Министерство образования Республики Беларусь

Учреждение образования

«Брестский Государственный технический университет»

Кафедра ИИТ

**Лабораторная работа №3**

По дисциплине «Аппаратное и программное обеспечение сетей»

Тема: «АНАЛИЗ СЕТЕВОГО ТРАФИКА И ПРОТОКОЛОВ НА БАЗЕ WIRESHARK»

**Выполнил:**

Студент 3 курса

Группы ИИ-21

Пучинский А.А.

**Проверил:**

Степанчук В.И.

Брест 2023

**Цель работы:** изучить типы фильтрации трафика, правила построения фильтров, приемы статистической обработки сетевого трафика в Wireshark.

**Ход работы:**

1. Запустив Wireshark на захват, выполнить загрузку доступной в лабораторных условиях страницы (bstu.by, iit.bstu.by или др.). Остановить и сохранить захват. Для захваченных пакетов определить статистические данные:

* процентное соотношение трафика разных протоколов в сети;
* среднюю скорость кадров/сек;
* среднюю скорость байт/сек;
* минимальный, максимальный и средний размеры пакета;
* степень использования полосы пропускания канала (загрузку сети).

2. Отфильтровать в захвате IP пакеты. Определить статистические данные:

* процентное соотношение трафика разных протоколов стека tcp/ip в сети;
* средний, минимальный, максимальный размеры пакета.

На примере любого IP-пакета указать структуры протоколов Ethernet и IP. Отметить поля заголовков и описать их и интерпретировать их значения.

3. Запустив Wireshark на захват, выполнить команду ping для IP адреса соседней рабочей станции в лаборатории (предварительно определив ее адрес с помощью ipconfig). Сохранить результат. Сформировав нужный фильтр, отфильтровать пакеты, относящиеся к выполнению команды ping. На базе полученных пакетов и значений их полей интерпретировать результат работы утилиты ping. Описать все протоколы, используемые утилитой. Составить диаграмму взаимодействия машин при работе утилиты ping.

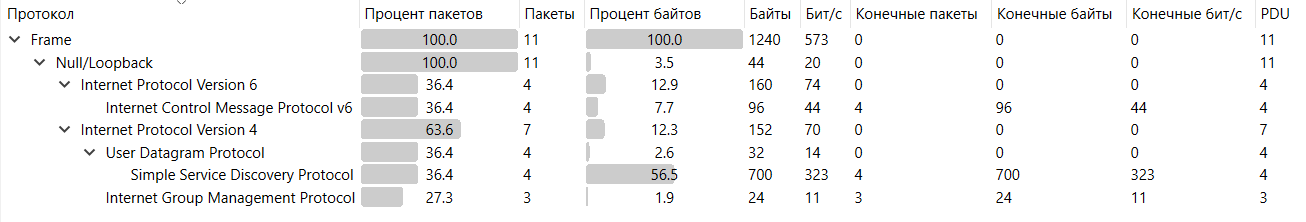
4. Запустив Wireshark на захват, выполнить разработанный в предыдущей лабораторной работе TCP-сервер и TCP-клиент. Сохранить результат. Сформировав нужный фильтр, отфильтровать пакеты данного сеанса. На примере любого TCP-сегмента указать структуру протокола TCP. Отметить поля заголовка, описать их и интерпретировать их значения. Составить диаграмму взаимодействия TCP-сервера и TCP-клиента.

5. Запустив Wireshark на захват, выполнить разработанный в предыдущей лабораторной работе UDP-сервер и UDP-клиент. Сохранить результат. Сформировав нужный фильтр, отфильтровать пакеты данного сеанса. На примере любого UDP-сегмента указать структуру протокола UDP. Отметить поля заголовка, описать их и интерпретировать их значения.

