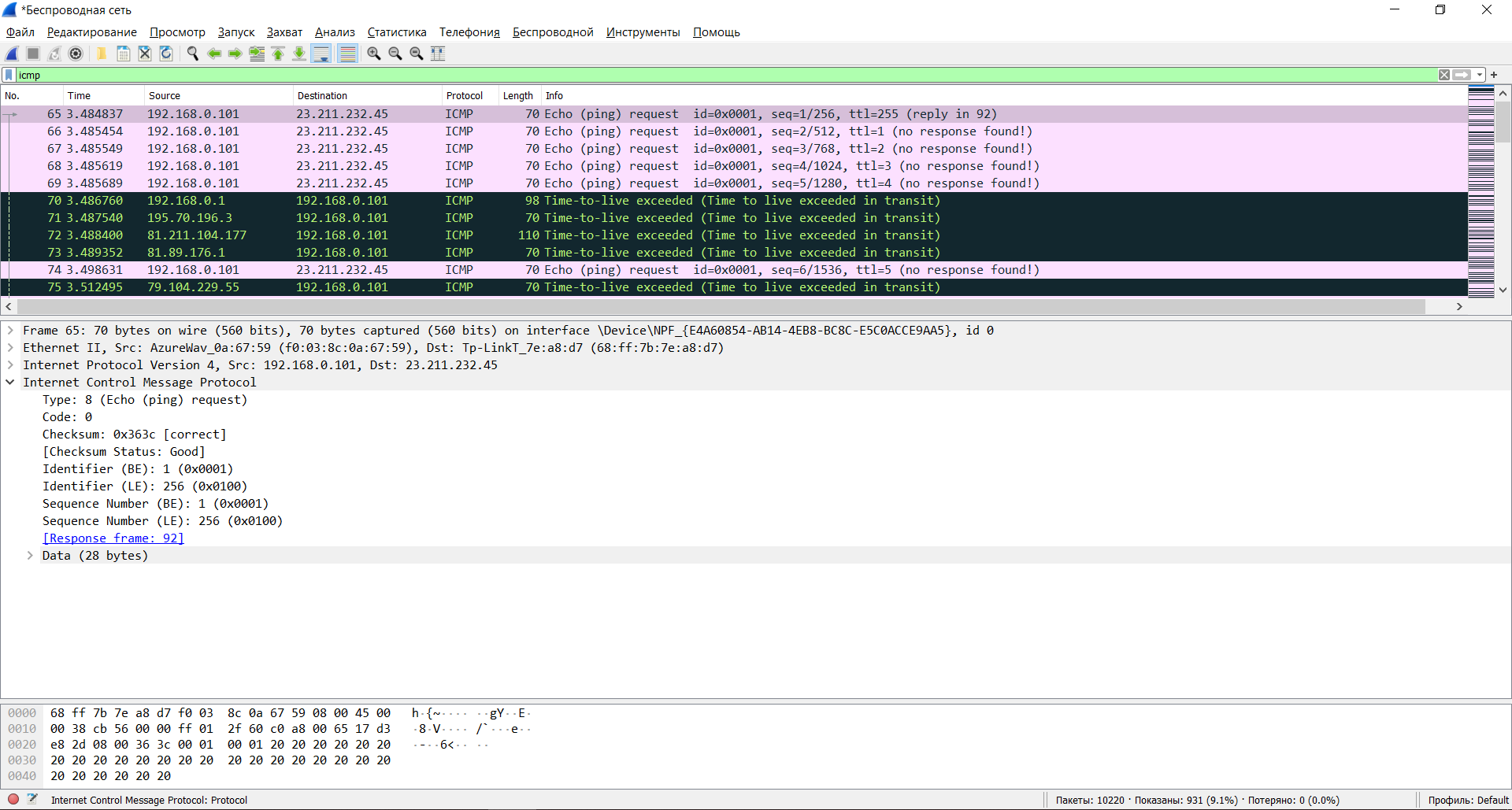
# Wireshark.

