Министерство науки и высшего образования Российской Федерации

**Федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

«Владимирский государственный университет

имени Александра Григорьевича и Николая Григорьевича Столетовых»

(ВлГУ)

Кафедра информационных систем и программной инженерии

**Лабораторная работа №7**

**по дисциплине**

**«Информационные сети»**

**ИЗУЧЕНИЯ СРЕДСТВ МОНИТОРИНГА И АНАЛИЗА СЕТЕВОГО ТРАФИКА.**

**СНИФФЕР WIRESHARK (ETHREAL)**

**Выполнил**:

ст. гр. ПРИ-120

Д. А. Грачев

**Принял**:

Доцент кафедры ИСПИ

Курочкин С. В.

Владимир, 2022

ЦЕЛЬ РАБОТЫ

Знать принципы анализа сетевого трафика. Научиться использовать сетевой анализатор (сниффер Wireshark). Научиться анализировать сетевой трафик на примере протоколов ARP, IP и ICMP.

ВЫПОЛНЕНИЕ РАБОТЫ

1. Захватим 100 пакетов программой wireshark

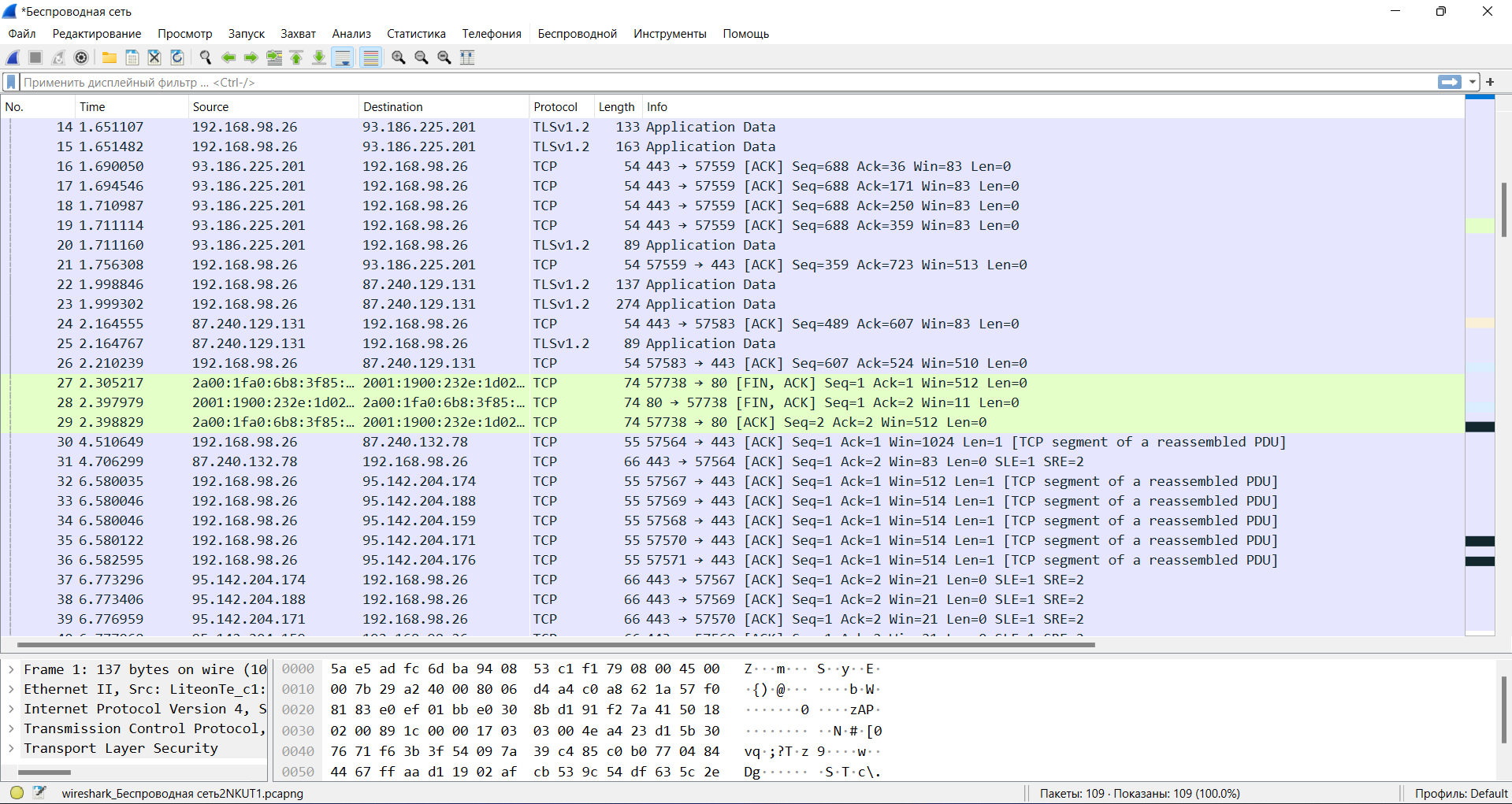


Рисунок . Захваченные пакеты

1. Узнаем процентное соотношение трафика разных протоколов в сети

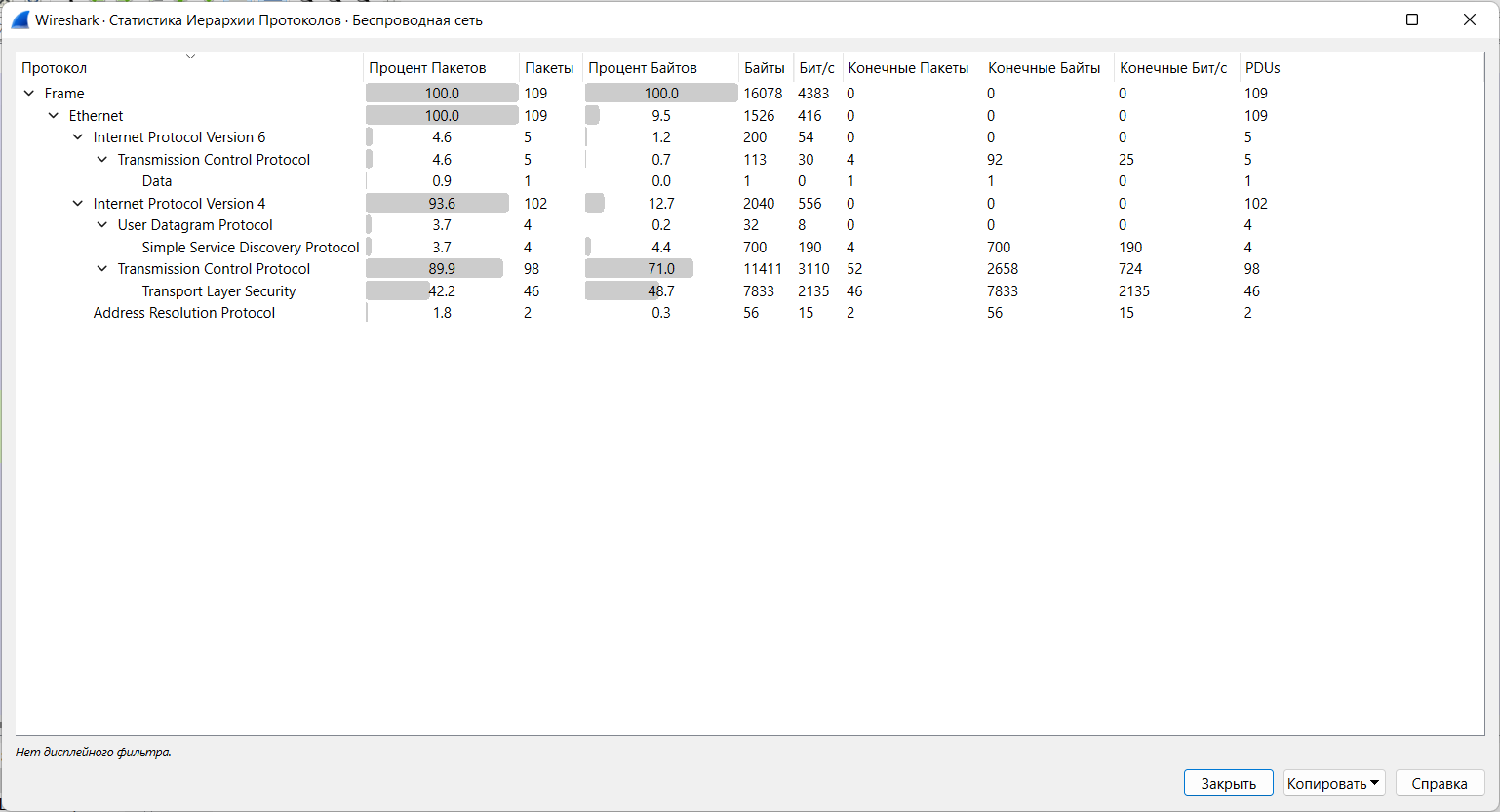


Рисунок . Статистика иерархии протоколов

