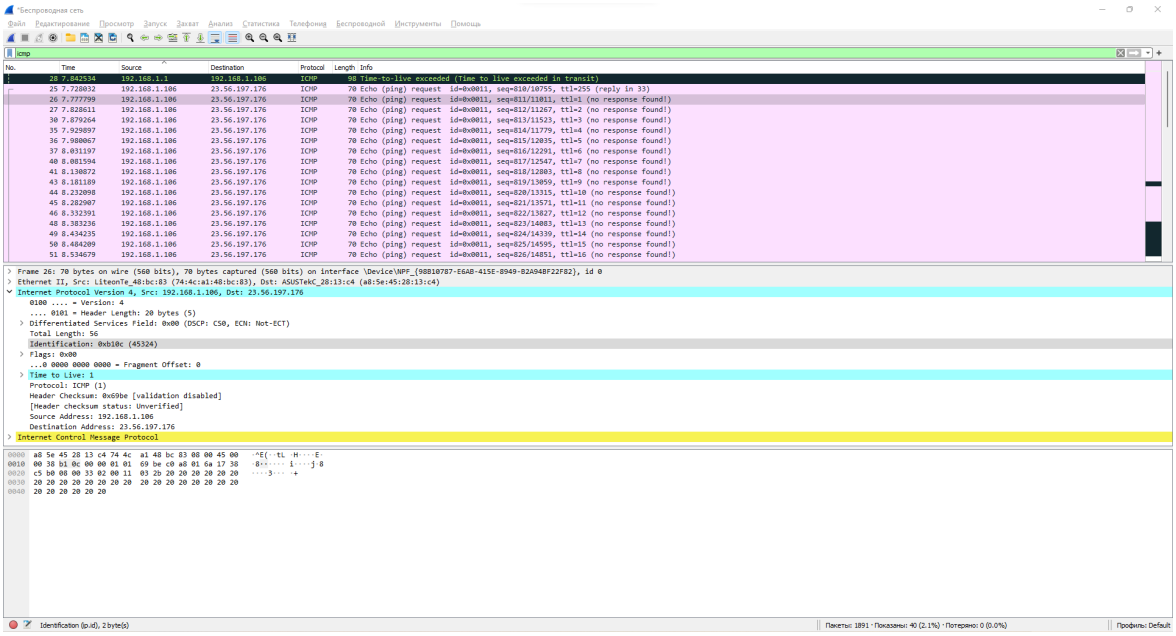
Значение поля Identification с каждым последующим эхо-запросом увеличивается на 1.





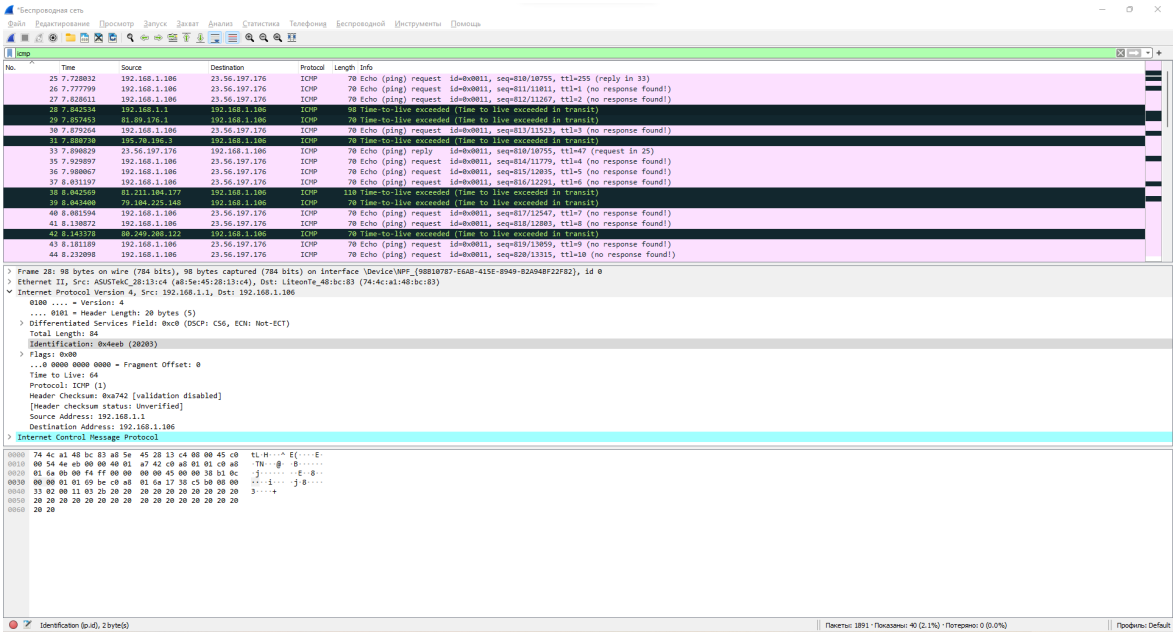
5. Какое значение содержится в поле Identification (Идентификация), а какое – в поле TTL?

В поле Identification содержится значение 45324, а в поле TTL – 1.