## Изучение трассы.

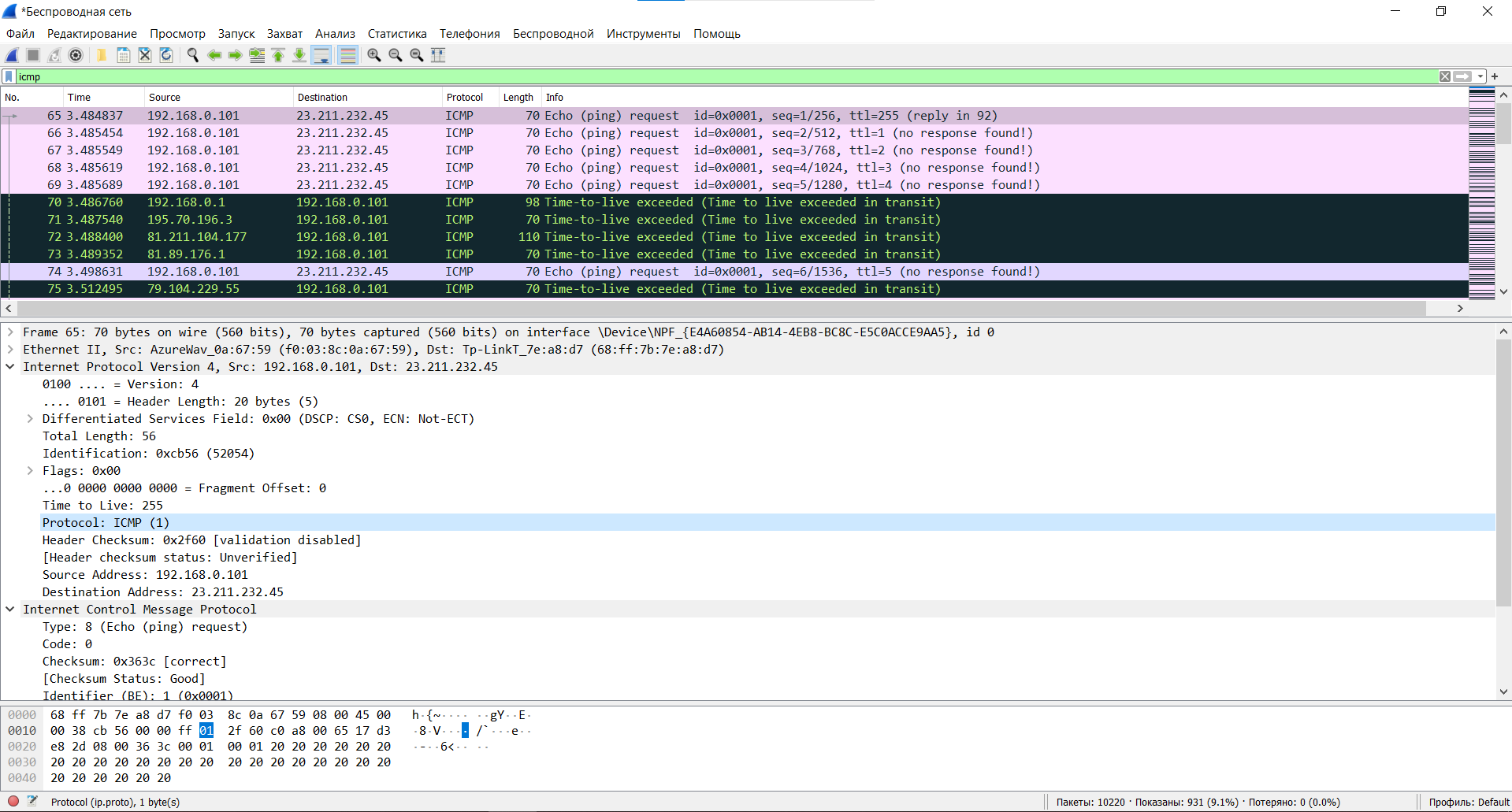
### **1.** Выберите первое ICMP-сообщение эхо-запроса, отправленное вашим компьютером, и раскройте часть информации о пакете Internet Protocol в окне подробной информации. Каков IP-адрес вашего компьютера?

