Санкт-Петербургский государственный политехнический университет

Институт компьютерных наук и кибербезопасности

Высшая школа компьютерных технологий и информационных систем

**Отчет по лабораторной работе №4**

**по курсу «Технологии компьютерный сетей»**

«Wireshark: ICMP & IP»

**Работу выполнил студент группы №5130901/10203:**

Алексеев Лев Сергеевич

Подпись:

**Работу принял преподаватель:**

Богач Наталья Владимировна

Подпись:

Санкт-Петербург

2024

**Wireshark: ICMP**

В этой лабораторной работе мы исследуем ряд аспектов протокола ICMP:

• ICMP-сообщения, генерируемые программой Ping;

• ICMP-сообщения, генерируемые программой Traceroute;

• Формат и содержимое ICMP-сообщения.

Начнем нашу работу над протоколом ICMP с захвата пакетов, сгенерированных программой Ping.

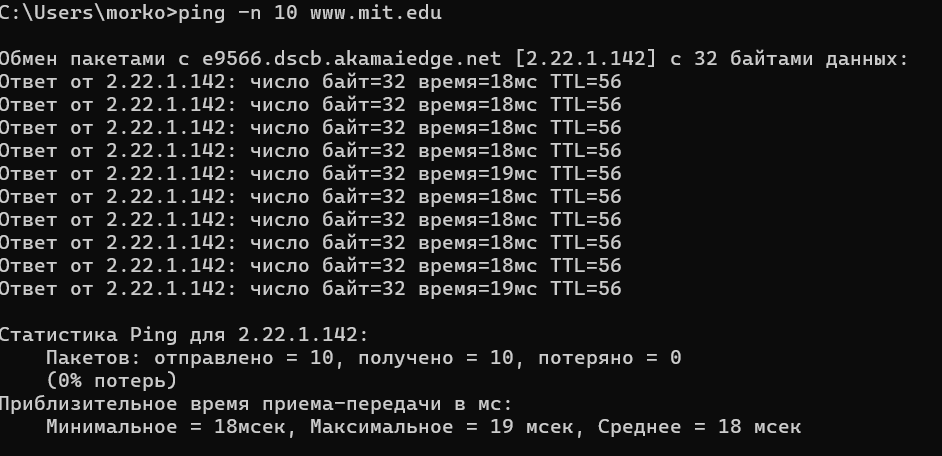
****

Рис. 1. Снимок после выполнения запроса PING

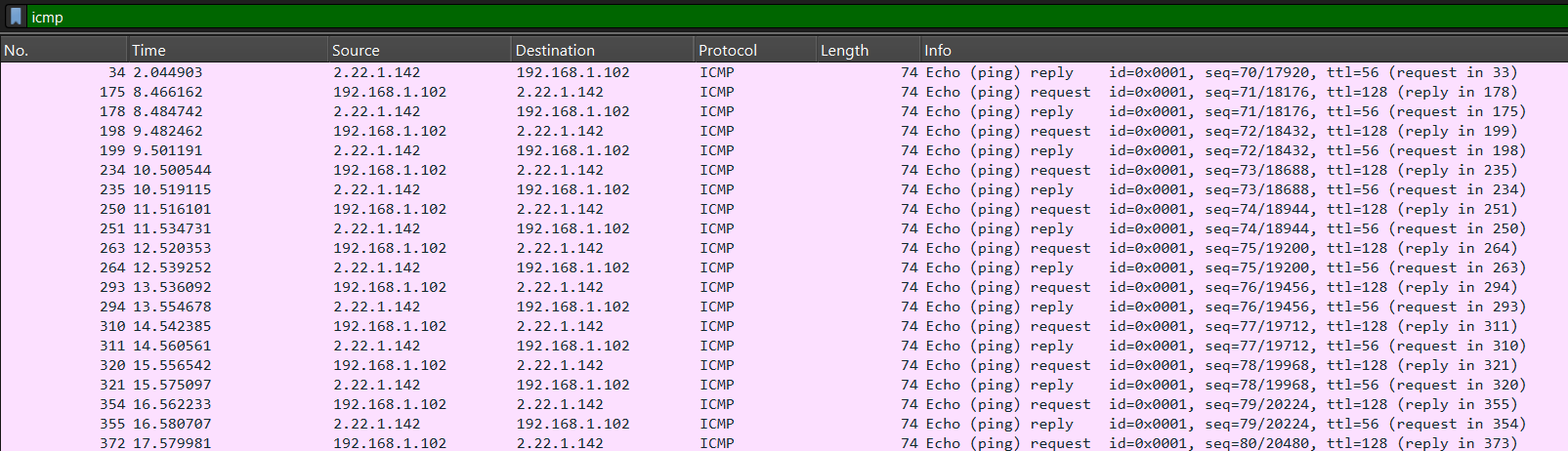


Рис. 2. Вывод Wireshark для программы Ping

1. Каков IP-адрес вашего хоста? Каков IP-адрес хоста назначения?

IP-адрес моего хоста – 192.168.1.102. IP-адрес хоста назначения – 2.22.1.142

1. Почему ICMP-пакет не обладает номерами исходного и конечного портов?

