**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**федеральное государственное бюджетное образовательное учреждение высшего образования**

**«Российский экономический университет имени Г.В. Плеханова»**

**Московский приборостроительный техникум**

**Лабораторная работа №11**

по учебной практике

УП.01.02 Средства мониторинга и анализа в локальных сетях

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*индекс по УП и наименование практики*

Профессионального модуля ПМ.01«Выполнение работ по проектированию

сетевой инфраструктуры»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*индекс по УП и наименование профессионального модуля*

Специальность 09.02.06 Сетевое и системное администрирование

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*код и наименование специальности*

Студент Карпов Артем Владимирович

*(фамилия, имя, отчество)*

Группа СА50-1-22

Руководитель по практической подготовке от техникума

Кульчинская Нелли Андреевна

*(фамилия, имя, отчество)*

«\_\_\_\_» \_\_\_\_\_\_\_\_\_ 2024 года

1. Открываем wireshark и запускаем снифинг с рабочего интерфейса и оставляем так на 10 мин.

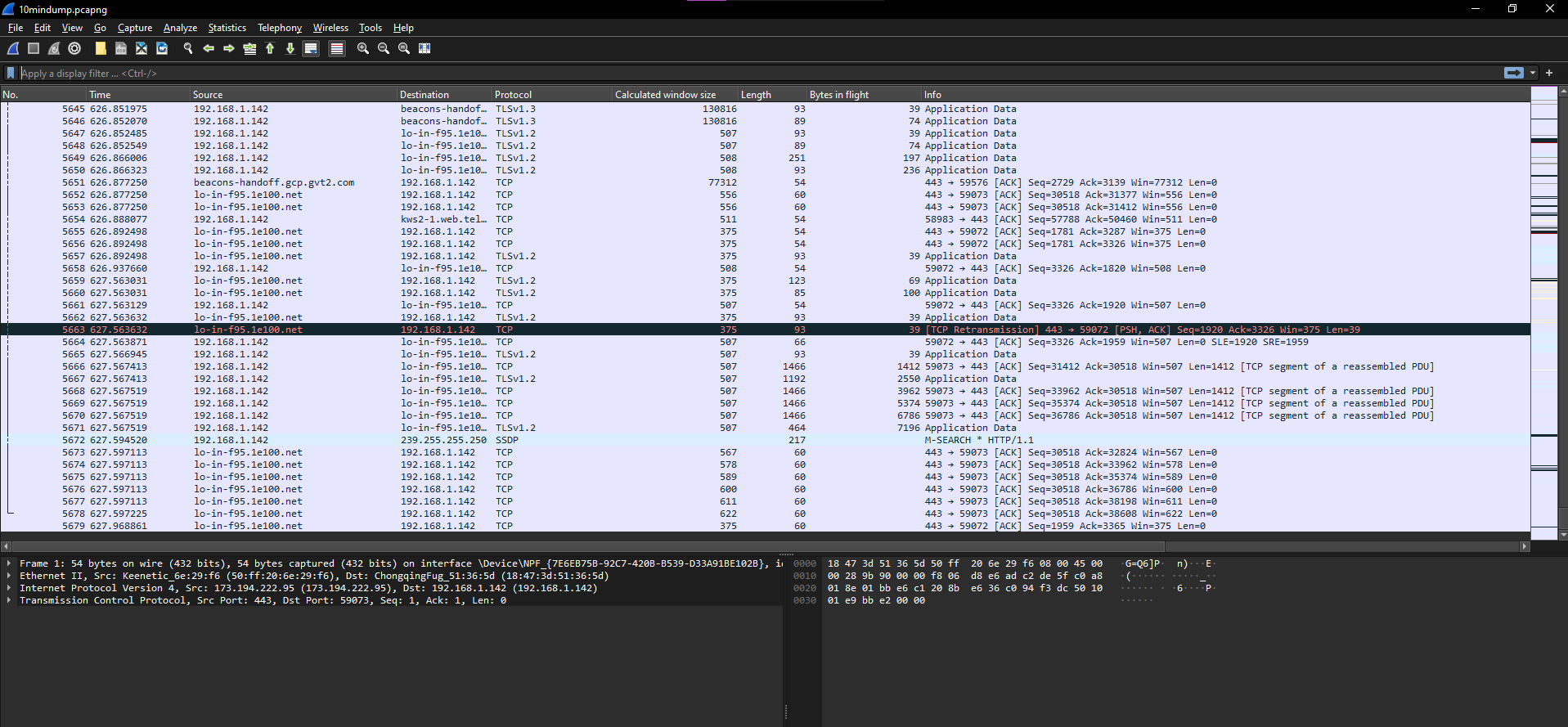


Рис. 1 – прослушка интерфейса.