192.168.0.101



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

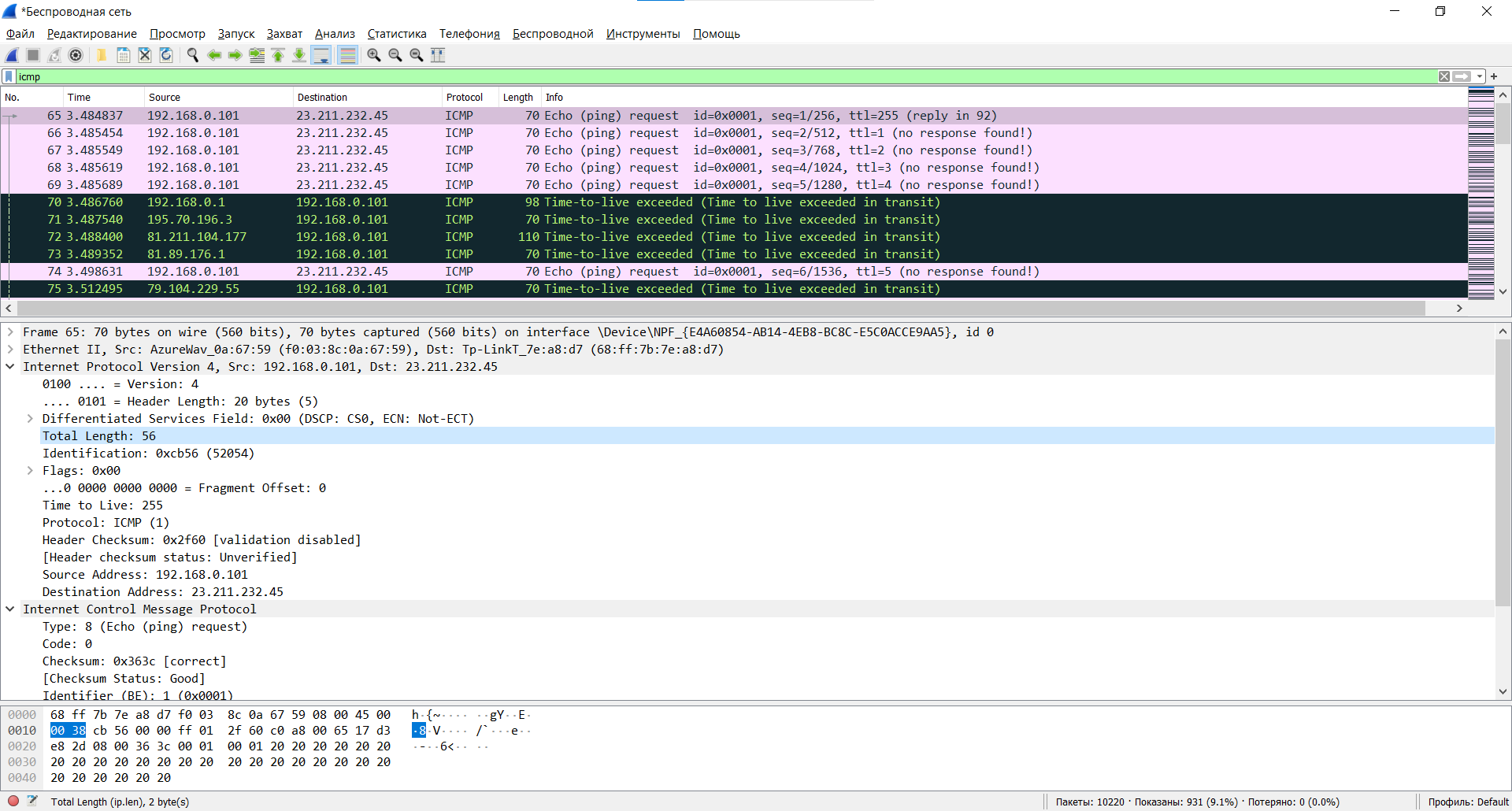
ICMP (1)



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

Заголовок - 20 байт, total - 56.