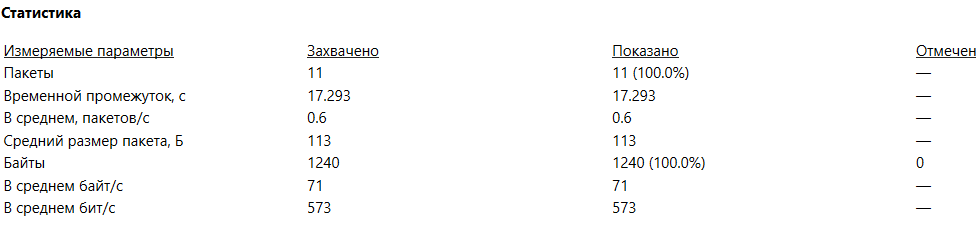
6. Выполнить анализ ARP-протокола по примеру из методических указаний.

**1.**

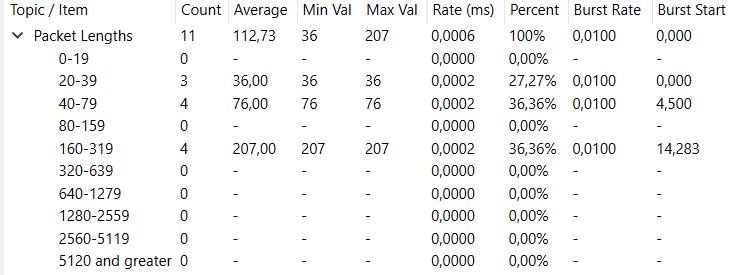
**Процентное соотношение трафика разных протоколов в сети:**



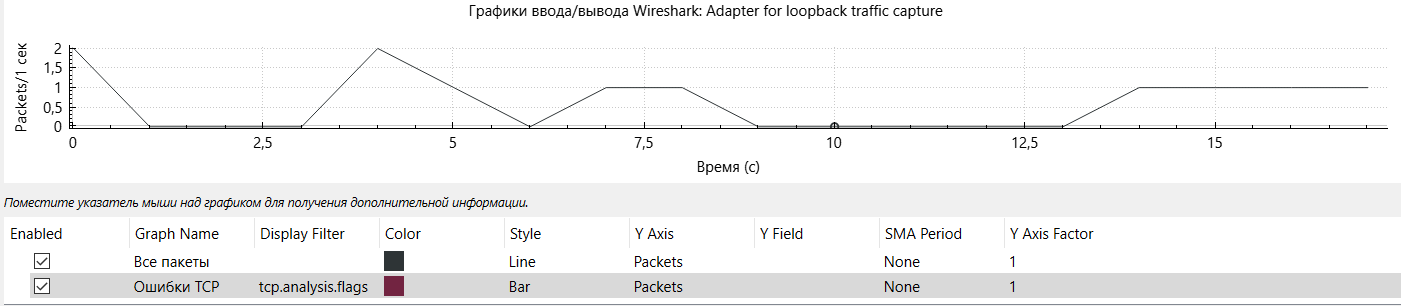
**Средняя скорость кадров/сек, байт/сек:**



