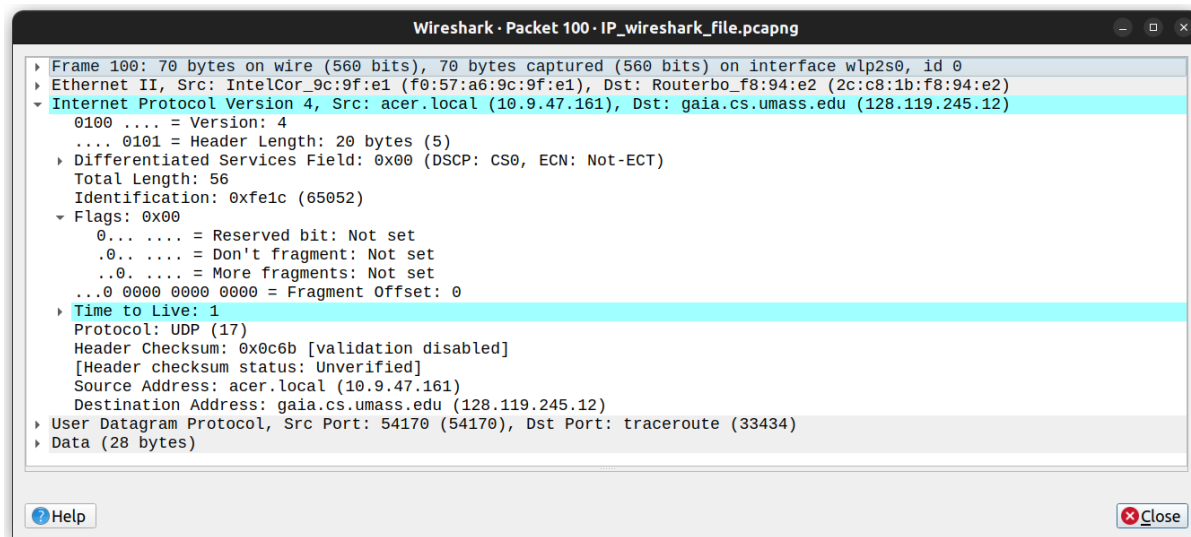


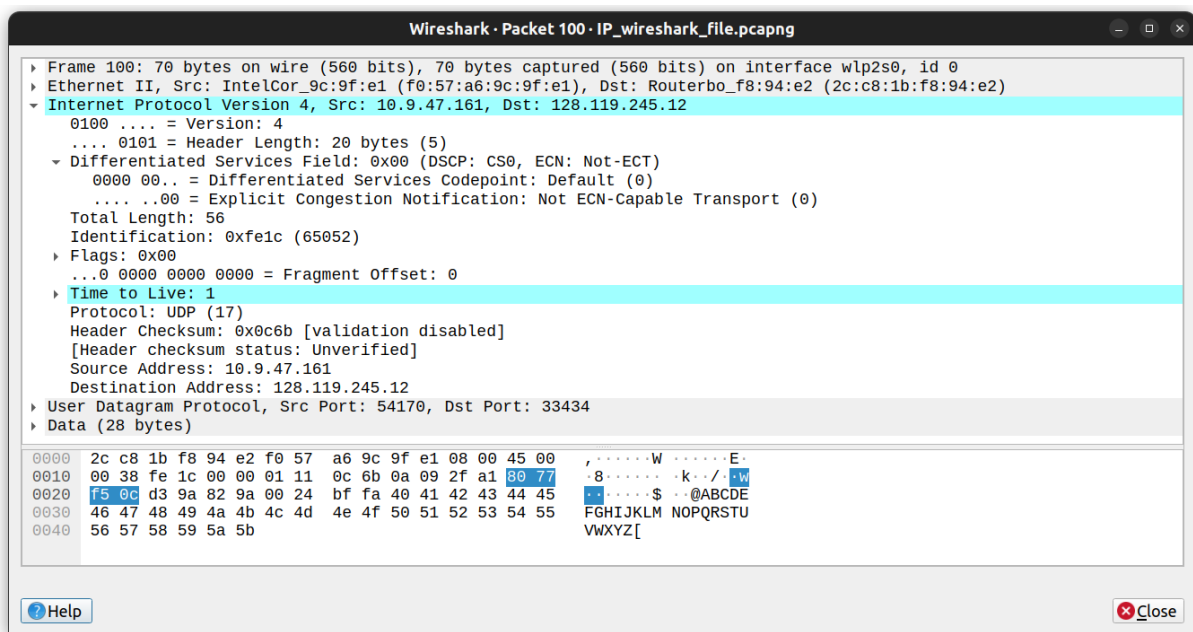
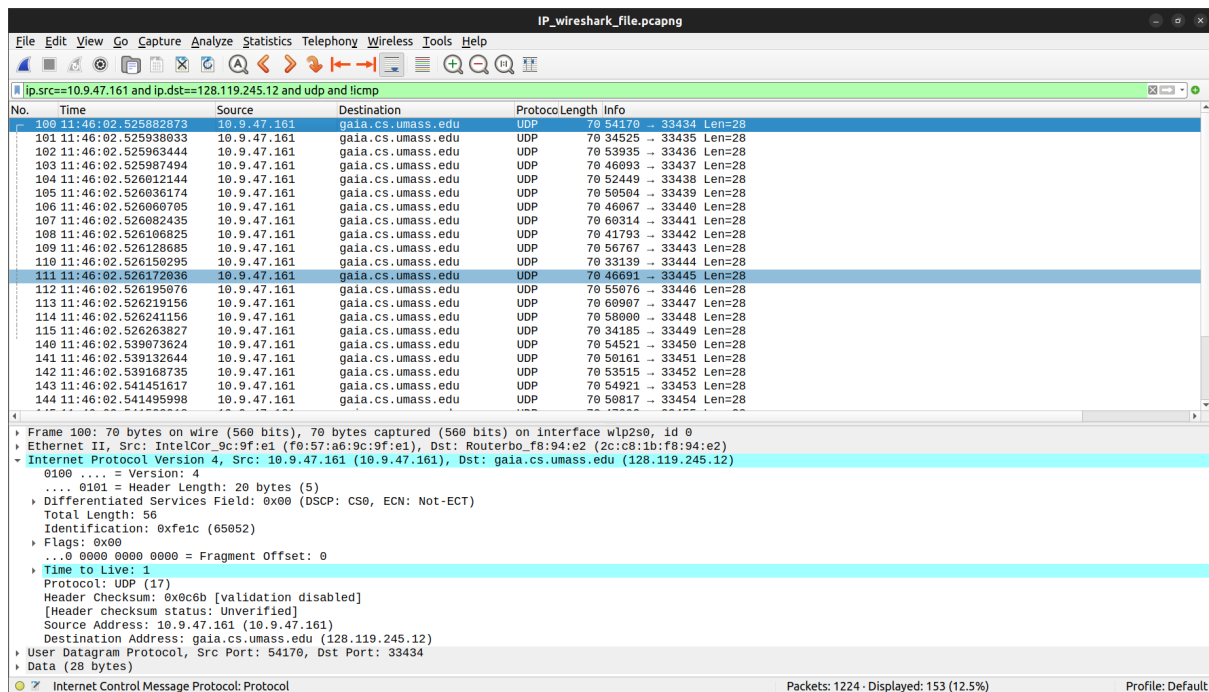
Часть 1: Базовый IPv4

Выберите первый сегмент UDP, отправленный вашим компьютером через трассировку команда для *gaia.cs.umass.edu*. Разверните часть пакета Интернет-протокола в окне сведений о пакете.



1. Какой IP-адрес вашего компьютера?
 - IP-адрес acer-local - 10.9.47.161
2. Каково значение поля времени жизни (TTL) в заголовке этой дейтаграммы IPv4?
 - Time to Live - 1
3. Какое значение имеет поле протокола верхнего уровня в заголовке этой дейтаграммы IPv4?
 - Protocol - 17 (UDP)
4. Сколько байтов в заголовке IP?
 - Header length - 20 байтов
5. Сколько байтов содержится в полезной нагрузке IP-датаграммы? Объясните, как вы определили количество байтов полезной нагрузки.
 - Header length - 20, Total length - 56. Тогда полезная нагрузка имеет размер 36
6. Фрагментирована ли эта IP-датаграмма? Объясните, как вы определили, была ли дейтаграмма фрагментирована.
 - IP-датаграмма не фрагментирована, так как не установлен флаг *More fragments*, и нет предшествующих пакетов IPv4 с установленным флагом *More fragments*
 - Фактический размер датаграммы равен ожидаемому (заданному при вызове *traceroute*)

Далее давайте посмотрим на последовательность сегментов UDP, отправляемых с вашего компьютера через *traceroute*, предназначенных для 128.119.245.12



7. Какие поля в дейтаграмме IP всегда изменяются при переходе от одной дейтаграммы к другой в этой серии UDP-сегментов? Почему?

- Изменяются следующие поля: *Identification*, *Header Checksum*, *Time to Live*.
- Поле *Identification* - уникальный идентификатор датаграммы, поэтому это поле изменяется.

- Поле *Header Checksum* - контрольная сумма заголовка датаграммы, т.к. заголовки разные (в том числе из-за поля *Identification*), то и контрольные суммы разные.
- Поле *Time to Live* - время жизни датаграммы, изменяется из-за того, что утилита *traceroute* постепенно увеличивает время жизни датаграмм, чтобы выполнить трассировку пути.