1. Посмотрим в нашем dump какие протоколы использовались чаще всего. Для этого воспользуемся инструментом protocol Hierarchy

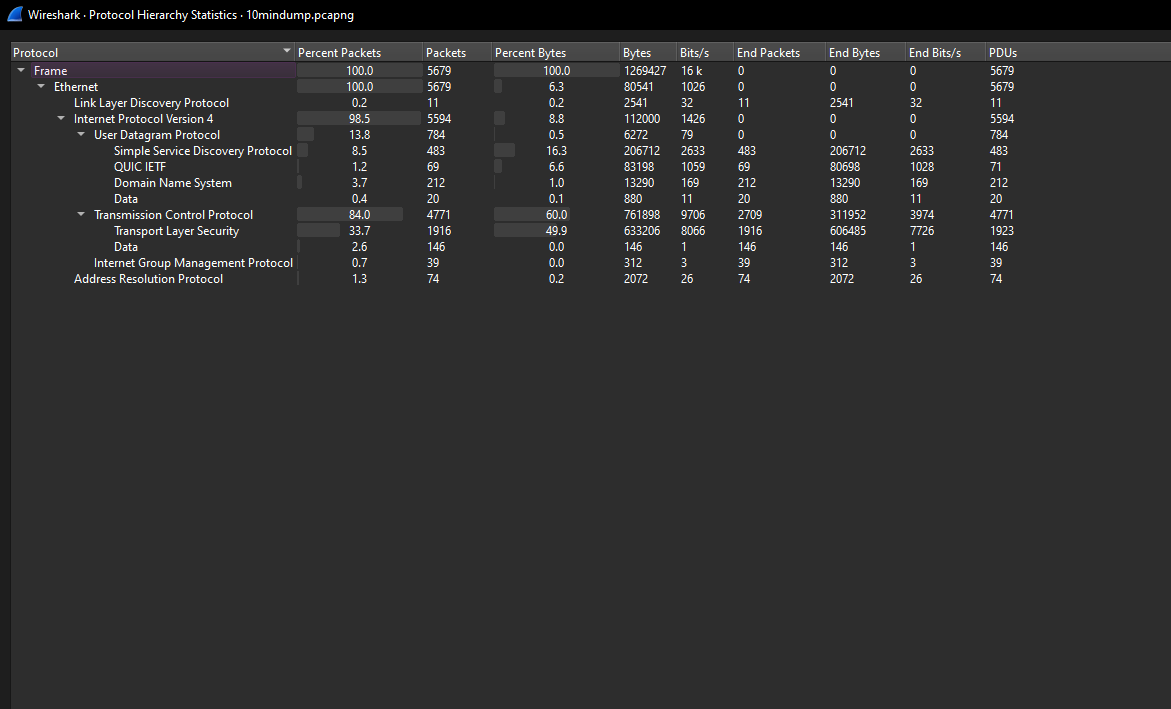


Рис. 2 – иерархия протоколов

1. Здесь можно посмотреть, например кто шлет ARP запросы, для этого нужно нажать на протокол ARP. В основном это роутер.