Полезная: 36 байт

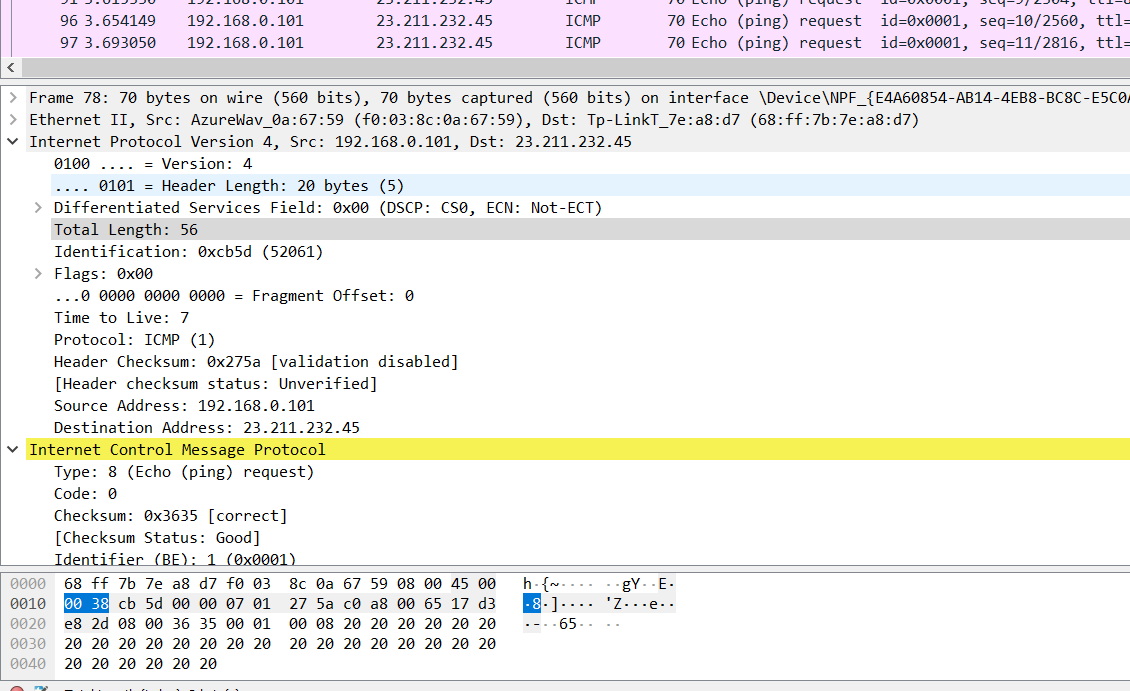


### 4. Отсортируйте отслеженные пакеты по их исходному IP-адресу; для этого щелкните по заголовку столбца Source. Выберите первое сообщение эхо-запроса, отосланное вашим компьютером по протоколу ICMP, и раскройте раздел Internet Protocol.

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

TTL, header checksum, identification

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

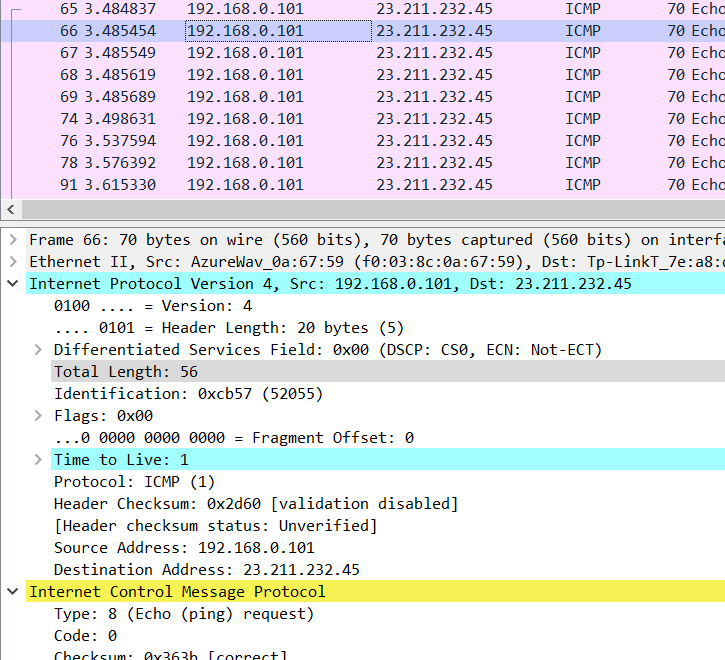
Не изменяются все остальные:  