8. Какие поля в этой последовательности IP-датаграмм остаются неизменными?

Почему?

- Неизменными остаются поля *Version*, *Header Length*, *Differentiated Services*, *Total Length*, *Flags*, *Protocol*, *Source Address*, *Destination Address*
- Формат датаграммы, источник и получатель не изменяются утилитой *traceroute*

9. Опишите шаблон, который вы видите в значениях в поле *Identification* IP-датаграмм, отправляемых вашим компьютером.

- Никакого шаблона не наблюдается, значения поля *Identification* случайны

Теперь давайте посмотрим на ICMP-пакеты, возвращаемые на ваш компьютер промежуточными маршрутизаторами, где значение TTL было уменьшено до нуля.

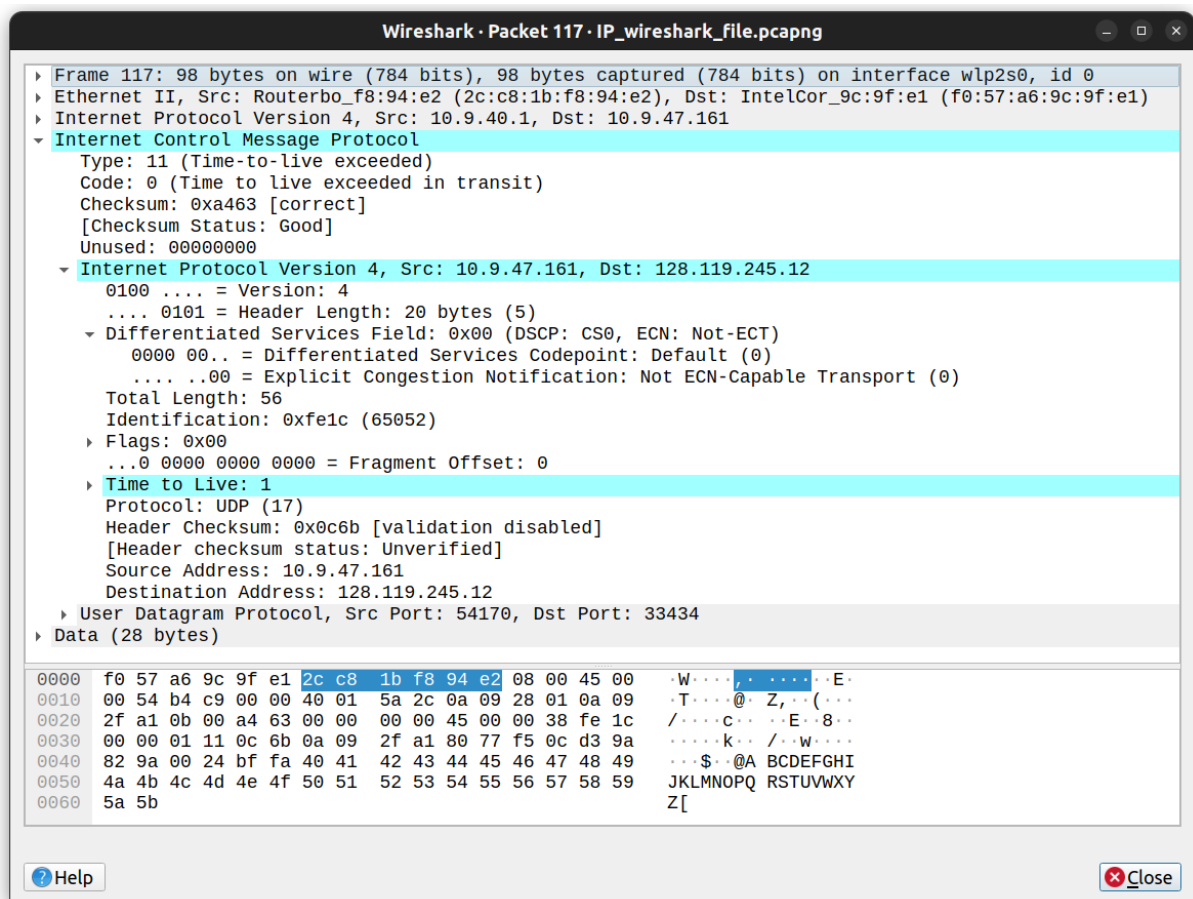
No.	Time	Source	Destination	Protocol	Length	Info
116	11:46:02.528495549	10.9.40.1	10.9.47.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
117	11:46:02.528496129	10.9.40.1	10.9.47.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
118	11:46:02.528496199	10.9.40.1	10.9.47.161	ICMP	98	Time-to-live exceeded (Time to live exceeded in transit)
119	11:46:02.529008184	84.237.49.155	10.9.47.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
120	11:46:02.529008454	84.237.49.73	10.9.47.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
121	11:46:02.529008524	84.237.49.155	10.9.47.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
122	11:46:02.529008604	84.237.49.73	10.9.47.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
123	11:46:02.529008674	84.237.49.73	10.9.47.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
124	11:46:02.529008744	84.237.49.155	10.9.47.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
125	11:46:02.529008824	95.170.130.189	10.9.47.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
126	11:46:02.529008894	95.170.130.189	10.9.47.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
127	11:46:02.529008964	95.170.130.189	10.9.47.161	ICMP	70	Time-to-live exceeded (Time to live exceeded in transit)
131	11:46:02.5290095713	217.150.54.70	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
132	11:46:02.5290095783	217.150.54.70	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
134	11:46:02.532083575	217.150.54.70	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
159	11:46:02.504066337	149.6.168.50	10.9.47.161	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
162	11:46:02.598810905	149.6.168.50	10.9.47.161	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
163	11:46:02.598810825	149.6.168.50	10.9.47.161	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
181	11:46:02.604841095	130.117.50.225	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
184	11:46:02.607861195	154.54.61.241	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
186	11:46:02.611101037	154.54.61.241	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
188	11:46:02.616202848	154.54.61.237	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
190	11:46:02.627942604	154.54.61.229	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
192	11:46:02.628893333	154.54.61.229	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
198	11:46:02.632837132	154.54.61.221	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
200	11:46:02.646531218	154.54.38.205	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
202	11:46:02.655949661	154.54.36.89	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
203	11:46:02.655950251	154.54.36.89	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
207	11:46:02.690985278	154.54.38.209	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
208	11:46:02.690985508	154.54.38.205	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
215	11:46:02.703387881	154.54.56.93	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
220	11:46:02.705871356	154.54.56.93	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
223	11:46:02.769947170	154.54.82.34	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
224	11:46:02.769947950	154.54.82.34	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
227	11:46:02.776191822	130.117.51.41	10.9.47.161	ICMP	182	Time-to-live exceeded (Time to live exceeded in transit)
229	11:46:02.782100861	154.54.82.34	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
231	11:46:02.790667186	154.54.40.182	10.9.47.161	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)