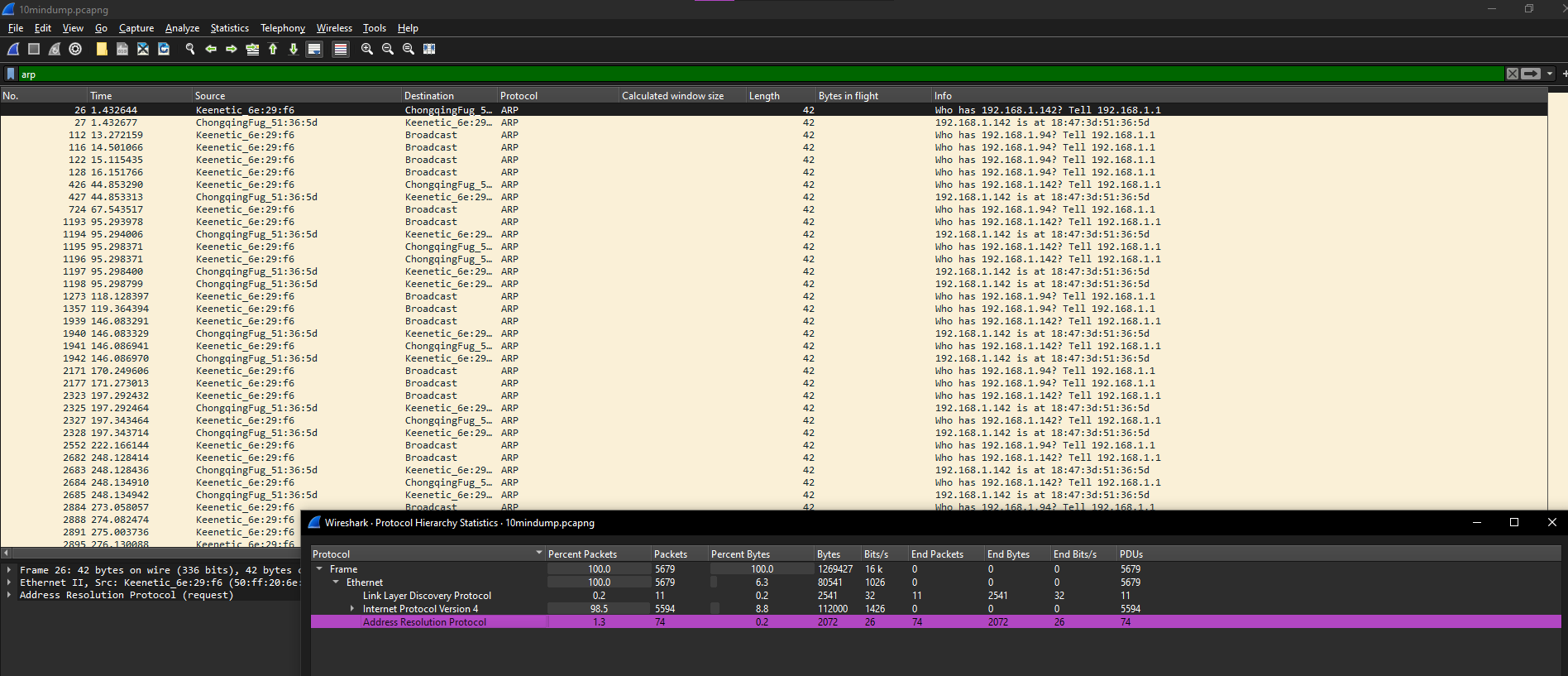


Рис. 3 – ARP

1. Теперь воспользуемся утилитой Endpoints.



Рис. 4 – Endpoints.

1. С помощью этой утилиты можно, например посмотреть какой хост самый активный. Отфильтровать по Bytes. Самым активным является мой компьютер.