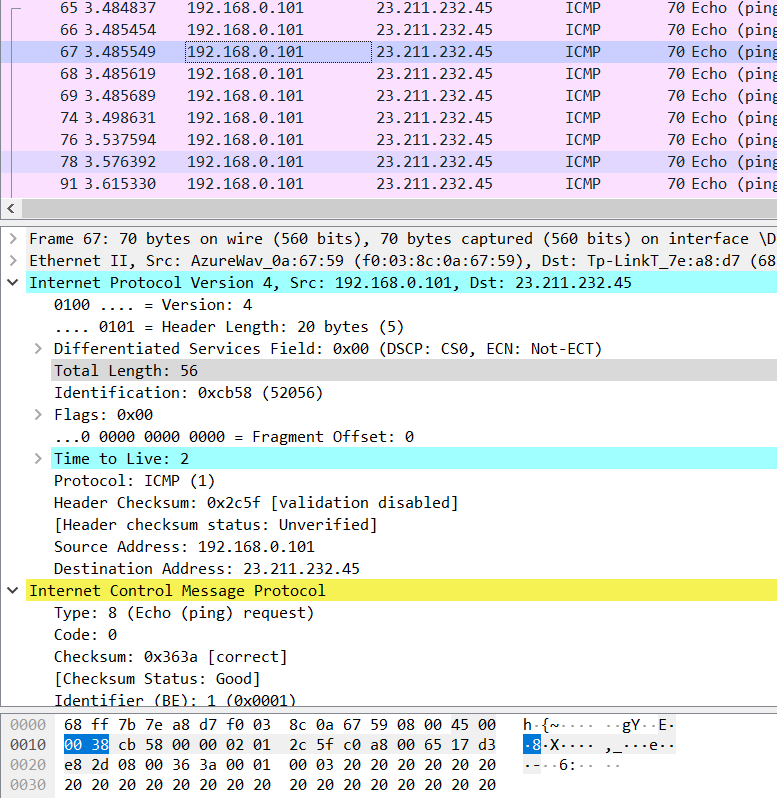
Неизменными должны быть: Version, Header Length, Total Length, Protocol.

Изменяться должны: Header Checksum, Identification

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

Да, закономерность есть. Оно увеличивается на 1.