Frame 116: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface wlp2s0, id 0

Identification (ip.id), 2 bytes

Packets: 1224 - Displayed: 136 (11.1%)

Profile: Default



10. Какой протокол верхнего уровня указан в IP-датаграммах, возвращаемых маршрутизаторами?

- Protocol - ICMP

11. Похожи ли значения в полях *Identification* (в последовательности всех пакетов ICMP от всех маршрутизаторов) на ваш ответ на вопрос 9 выше?

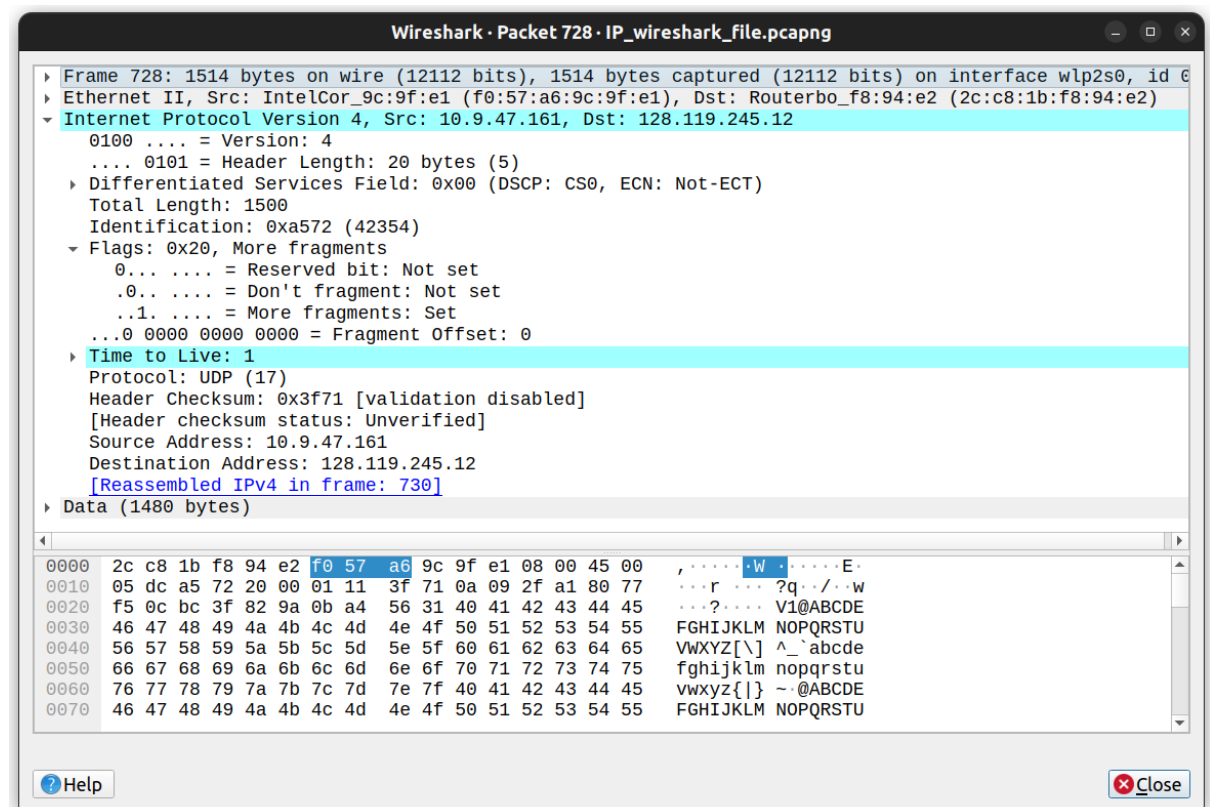
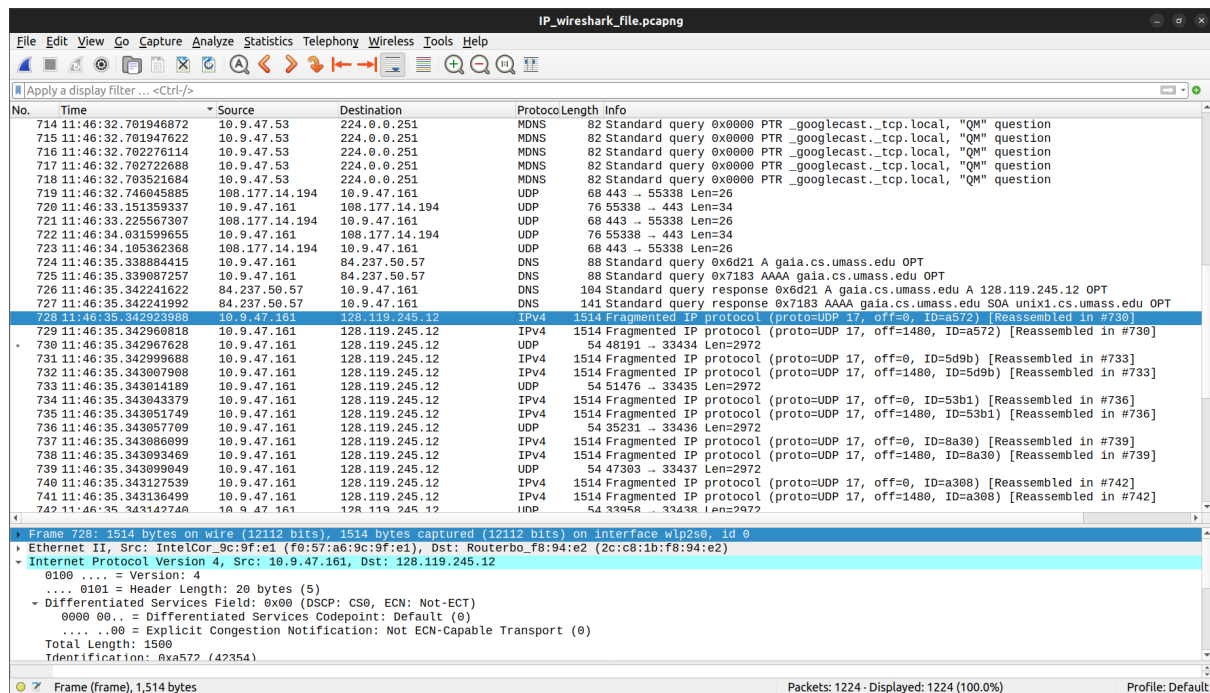
- Нет, значения поля *Identification* расположены последовательно от каждого маршрутизатора

12. Одинаковы ли значения полей *TTL* во всех ICMP-пакетах от всех маршрутизаторов?

- Нет, значения поля *TTL* одинаковы для каждого маршрутизатора

Часть 2: Фрагментация

Найдите первую IP-дейтаграмму, содержащую первую часть сегмента, отправленного на 128.119.245.12 отправлено вашим компьютером с помощью команды *traceroute* на *gaia.cs.umass.edu* , после того как вы указали, что длина пакета *traceroute* должна быть 3000.



13. Был ли этот сегмент фрагментирован более чем на одну IP-датаграмму?

- Сегмент фрагментирован на 3 датаграммы

14. Какая информация в заголовке IP указывает на то, что эта дейтаграмма была фрагментирована?