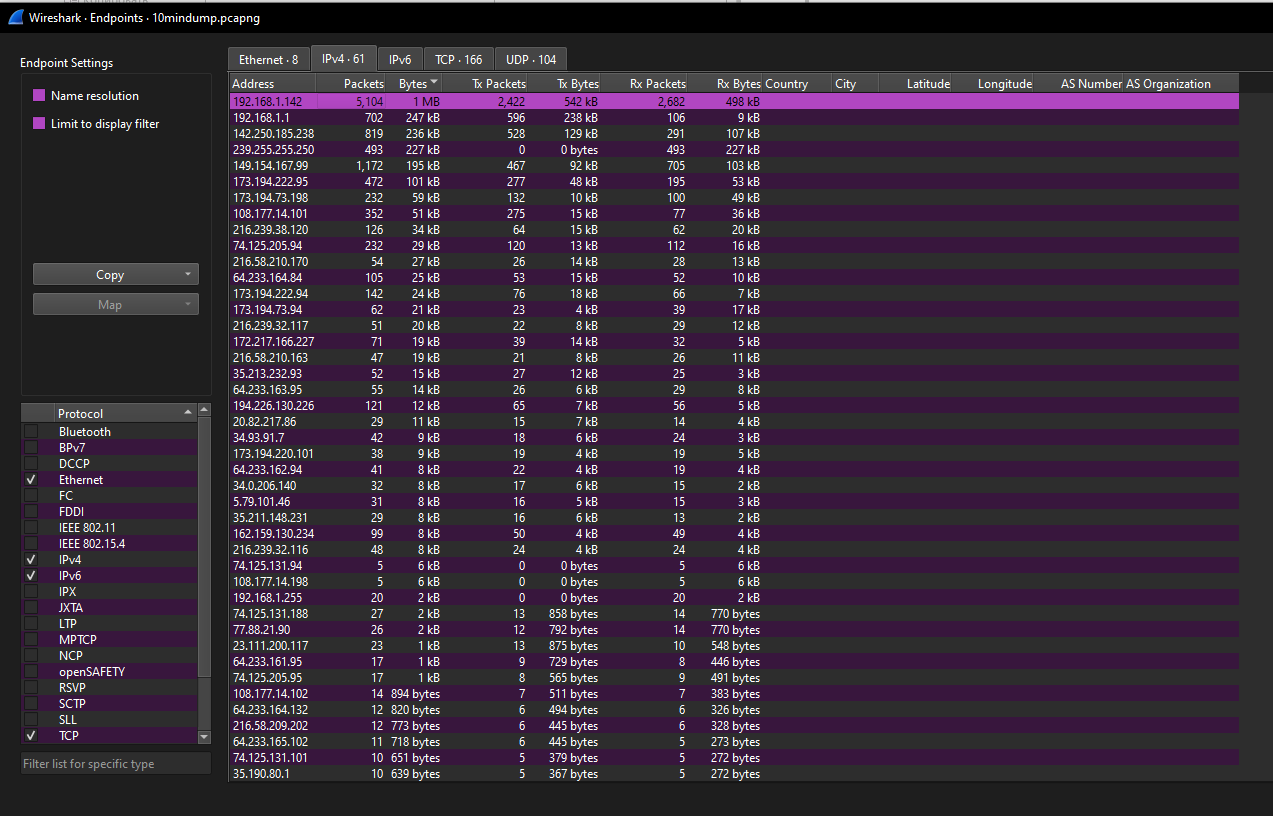


Рис. 5 – активность хоста

1. Мы сразу оттуда можем его отфильтровать по Ip адресу.