ICMP-пакет не обладает номерами исходного и конечного портов, так как он предназначен для передачи информации сетевого уровня между хостами и маршрутизаторами, а не между процессами прикладного уровня. Каждый ICMPпакет обладает «типом» (Type) и «кодом» (Code). Комбинация типа и кода идентифицирует конкретное полученное сообщение. Поскольку сетевое ПО само интерпретирует все ICMP-сообщения, номера портов не нужны, так как нет необходимости направлять ICMP-сообщение процессу прикладного уровня.

1. Рассмотрите один из ping-запросов, отправленных вашим хостом. Каковы ICMP-тип и кодовый номер этого пакета? Какие еще поля есть в этом ICMP-пакете? Сколько байт приходится на поля контрольной суммы, порядкового номера и идентификатора?

ICMP-тип имеет значение 8, а код – 0. Кроме того, у ICMP-пакета есть контрольная сумма, идентификатор, порядковый номер и поля данных. Поля контрольной суммы, идентификатора и порядкового номера содержат по два байта каждое.

1. Рассмотрите соответствующий ping-пакет, полученный в ответ на предыдущий. Каковы ICMP-тип и кодовый номер этого пакета? Какие еще поля есть в этом ICMPпакете? Сколько байт приходится на поля контрольной суммы, порядкового номера и идентификатора?

ICMP-тип имеет значение 0, код – 0. Кроме того, у ICMP-пакета есть контрольная сумма, идентификатор, порядковый номер и поля данных. Поля контрольной суммы, идентификатора и порядкового номера содержат по два байта каждое.

Продолжим работу с протоколом ICMP и выполним захват пакетов, сгенерированных программой Traceroute.