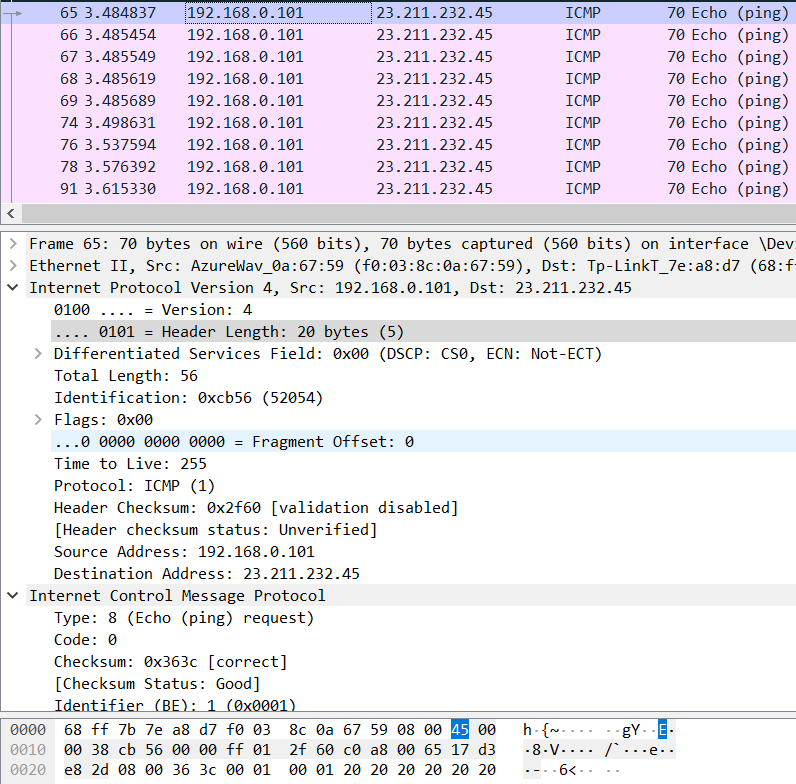




### 5. Какое значение содержится в поле Identification (Идентификация), а какое – в поле TTL?

Identification: 0xcb56 (52054)

Time to Live: 255



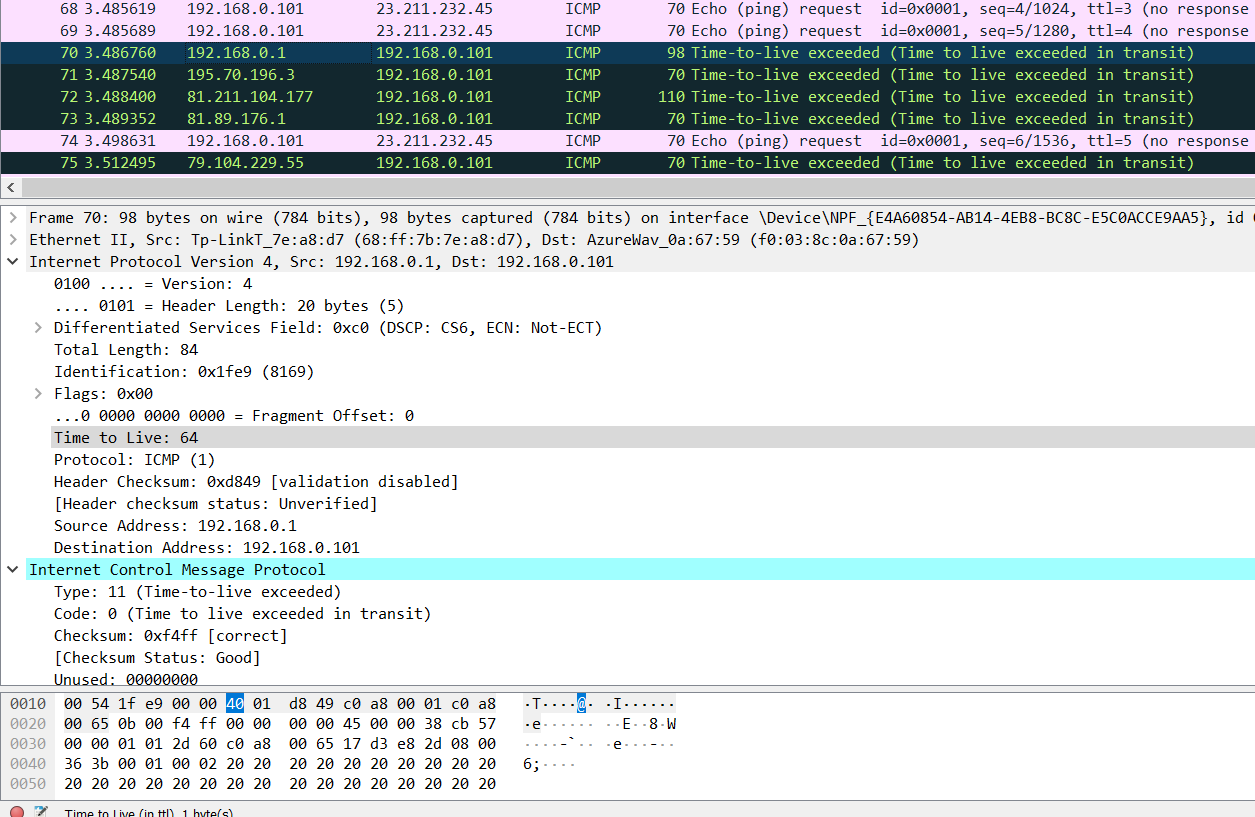
### 6. Остаются ли эти значения неизменными во всех сообщениях протокола ICMP, где содержится информация об истечении предписанного времени жизни; рассмотрите только те из таких сообщений, которые поступили на компьютер с ближайшего (первого транзитного) маршрутизатора.