**Минимальный, максимальный и средний размеры пакета:**

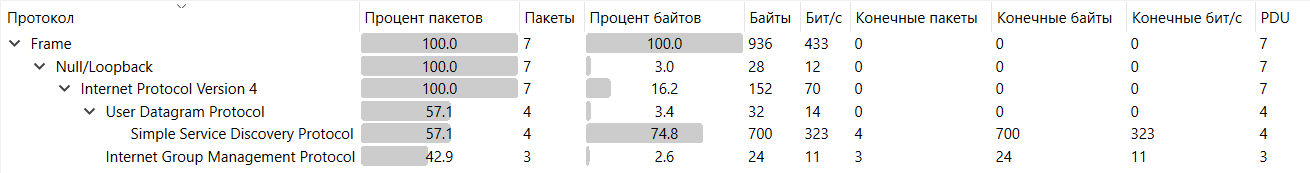


**Степень использования полосы пропускания канала (загрузку сети):**

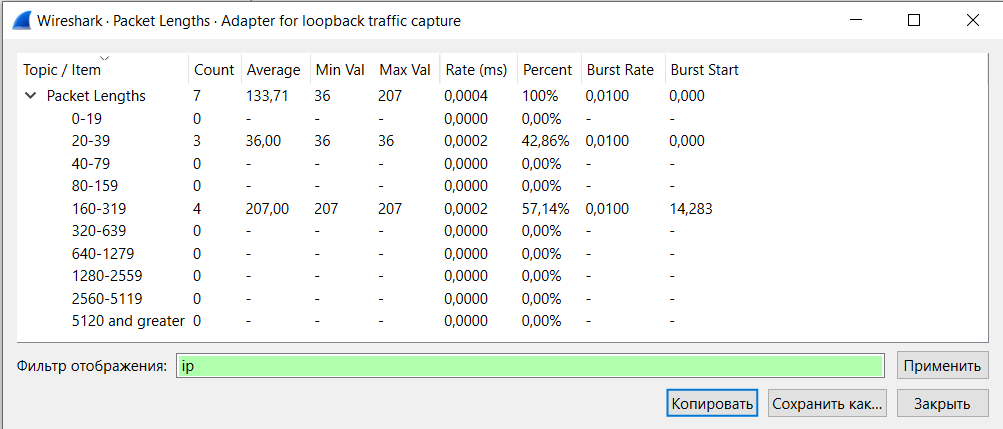


**2.**

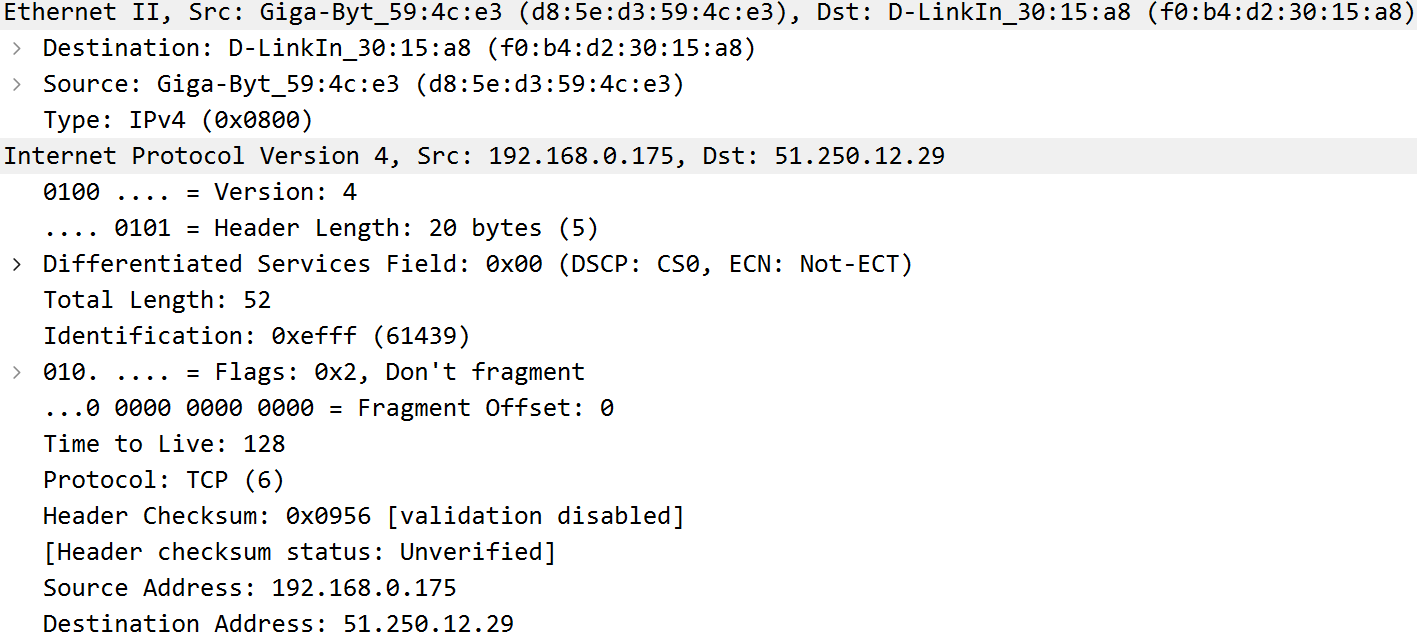
**Процентное соотношение трафика разных протоколов стека tcp/ip в сети:**