Рис. 3. Снимок после выполнения запроса tracert

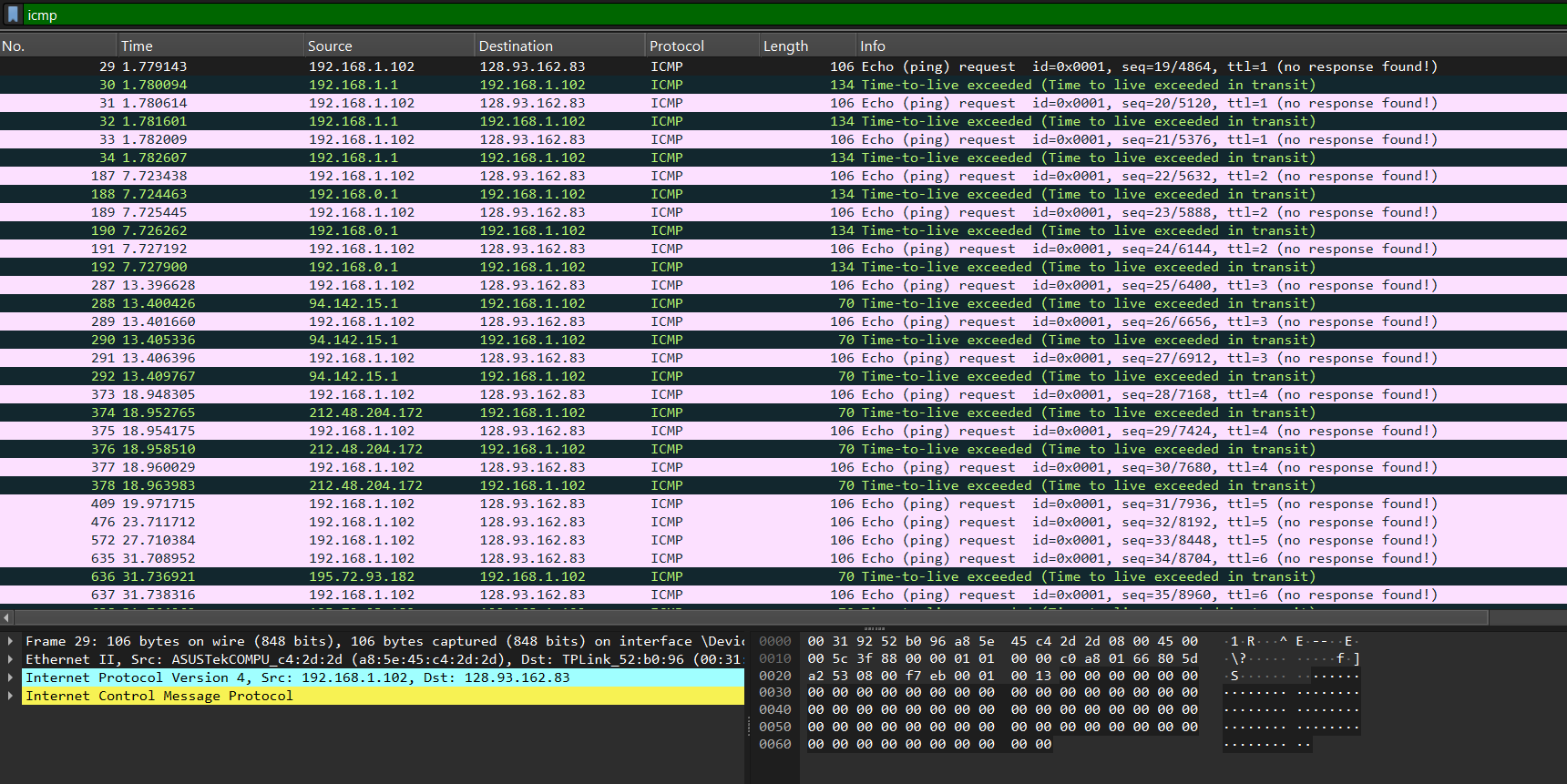


Рис. 4. Сообщение об ошибке, передаваемое по протоколу ICMP

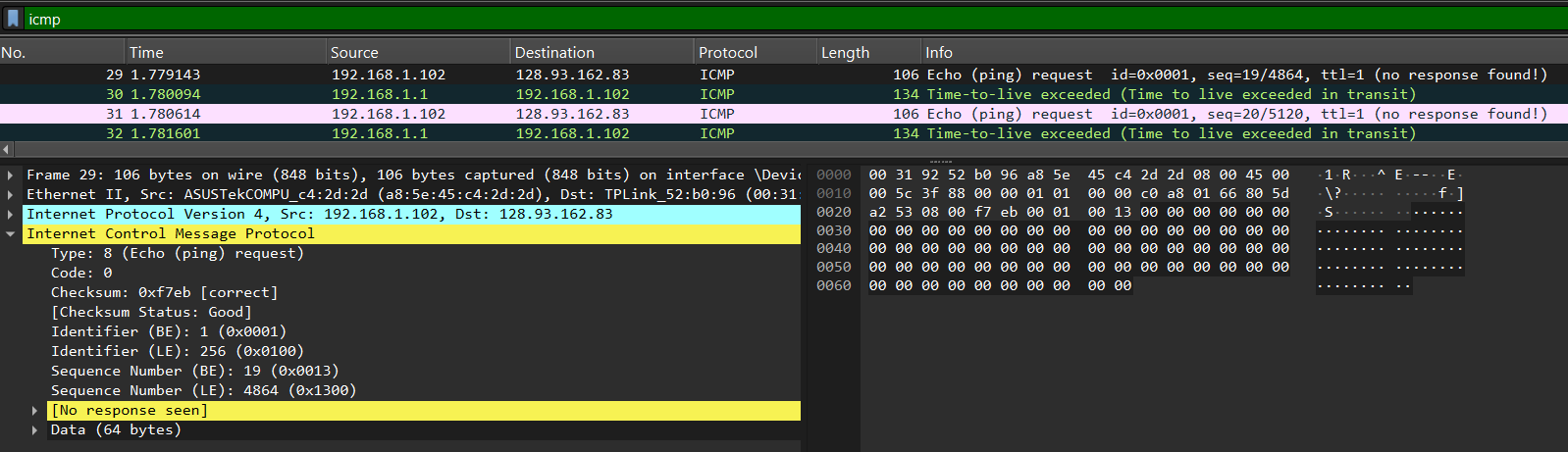


Рис. 5. Сообщение с эхо-запросом, передаваемое по протоколу ICMP

1. Каков IP-адрес вашего хоста? Каков IP-адрес хоста назначения?

IP-адрес моего хоста – 192.168.1.1. IP-адрес хоста назначения – 128.93.162.83.

1. Если по протоколу ICMP будут посылаться пакеты UDP (как в Unix/Linux), то сохранится ли за протоколом IP номер 01 (в зондирующих пакетах)? Если нет – какой номер это будет?

В таком случае номер IP-протокола будет 0x11.

1. Рассмотрите ICMP-пакет с эхо-запросом на вашем скриншоте. Отличается ли он от ICMP-пакетов с ping-запросами, изученных в первой части этой работы? Если да – то как?

ICMP-пакет с эхо-запросом будет иметь такие же поля, как и пакеты с ping запросами

1. Рассмотрите на вашем скриншоте ICMP-пакет с сообщением об ошибке. В нем больше полей, чем в ICMP-пакете с эхо-запросом. Какая информация содержится в этих дополнительных полях?

ICMP-пакеты с сообщениями об ошибке не такие, как ping-пакеты с запросами. В пакете с сообщением об ошибке содержится как IP-заголовок, так и первые 8 байт исходного ICMP-пакета, в котором произошла ошибка.

1. Рассмотрите три последних ICMP-пакета, полученных исходным хостом. Чем эти пакеты отличаются от ICMP-пакетов, сообщающих об ошибках? Чем объясняются такие отличия?