1. Узнаем среднюю скорость кадров/сек, байт/сек и средний размер пакета

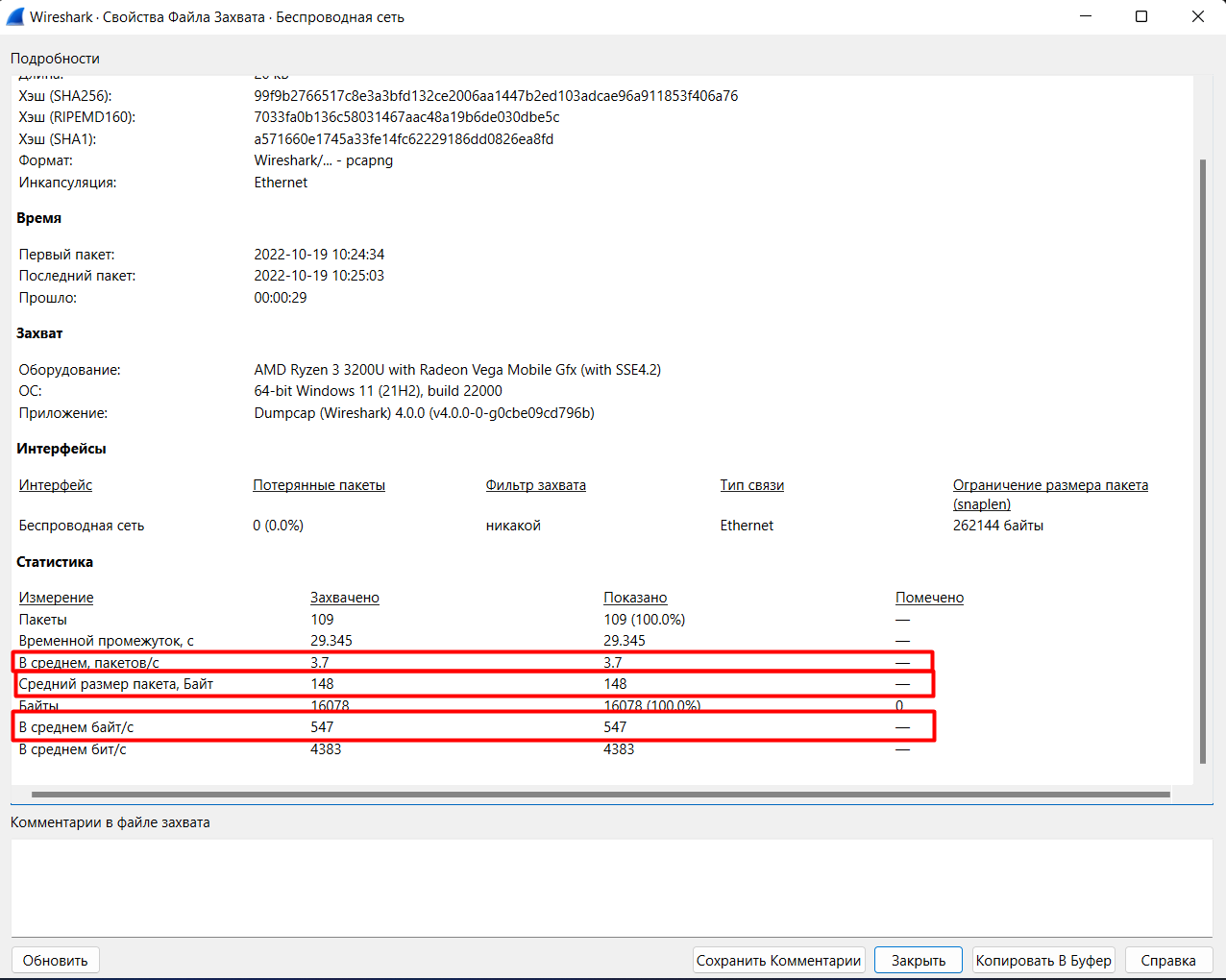


Рисунок . Статистика скорости

1. Узнаем степень использования полосы пропускания канала

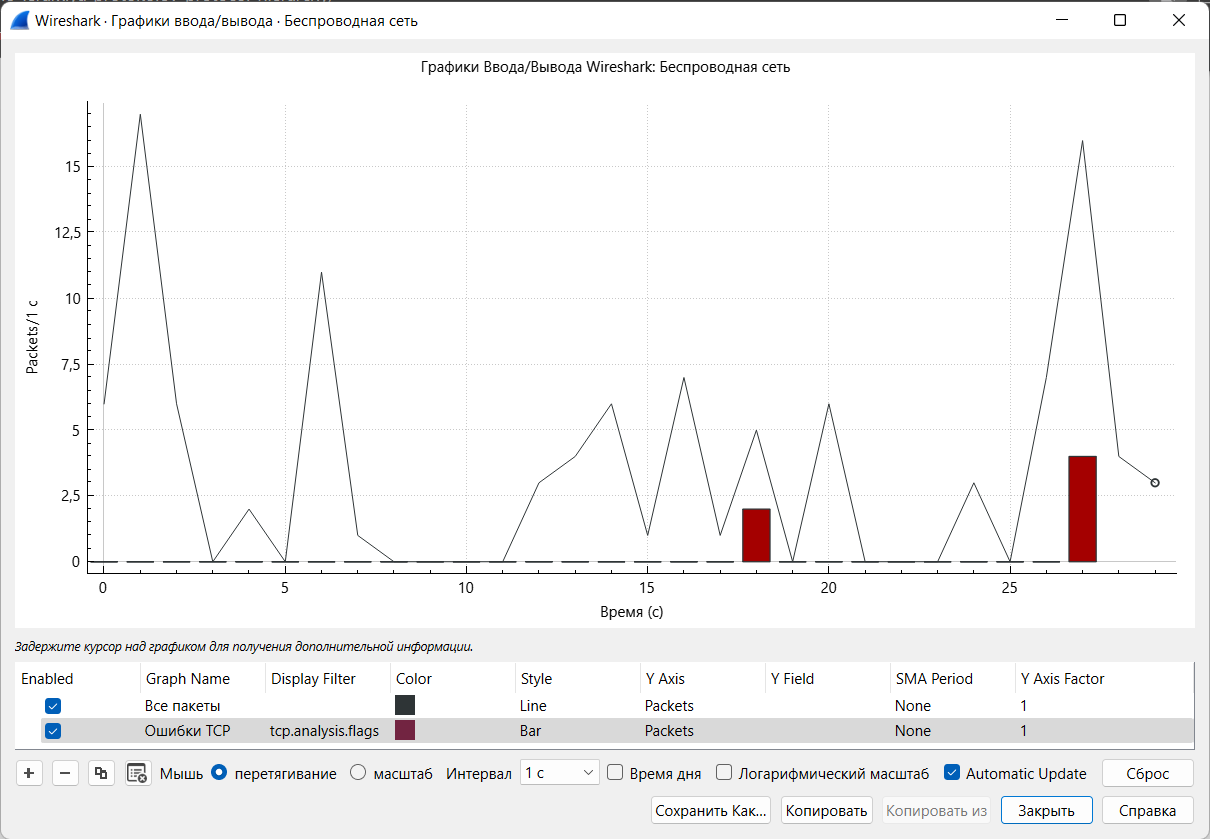


Рисунок .График ввода/вывода

1. Настроим фильтр на получение только ip-пакетов