**Средний, минимальный, максимальный размеры пакета:**

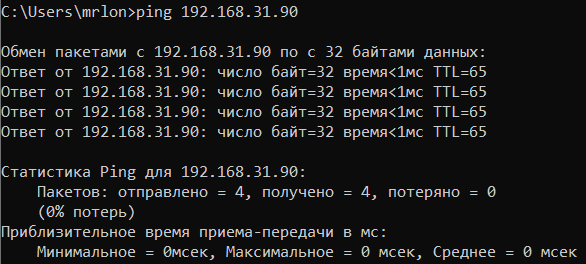


**Структуры протоколов Ethernet и IP:**

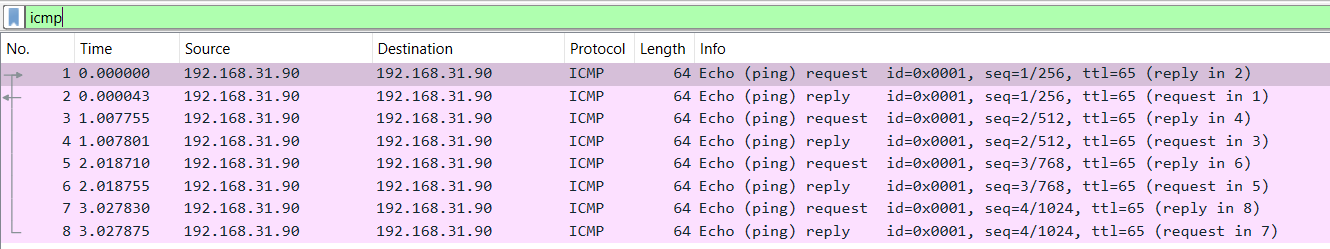
****

**3.**

**Результат команды ping:**



**Захват трафика и фильтрация по пакетам,** **относящиеся к выполнению команды ping:**



* Присутствие ICMP Echo Request и ICMP Echo Reply пакетов свидетельствует о том, что пакеты успешно прошли до целевого устройства и были возвращены обратно.
* Коды сообщений ICMP могут указывать на различные ситуации, например, успешное выполнение, недоступность хоста и т. д.
* Время жизни (TTL) показывает, сколько промежутков времени прошло, прежде чем пакет был отброшен или достиг своего назначения.

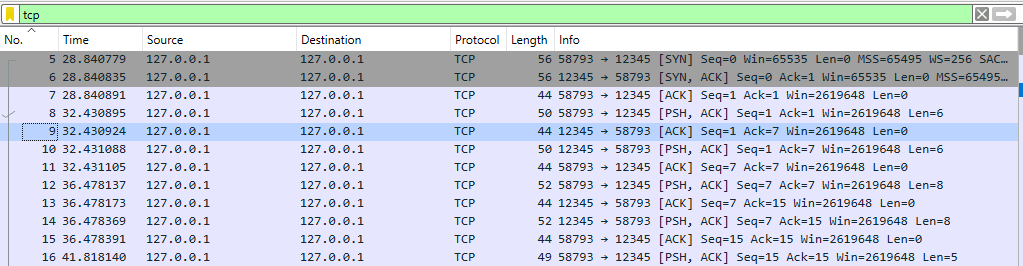
**Диаграмма взаимодействия машин при работе утилиты ping:**