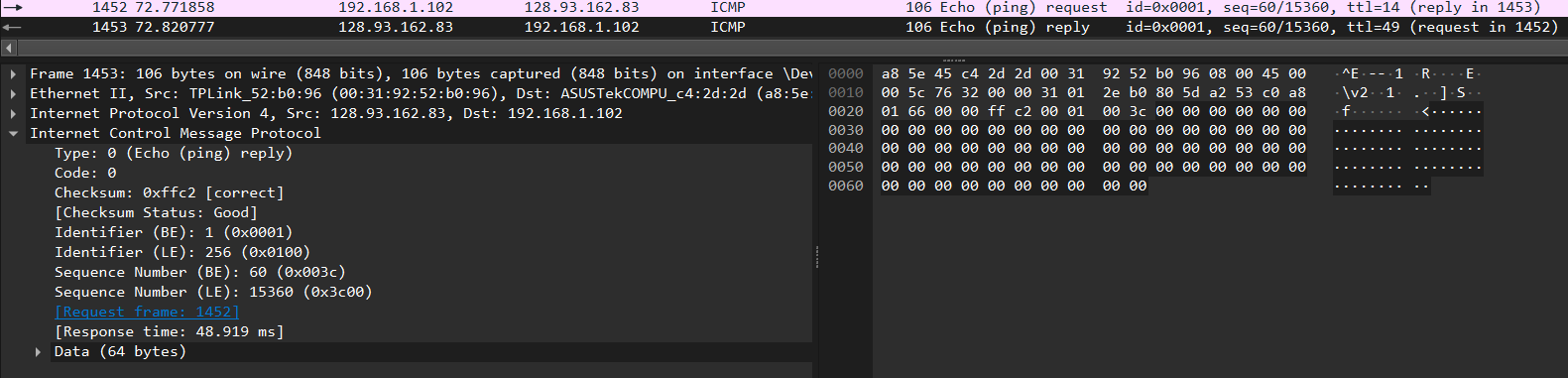


Рис. 6. Три последних ICMP-пакета

Тип сообщения у последних трех ICMP-пакетов равен 0 (эхо-запрос), а не 11 (предписанное время жизни исчерпано). Типы отличаются, так как дейтаграммы успевают достичь хоста назначения до того, как истечет их предписанное время жизни

1. Если измерения выполняются при помощи программы tracert, есть ли такой канал, задержка в котором существенно превышает среднее значение? Обратитесь к скриншоту с рис. 4 – есть ли там канал, задержка в котором значительно выше, чем в остальных? Можете ли вы, опираясь на имена маршрутизаторов, определить местоположение двух маршрутизаторов, расположенных на обоих концах этого канала?

Каналы, работающие между этапами (4,6) и (6,9), задержка в котором существенно выше средней. Это линия связи, идущая из Северо-Запада России во Франкфурт и потом в Париж. На рис. 3 можно увидеть связанные с этой линией имена маршрутизаторов.

**Wireshark: IP**

Чтобы выполнить в этой лабораторной работе трассировку IP-дейтаграмм, воспользуемся программой traceroute и будем отсылать дейтаграммы разных размеров на тот или иной адрес назначения.

Важно, что маршрутизатор должен уменьшать на единицу значение в поле TTL каждой дейтаграммы, которую получает. Если значение в поле TTL достигает 0, маршрутизатор возвращает ICMP-сообщение (тип 11 – значение TTL исчерпано) хосту-отправителю. В результате такая дейтаграмма, которая имеет в поле TTL значение 1 (отправленная хостом, на котором выполняется программа traceroute), заставит маршрутизатор, расположенный в одном переходе от отправителя, вернуть отправителю сообщение протокола ICMP о том, что значение TTL достигло нуля.

Запустим программу traceroute так, чтобы она рассылала дейтаграммы разной длины. У меня система Windows, поэтому для начала установим программу PingPlotter и протестируем ее.

Затем начнем захват пакетов в программе Wireshark.

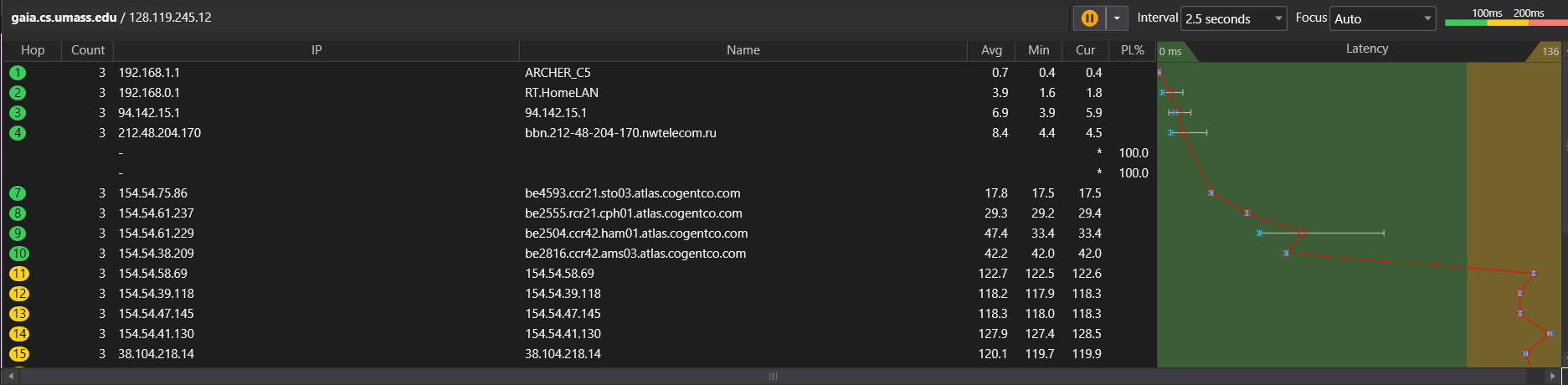


Рис. 1. Окно PingPlotter

В полученной трассе виден ряд эхо-запросов по протоколу ICMP. Эта информация отсылается компьютером, а сообщения ICMP о превышении предписанного времени жизни (обнулении поля TTL) возвращаются обратно с транзитных маршрутизаторов.