- На наличие фрагментации указывает установленный флаг *More fragments*

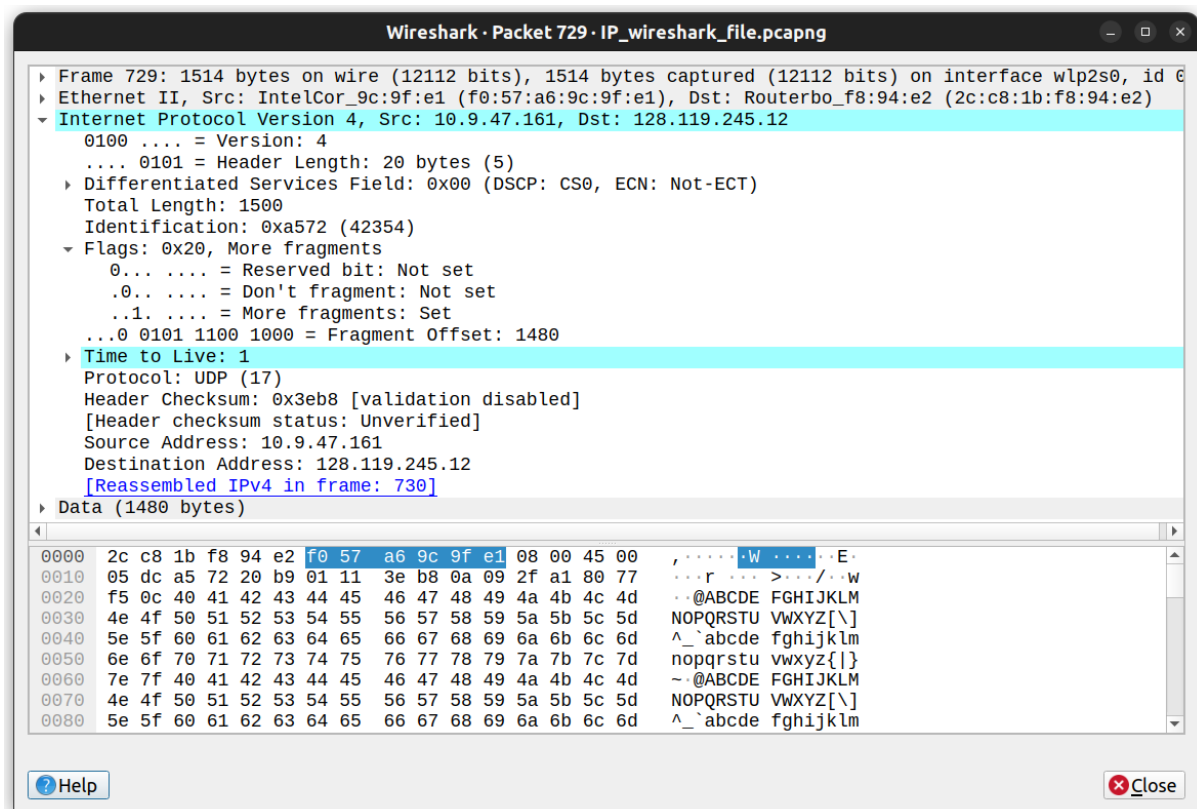
15. Какая информация в заголовке IP для этого пакета указывает, является ли это первым фрагментом или последним фрагментом?

- Датаграмма является первым фрагментом, на это указывает значение поля *Fragment Offset* равное 0

16. Сколько байтов в этой IP-датаграмме (заголовок плюс полезная нагрузка)?

- *Total Length* - 1500 байтов

Теперь проверьте дейтаграмму, содержащую второй фрагмент фрагментированного сегмента UDP.