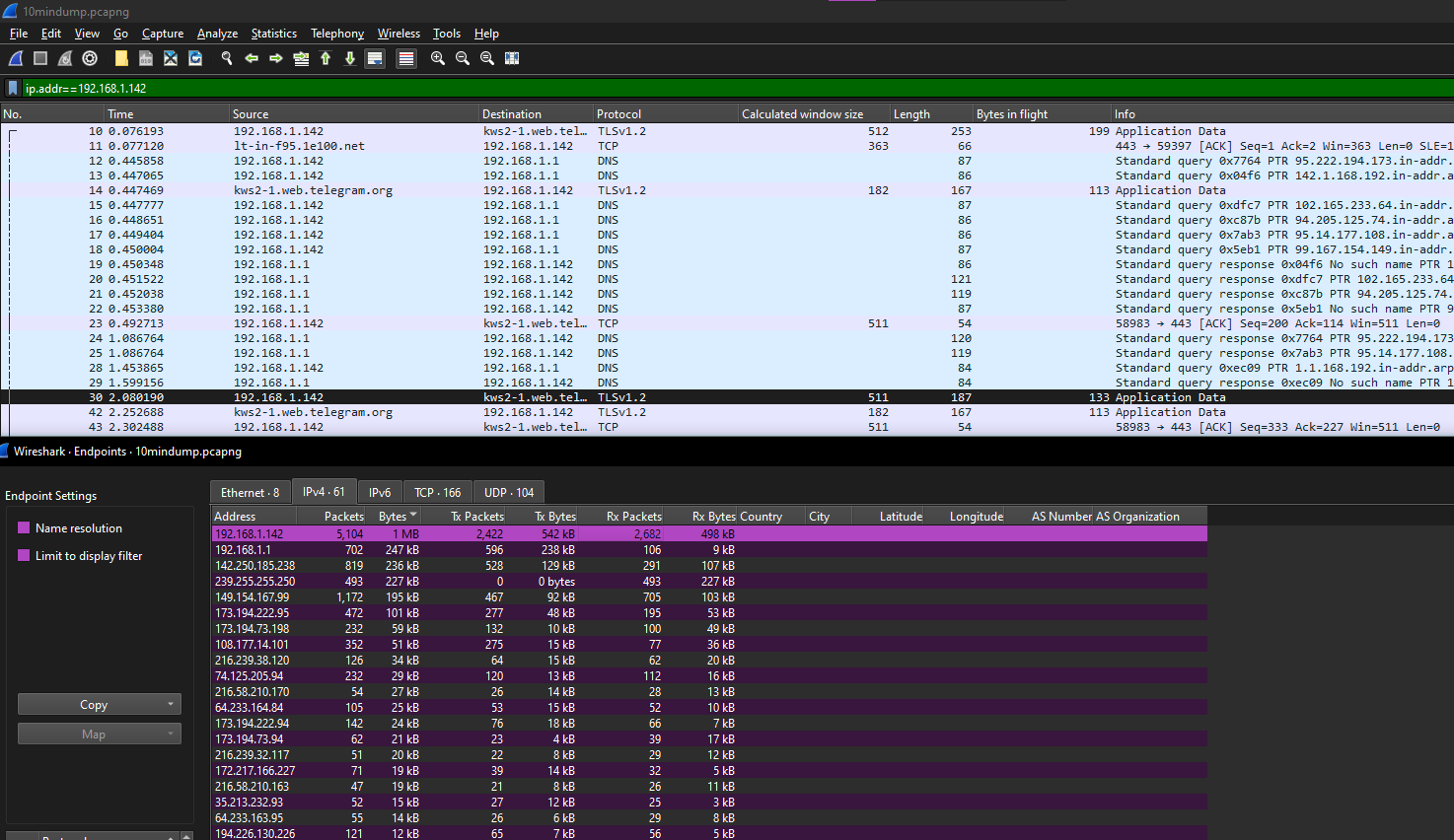


Рис. 6 – фильтрация по ip

1. Теперь мы можем использовать утилиту Conversations находясь в отфильтрованном трафике по хосту. Обязательно поставим галочку в Limit to display filter.