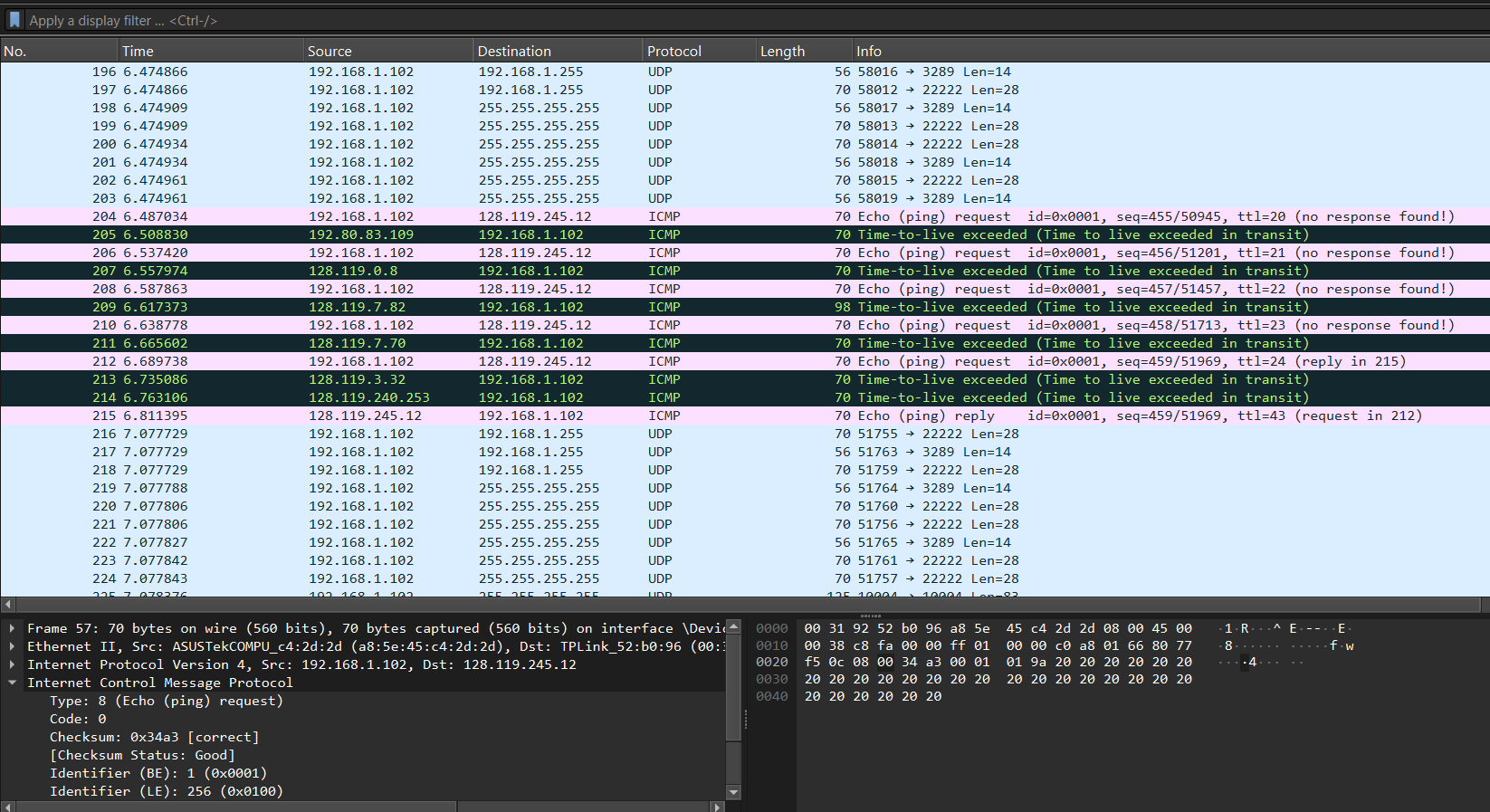


Рис. 2. Окно Wireshark

1. Каков IP-адрес вашего компьютера?

IP-адрес моего компьютера – 192.168.1.102

1. Какое значение указано в поле протокола верхнего уровня в заголовке IP-пакета?

В поле протокола верхнего уровня в заголовке IP-пакета содержится значение ICMP (0x01)

1. Сколько байт в IP-заголовке? Сколько байт приходится на полезную нагрузку IP-дейтаграммы? Опишите, как вы определили количество байт полезной нагрузки.