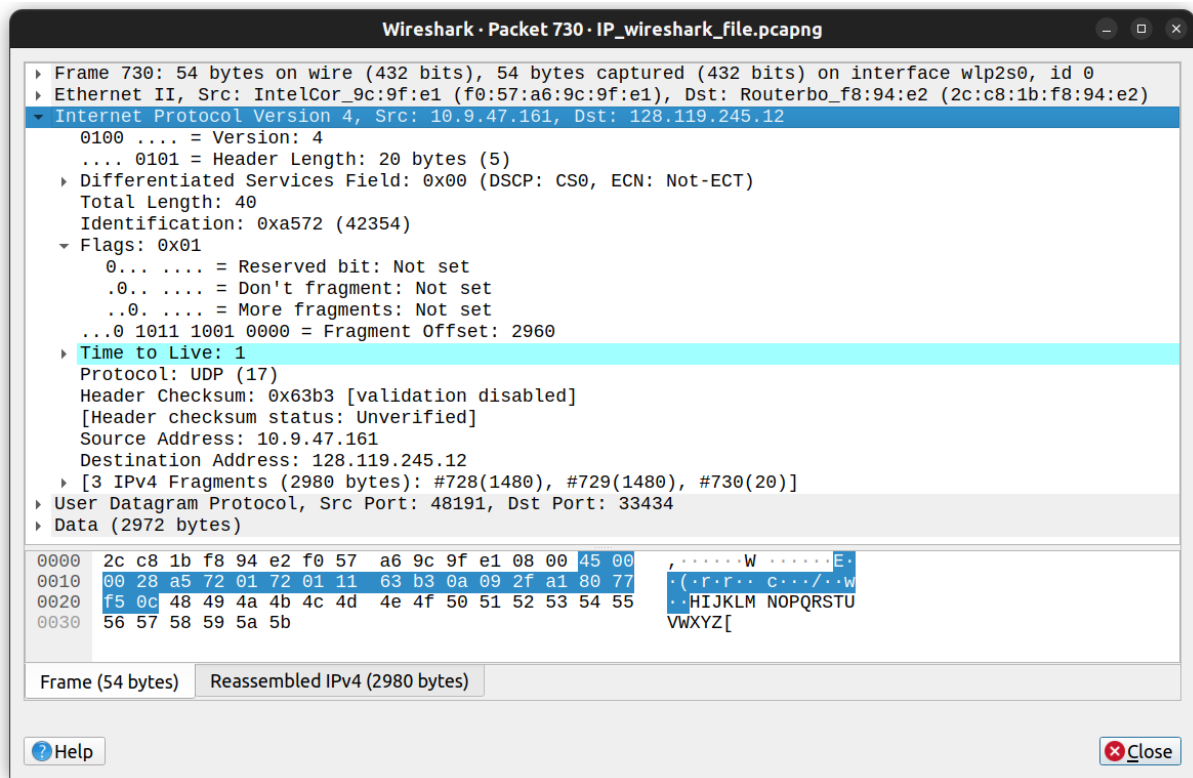
17. Какая информация в заголовке IP указывает на то, что это не первый фрагмент дейтаграммы?

- Фрагмент не является первым, об этом свидетельствует ненулевое значение поля *Fragment Offset*

18. Какие поля изменяются в заголовке IP между первым и вторым фрагментом?

- Изменились поля *Fragment Offset* и *Header Checksum*

Теперь найдите дейтаграмму IP, содержащую третий фрагмент исходного сегмента UDP.

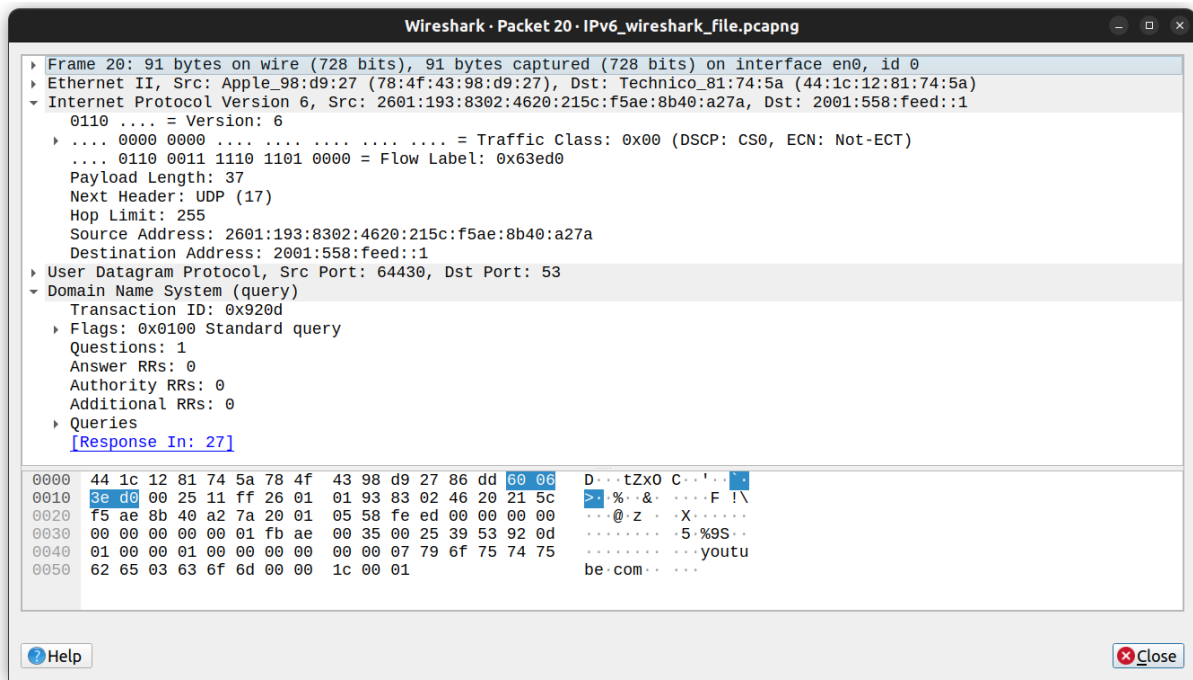


19. Какая информация в заголовке IP указывает на то, что это последний фрагмент этого сегмента?