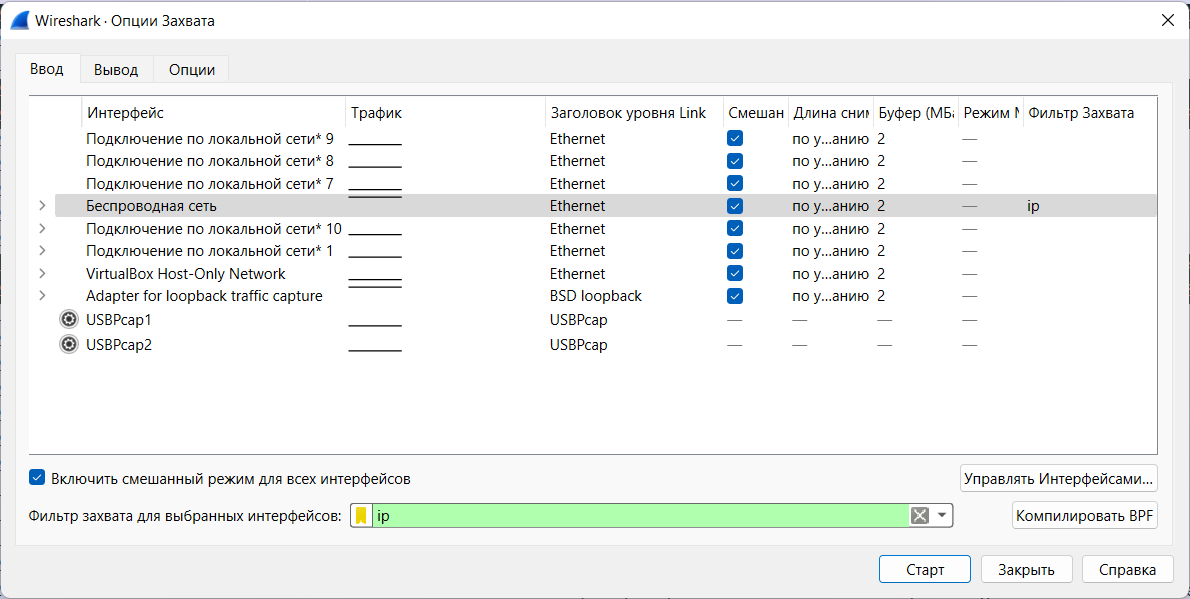


Рисунок . Настройка фильтра

1. Полученные ip-пакеты

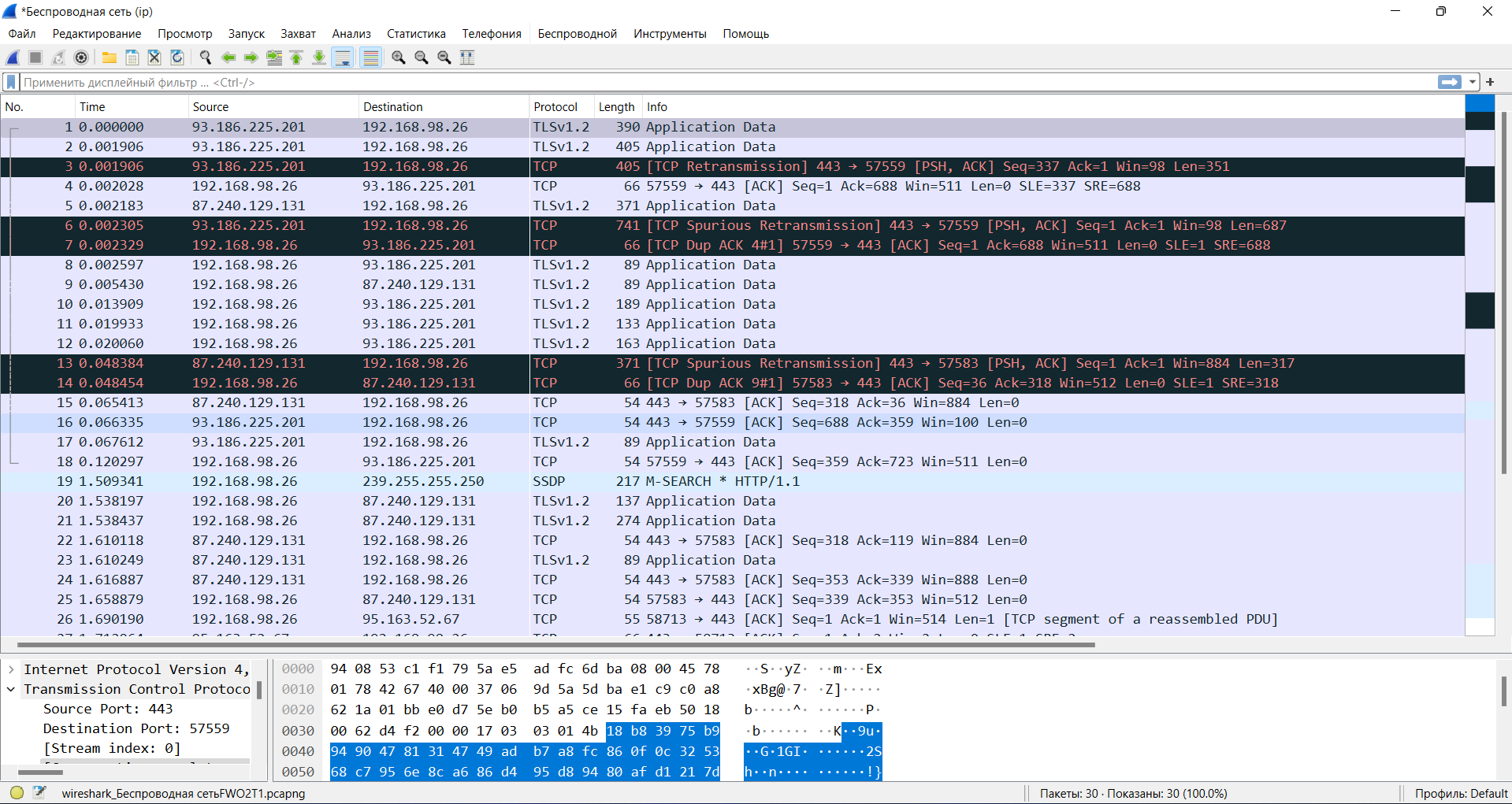


Рисунок . Захваченные пакеты

1. Узнаем процентное соотношение трафика разных протоколов стека tcp/ip в сети

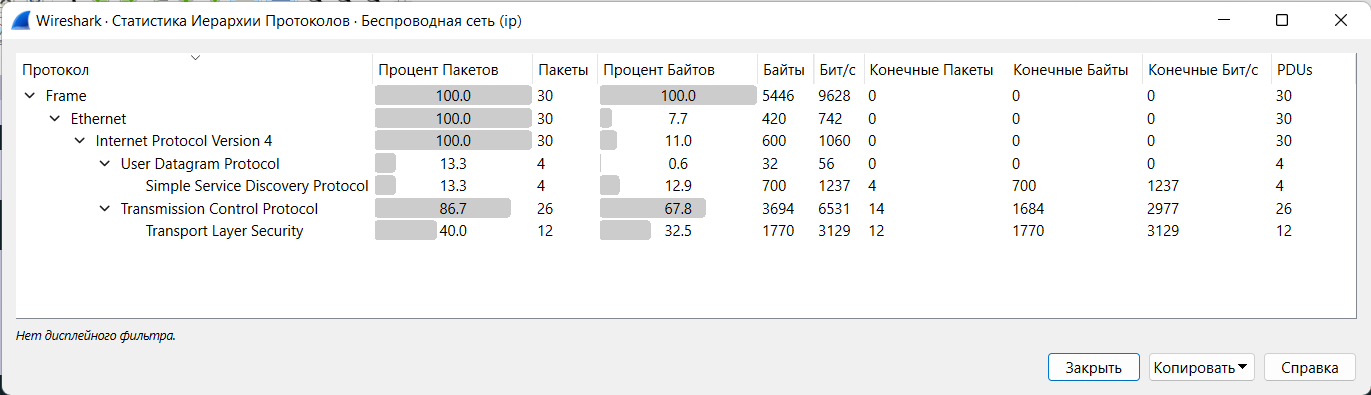


Рисунок . Статистика иерархии протоколов