В IP-заголовке – 20 байт, общая длина дейтаграммы – 56 байт. Таким образом, полезная нагрузка IP-дейтаграммы составляет 36 байт.

1. Была ли фрагментирована эта IP-дейтаграмма? Объясните, как вы определили, была ли дейтаграмма фрагментирована.

Разряд More fragments (Дополнительные фрагменты) равен 0 – значит, данные не фрагментированы.

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

Всегда изменяются поля Identification (Идентификационная информация), Time to live (Предписанное время жизни) и Header checksum (Контрольная сумма заголовка).

1. Какие поля не меняются? Какие поля должны оставаться неизменными? Какие поля должны изменяться? Почему?

Следующие поля остаются неизменными во всех IP-дейтаграммах:

* Версия
* Длина заголовка
* Исходный IP
* Конечный IP
* Дифференцированные службы
* Протокол верхнего уровня

Поля, которые должны оставаться неизменными:

* Версия
* Длина заголовка
* Исходный IP
* Конечный IP
* Дифференцированные службы
* Протокол верхнего уровня

Поля, которые должны изменяться:

* Идентификационная информация
* Предписанное время жизни
* Контрольная сумма заголовка

1. Опишите паттерн, который вы прослеживаете в значениях поля Identification IP-дейтаграммы.

Паттерн заключается в том, что значение в поле идентификационной информации IP-пакета возрастает с каждым последующим эхо-запросом (пингом)

1. Какое значение содержится в поле Identification, а какое – в поле TTL?

Identification: 51452

TTL: 64

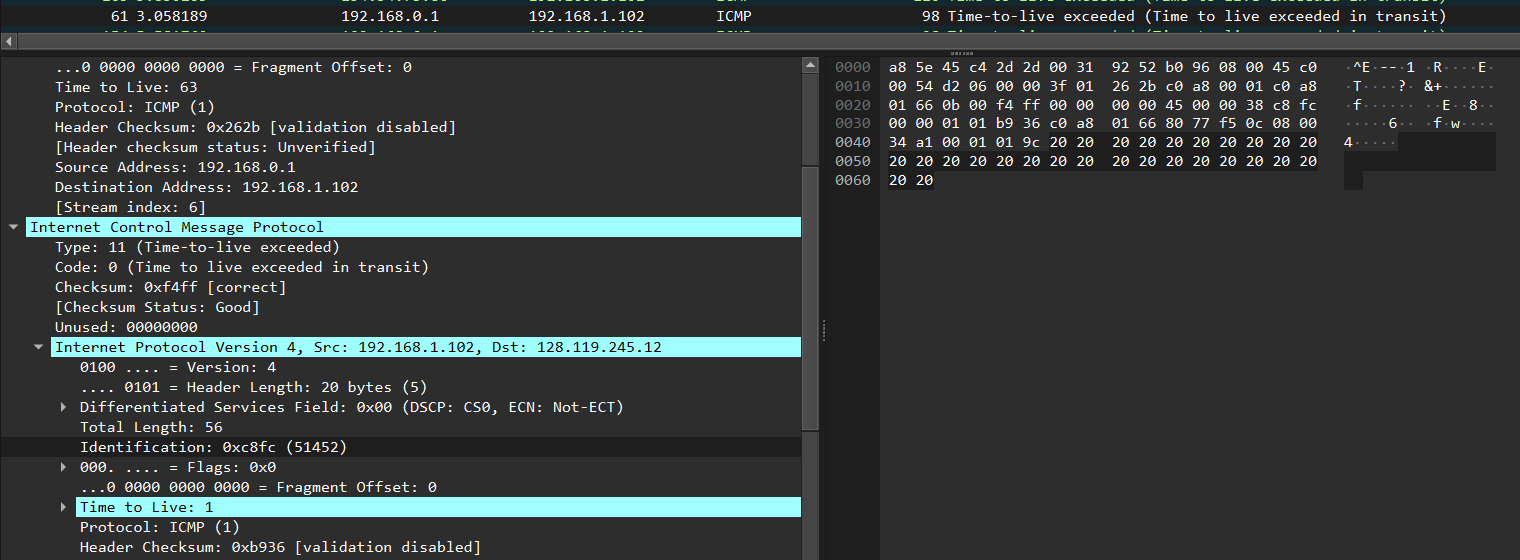


Рис. 3. Информация протокола IP

1. 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. Почему?

Поле с идентификационной информацией изменяется во всех откликах протокола ICMP, связанных с превышением предписанного времени жизни, поскольку в этом поле содержится уникальное значение.

Когда у двух или более IP-дейтаграмм данное значение совпадает, это означает, что такие дейтаграммы являются фрагментами одной и той же, более крупной дейтаграммы.

1. Найдите первое сообщение протокола ICMP с эхо-запросом, поступившее на ваш компьютер уже после того, как вы изменили значение Packet Size (Размер пакета) в pingplotter на 2000. Было ли это сообщение фрагментировано между двумя или более IP-дейтаграммами?

Да, этот пакет был фрагментирован между двумя или более дейтаграммами.