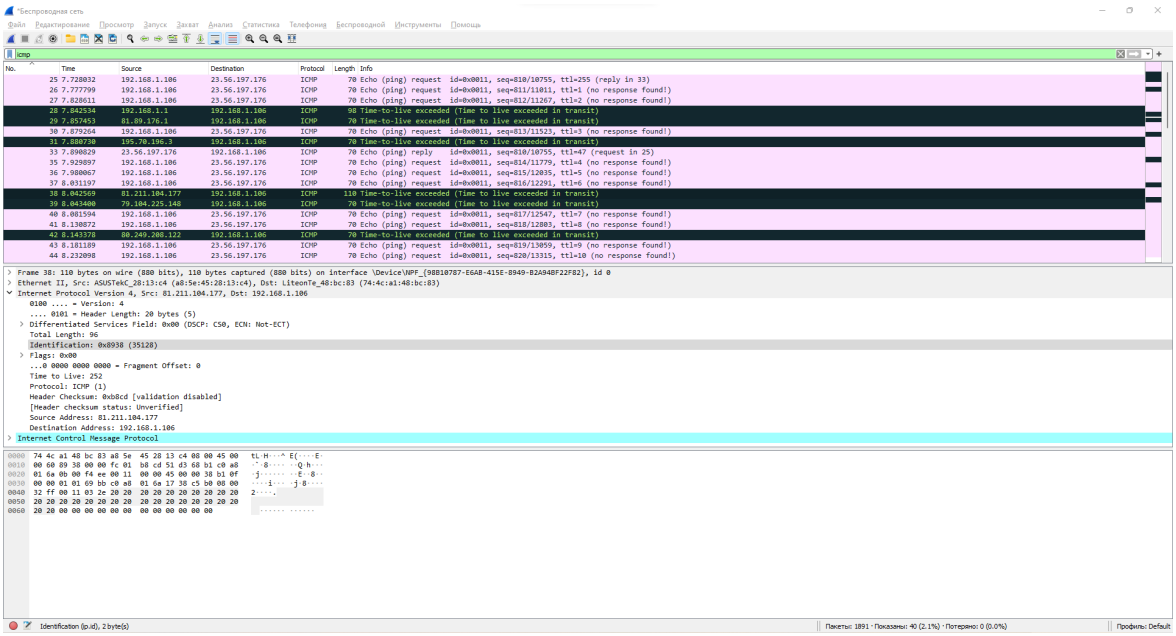
6. Остаются ли эти значения неизменными во всех сообщениях протокола ICMP, где содержится информация об истечении предписанного времени жизни; рассмотрите только те из таких сообщений, которые поступили на компьютер с ближайшего (первого транзитного) маршрутизатора.

Во всех сообщениях, поступивших с первого транзитного маршрутизатора, установлено фиксированное TTL=64. Поле Identification при этом меняется.



7. Найдите серии откликов ICMP, в которых содержатся сообщения об истечении предписанного времени жизни (time-to-live exceeded). Выберите один из пакетов. Какое значение содержится в поле Identification (Идентификация), а какое – в поле TTL?

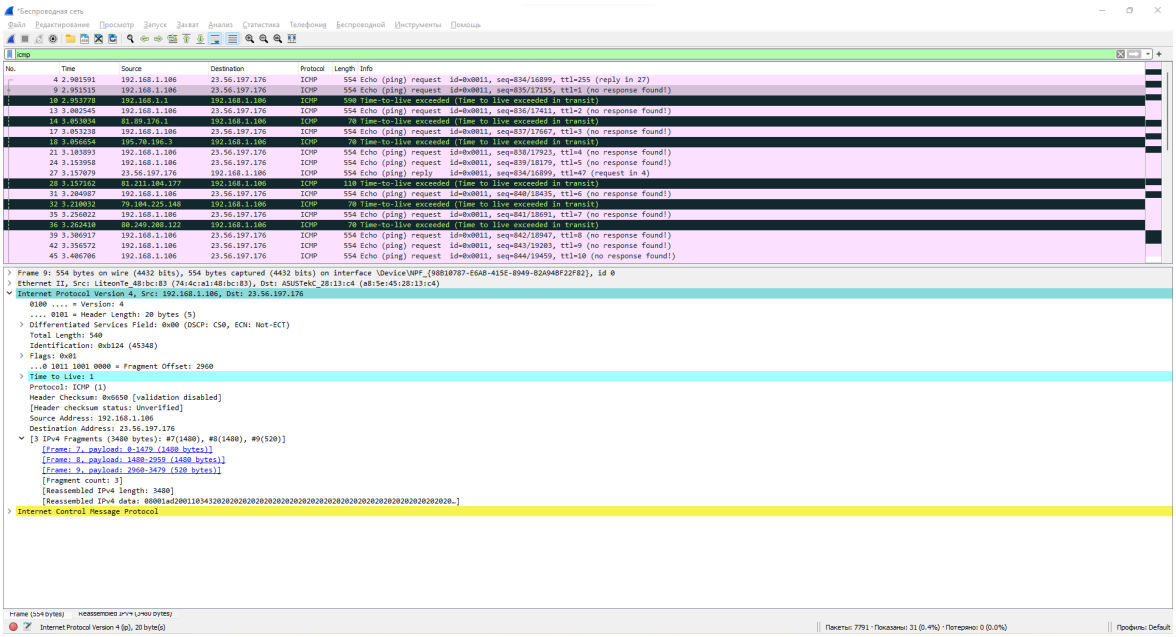
В поле Identification содержится значение 35128, а в поле TTL – 252. (В некоторых пакетах Identification=0)



8. Фрагментация. Остановите захват пакетов в Wireshark. Измените размер пакета Packet Size = 3500 байт. Снова запустите захват пакетов в Wireshark и перезапустите трассировку. (Для Unix заново запустите traceroute с длиной пакета 3500 байт). Найдите первое сообщение протокола ICMP с эхо-запросом, поступившее на ваш компьютер (с уже измененным размером пакета).

a. Было ли это сообщение фрагментировано между двумя или более IP-дейтаграммами? Если да, то сколько фрагментов было создано?

Да, было. Было создано 3 фрагмента.



b. Какие поля IP-заголовка изменяются в разных фрагментах?

Меняются поля Fragment Offset, Header Checksum. Также в последнем фрагменте меняются поля Total Length и Flags.