- Фрагмент является последним, т.к. снят флаг *More fragments*, свидетельствующий о том, что больше фрагментов нет

Часть 3: IPv6

Откройте файл *ip-wireshark-trace2-1.pcapng* в ZIP-файле трассировок. Начнем с более подробного рассмотрения 20-ого пакета в этой трассировке. Это DNS-запрос (содержащийся в дейтаграмме IPv6) к DNS-серверу IPv6 для IPv6-адреса *youtube.com*. Тип запроса DNS AAAA используется для преобразования имен в IP-адреса IPv6.



20. Какой IPv6-адрес компьютера, отправляющего запрос DNS AAAA?

- IPv6-адрес источника - 2601:193:8302:4620:215c:f5ae:8b40:a27a

21. Какой адрес назначения IPv6 для этой дейтаграммы?

- IPv6-адрес получателя - 2001:558:feed::1 (2001:558:feed:0:0:0:0:1)

22. Каково значение метки потока для этой дейтаграммы?

- *Flow Label* - 0x63ed0

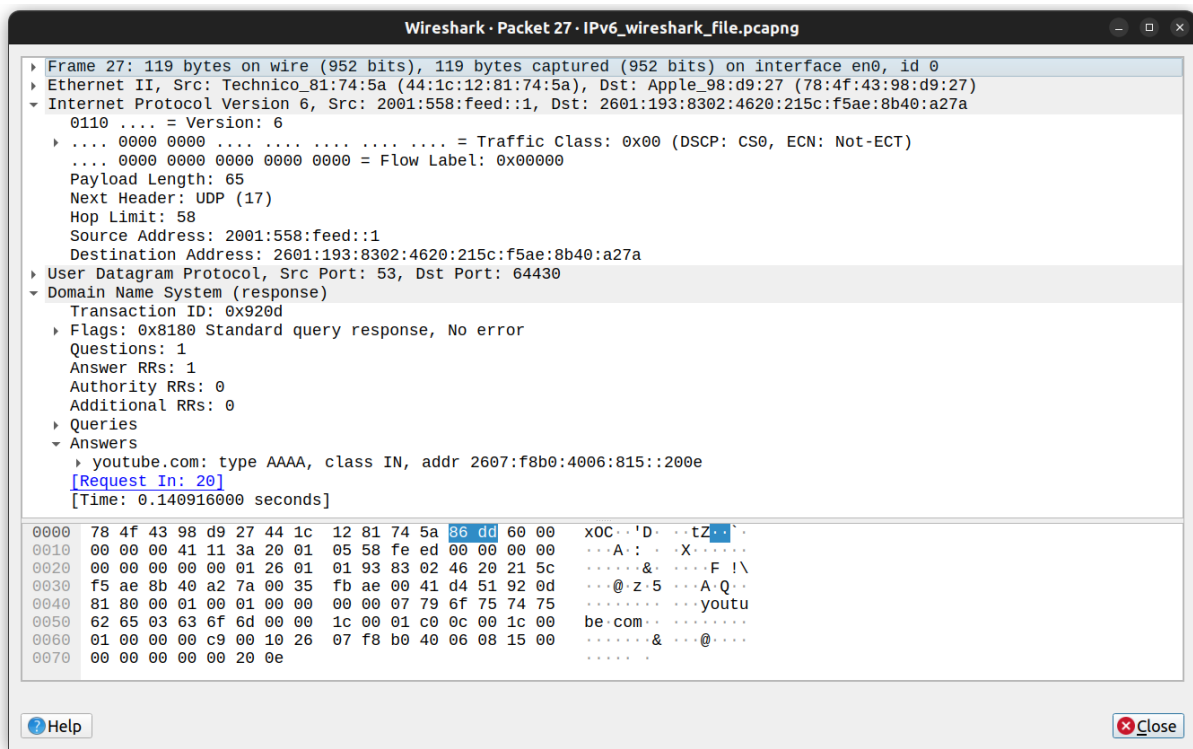
23. Сколько полезных данных содержится в этой дейтаграмме?

- *Payload Length* - 37

24. Каков протокол верхнего уровня, по которому полезная нагрузка этой дейтаграммы будет доставлена в пункт назначения?

- *Next Header* - UDP (17)

Наконец, найдите ответ IPv6 DNS на запрос IPv6 DNS AAAA, сделанный в 20-ом пакете этой трассировки.



25. Сколько адресов IPv6 возвращается в ответ на этот запрос AAAA?

- Вернулся один IPv6-адрес

26. Какой первый из IPv6-адресов, возвращенных DNS для youtube.com?

- IPv6-адрес - 2607:f8b0:4006:815::200e (2607:f8b0:4006:815:0:0:0:200e)