1. Распечатайте первую часть фрагментированной IP-дейтаграммы. Какая информация в IP-заголовке свидетельствует, что дейтаграмма была фрагментирована? Какая информация в IP-заголовке позволяет судить, какой фрагмент перед нами – первый или второй? Какова длина этой IP-дейтаграммы?

Установлен разряд «Flags» для дополнительных фрагментов. Это означает, что дейтаграмма была фрагментирована. Поскольку смещение фрагмента равно 0, нам известно, что это первый фрагмент. Общая длина первой дейтаграммы (с учетом заголовка) составляет 1500 байт

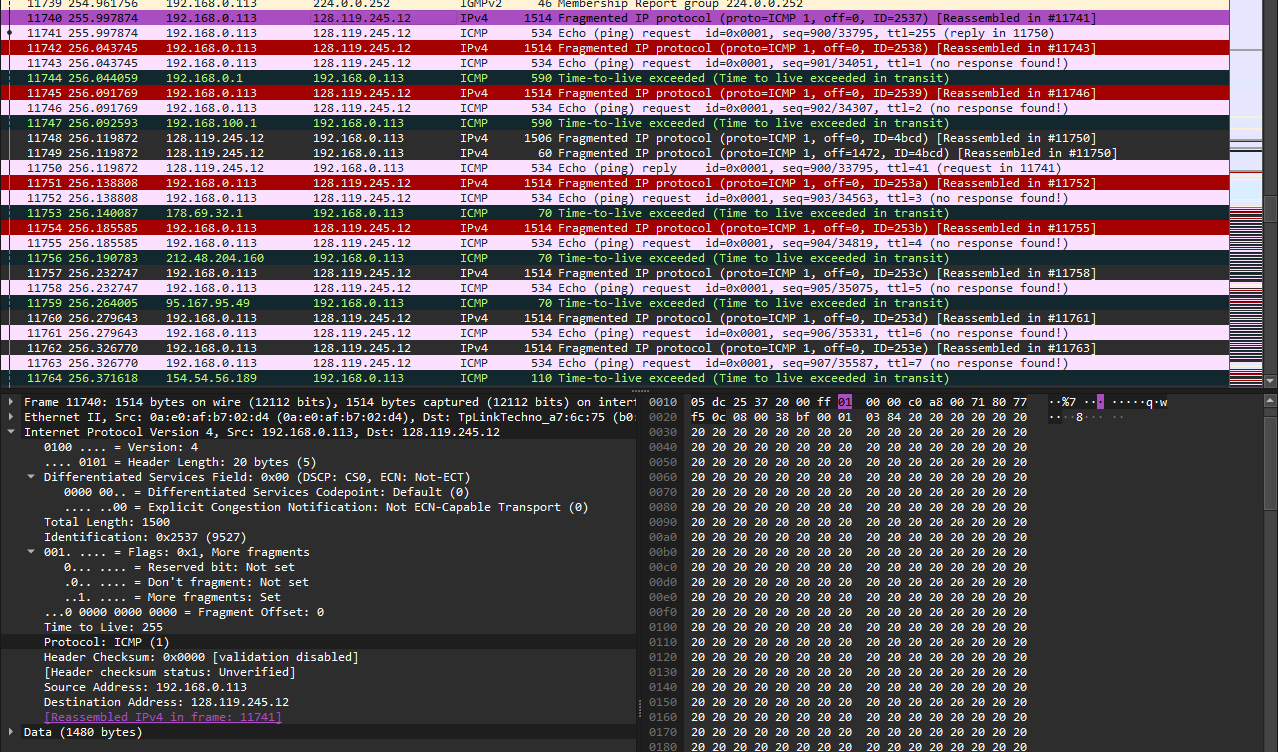


Рис. 4. Размер пакета эхо-запроса, передаваемого по протоколу ICMP = 2000

1. Распечатайте вторую часть фрагментированной IP-дейтаграммы. Какая информация в IP-заголовке свидетельствует, что это не первый фрагмент дейтаграммы? Есть ли и другие фрагменты этой дейтаграммы? Как вы это определили?

Мы можем определить, что это не первый фрагмент, поскольку смещение фрагмента равно 1480. Это последний фрагмент, так как флаг для дополнительных фрагментов не установлен.