**ICMP**

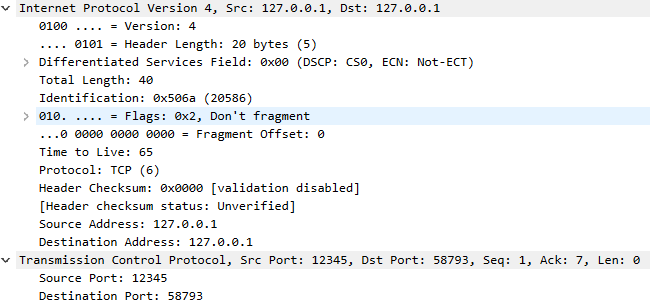
**192.168.31.90 192.168.31.90**

**4.**

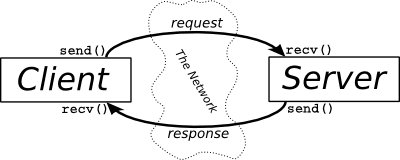
**Фильтрация пакетов, относящиеся только к TCP – клиенту(серверу):**



**Структура протокола TCP:**

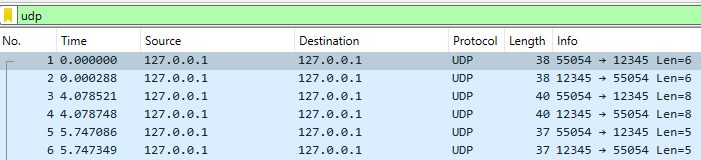


**Диаграмма взаимодействия TCP-сервера и TCP-клиента:**

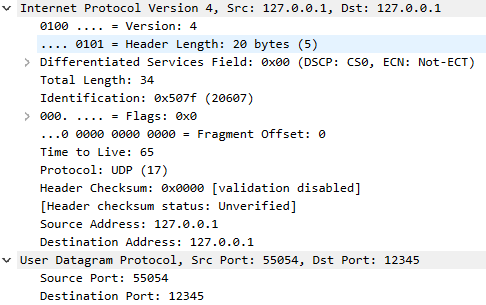


**5.**

**Фильтрация пакетов, относящиеся только к UDP – клиенту (серверу:**

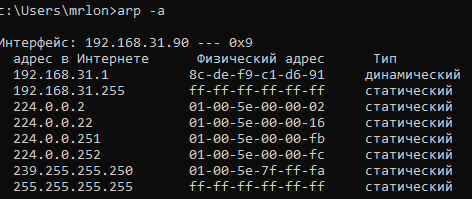


**Структура протокола UDP:**

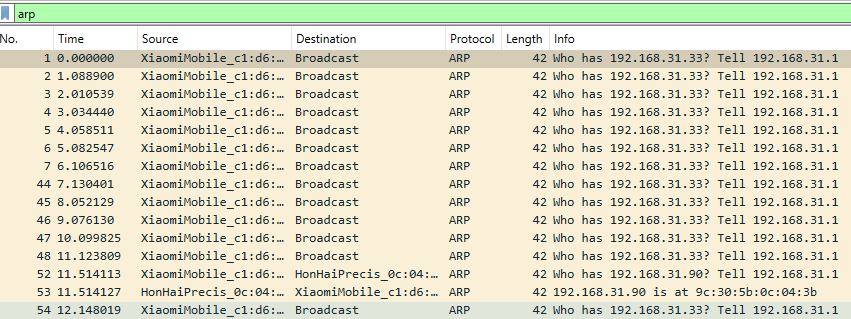


**6.**

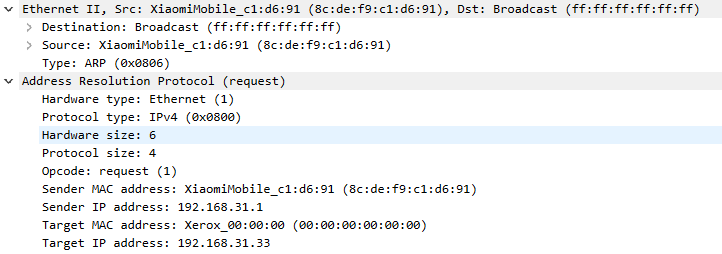
**Работа в консоли с ARP:**



**Фильтрация пакетов, относящиеся только к ARP-протоколу:**



**Структура ARP-протокола:**



**Вывод:** изучил типы фильтрации трафика, правила построения фильтров, приемы статистической обработки сетевого трафика в Wireshark.