1. Узнаем минимальный, максимальный и средний размер пакетов

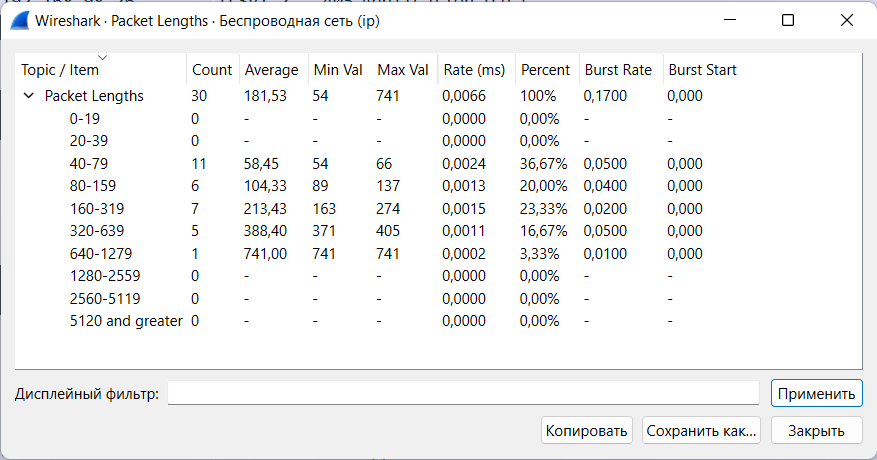


Рисунок . Длина пакетов

1. Настроим фильтр на получение только arp-пакетов

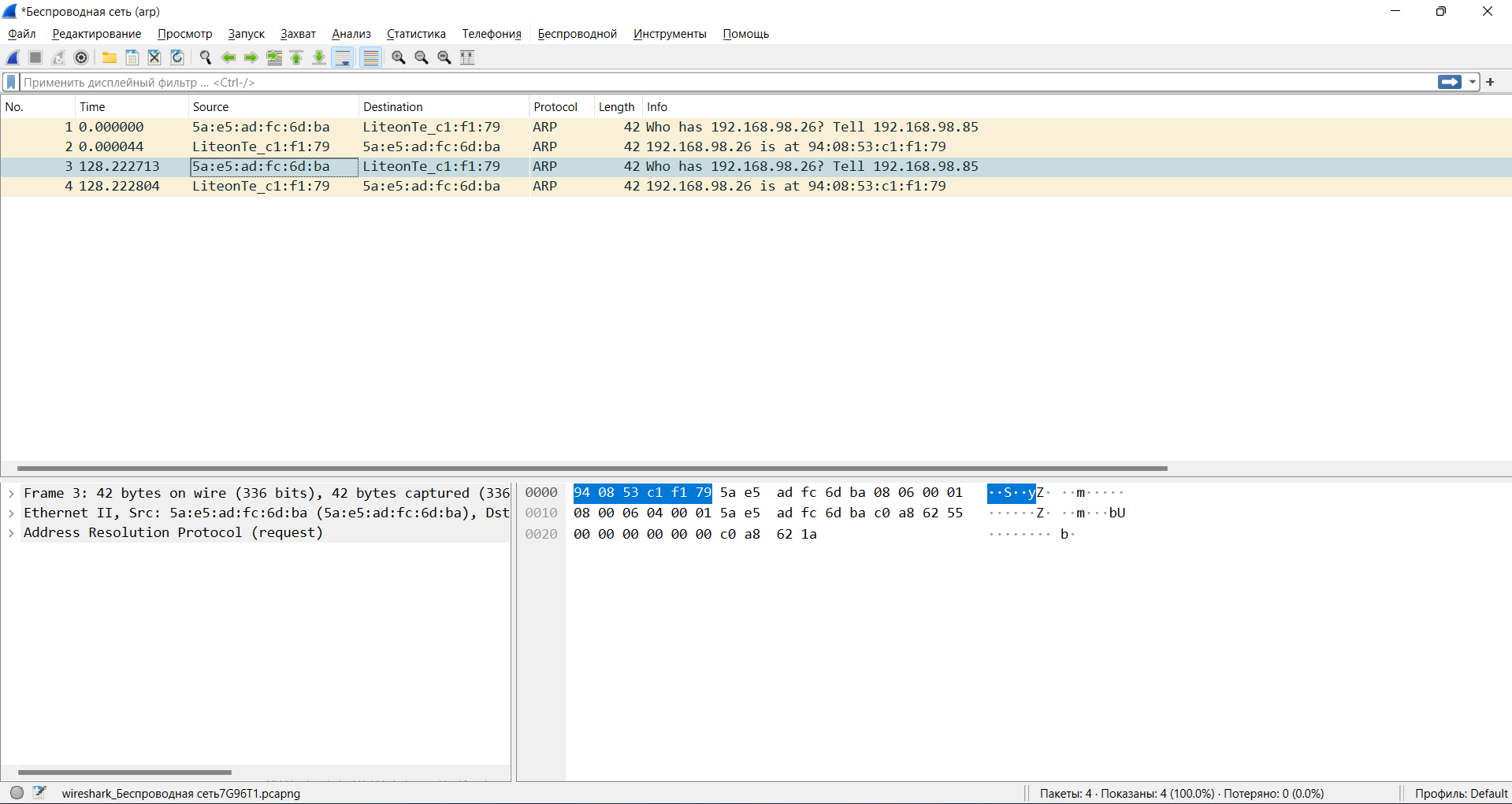


Рисунок . Захваченные arp пакеты

1. Откроем один из пакетов, чтобы его проанализировать

Мы можем видеть, что в пакете указаны MAC- и IP-адреса отправителя («Sender MAC address» и «Sender IP address» соответственно). Это параметры машины, с которой выполняется запрос. В данном случае запрос направлен на получения («Opcode: request» – запрос) MAC-адреса машины, у которой IP-адрес («Protocol type: IP») 192.168.98.26 («Target IP address»). При этом поле «Target MAC address» обнулено.