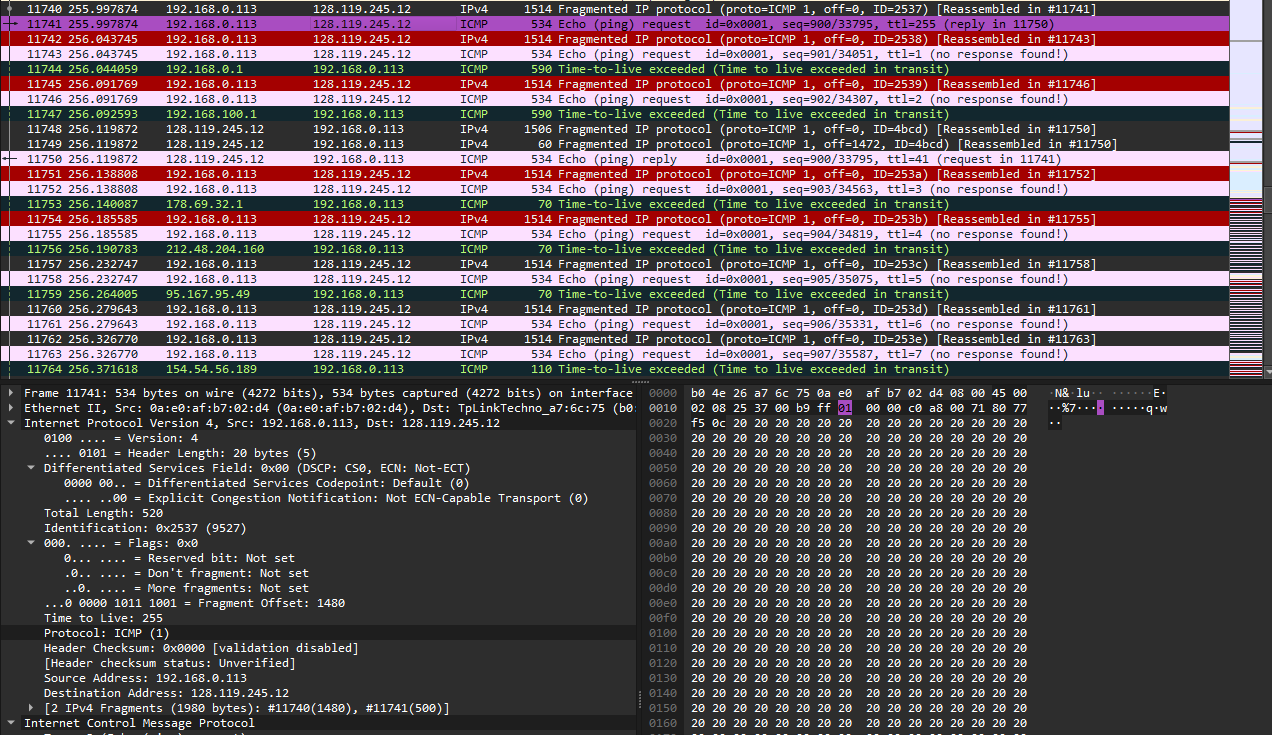


Рис. 5. Размер пакета эхо-запроса, передаваемого по протоколу ICMP = 2000, второй фрагмент

1. Какие поля в IP-заголовке отличаются в первом и во втором фрагменте?

У двух фрагментов отличается общая длина, флаги, смещение фрагмента, контрольная сумма

1. Сколько фрагментов было создано из исходной IP-дейтаграммы?

При изменении размера исходной дейтаграммы на 3500 она будет делиться на три фрагмента.

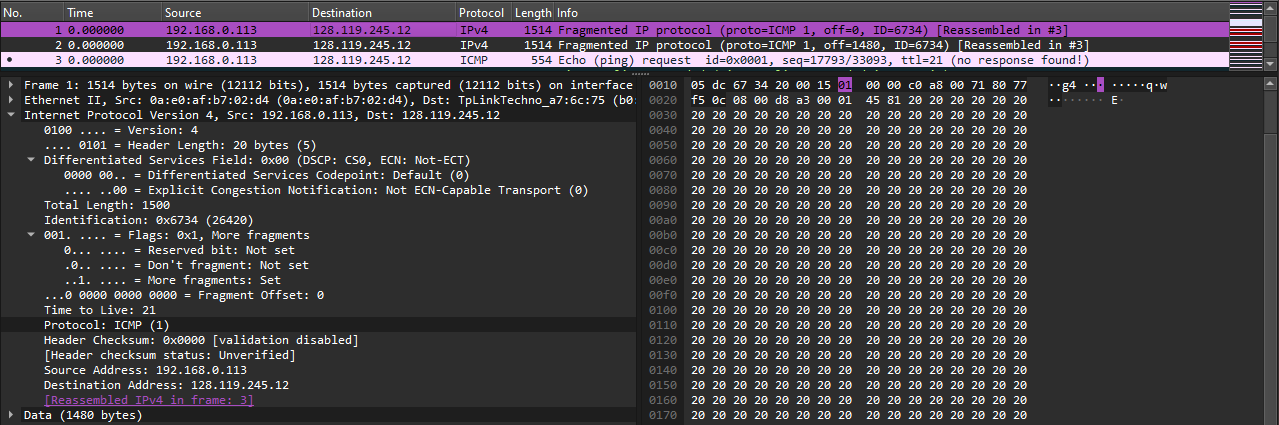


Рис. 6. Размер пакета эхо-запроса, передаваемого по протоколу ICMP = 3500

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

Поля IP-заголовка, которые изменяются между всеми пакетами: смещение фрагмента и контрольная сумма.

Наблюдается изменение длины между первыми двумя пакетами и последним пакетом, также видно изменения во флагах. Первые два фрагмента имеют общую длину по 1500, причем разряд дополнительных фрагментов у них равен единице. Длина последнего пакета равна 540, а разряд дополнительных пакетов у него равен нулю