Значения меняются.

### 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?

Identification: 0x1fe9 (8169)

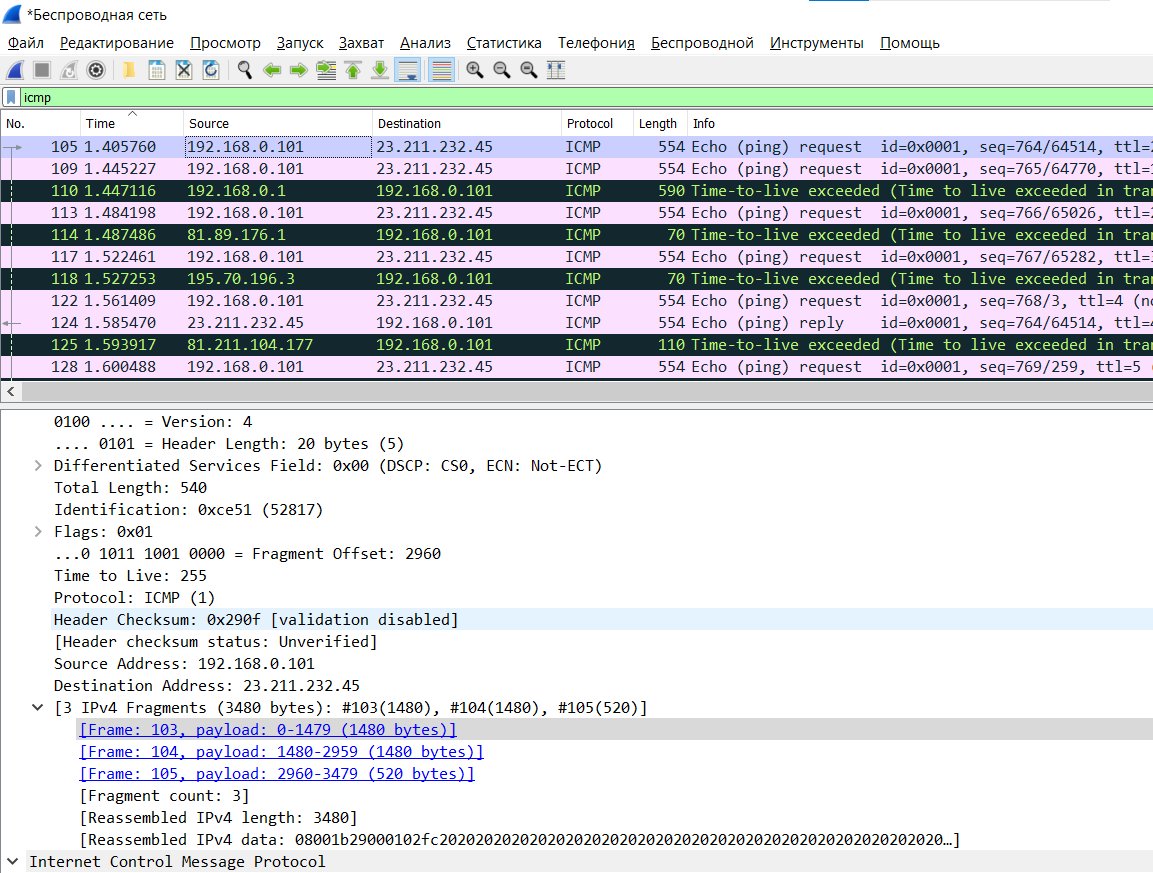
Time to Live: 64



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 IPдейтаграммами? Если да, то сколько фрагментов было создано?

Было создано 3 фрагмента.



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

Header ckecksum, Total Length, Flags, Fragment offset.