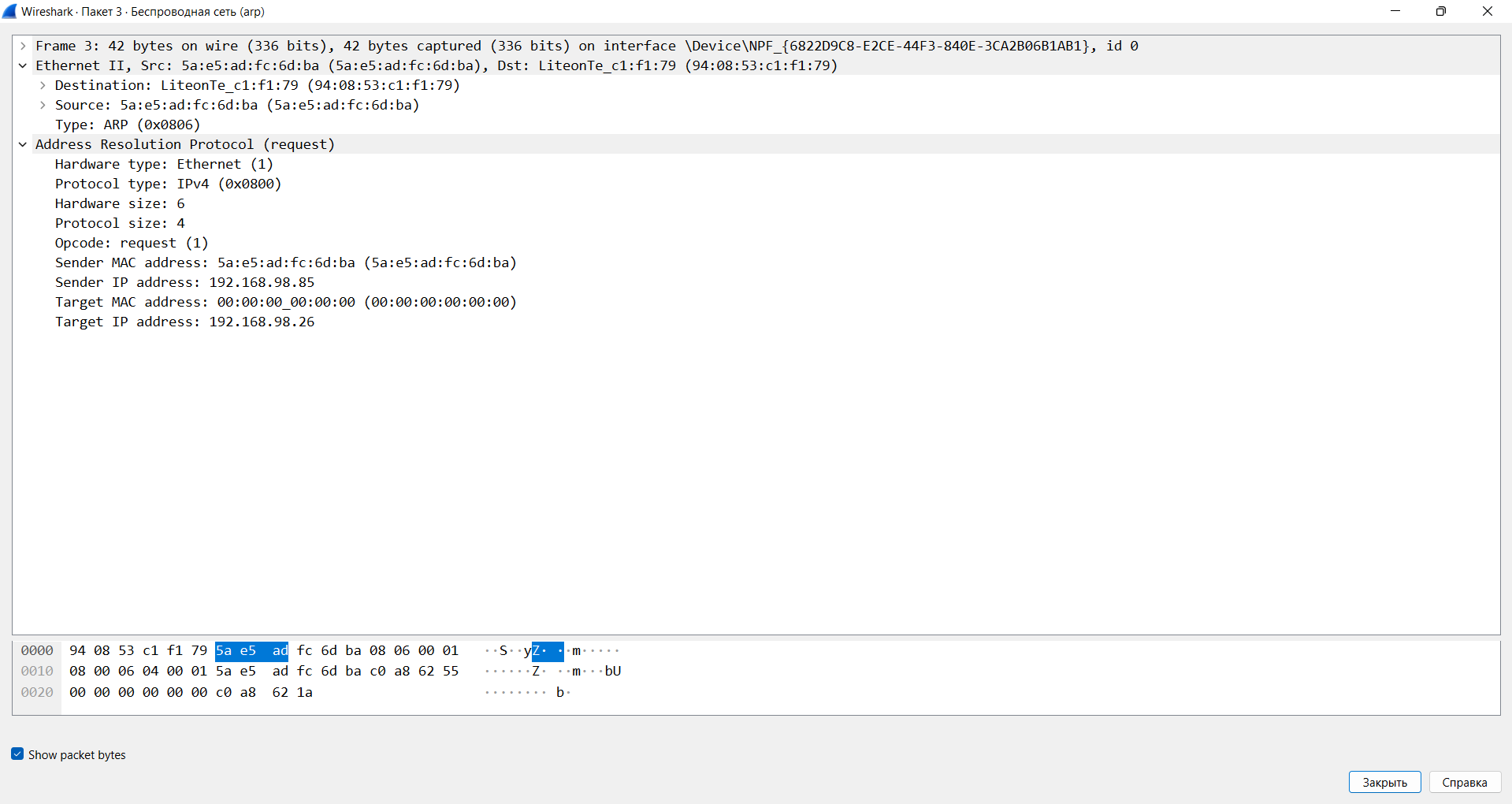


Рисунок . Подробная информация о пакете

1. На примере любого IP-пакета укажем структуры протоколов Ethernet и IP.

Пакет протокола IP состоит из заголовка и поля данных. Максимальная длина пакета 65 535 байт. Заголовок обычно имеет длину 20 байт и содержит информацию о сетевых адресах отправителя и получателя, о параметрах фрагментации, о времени жизни пакета, о контрольной сумме и некоторых других. В поле данных IP- пакета находятся сообщения более высокого уровня.

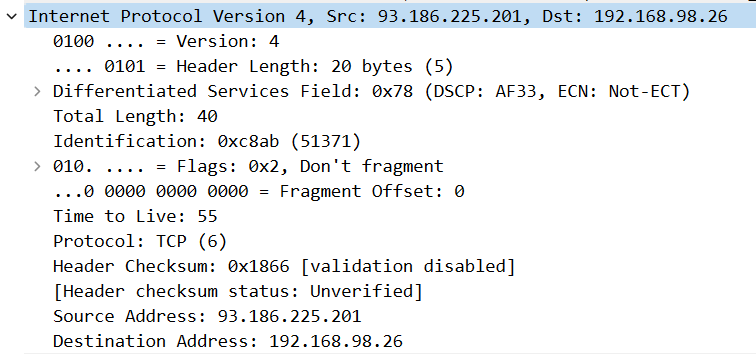


Рисунок . Информация о пакете

1. Ping — утилита для проверки целостности и качества соединений в сетях на основе TCP/IP, а также обиходное наименование самого запроса. Утилита отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply).

ВЫВОД

В ходе выполнения лабораторной работы были изучены принципы анализа сетевого трафика на примере протоколов ARP, IP и ICMP, использования сетевого анализатора.