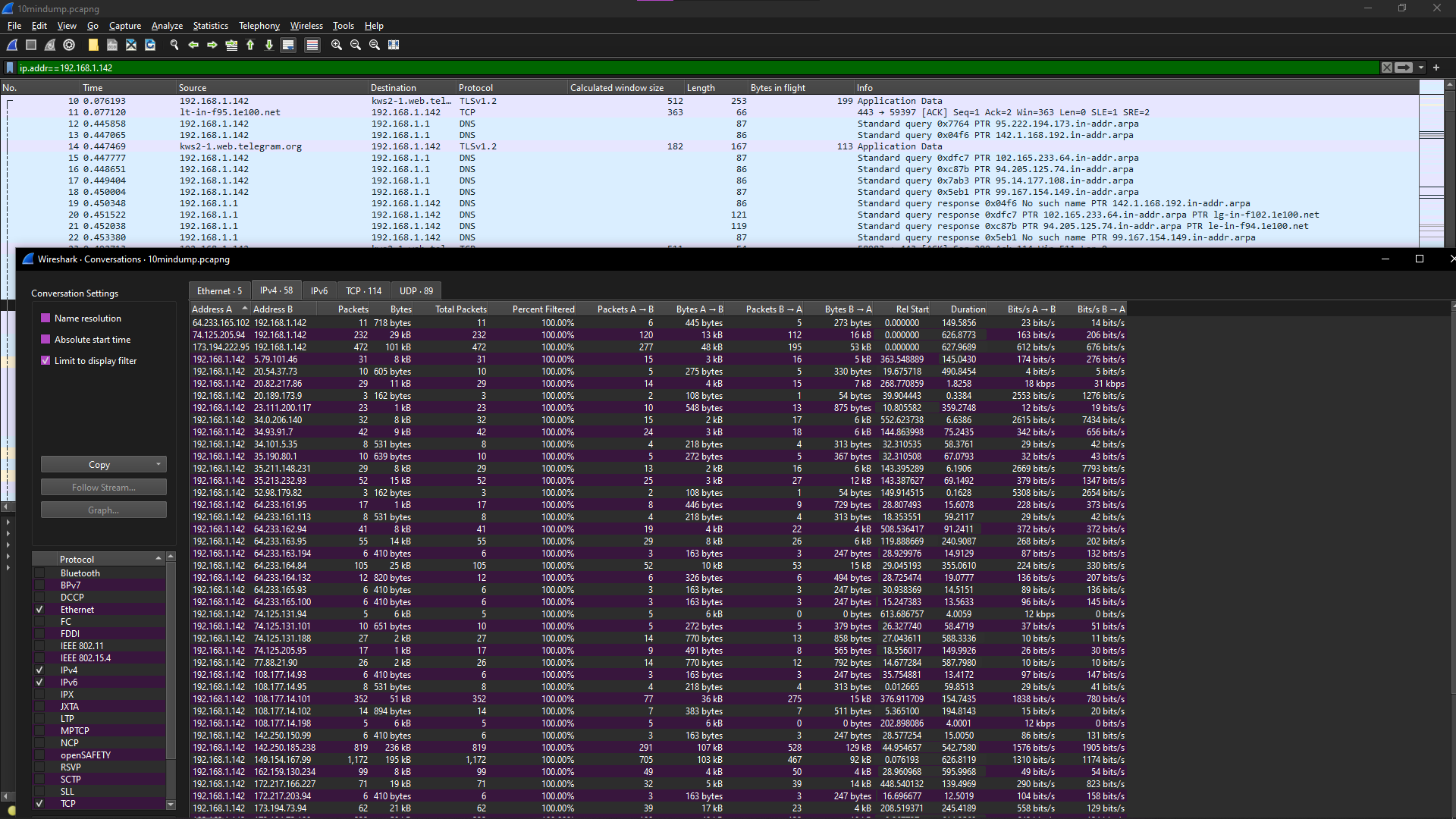


Рис. 7 – Conversations

1. Если мы поставим галочку напротив name resolution то увидим имена.

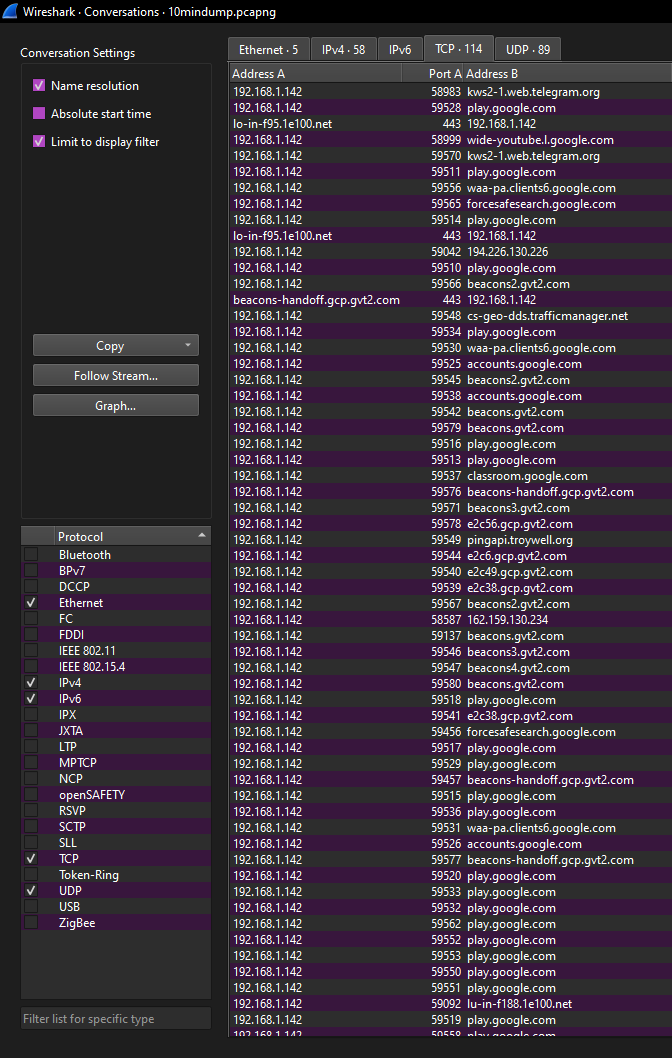


Рис. 8 – имена

1. Теперь переходим в инструмент I/O Graphs.

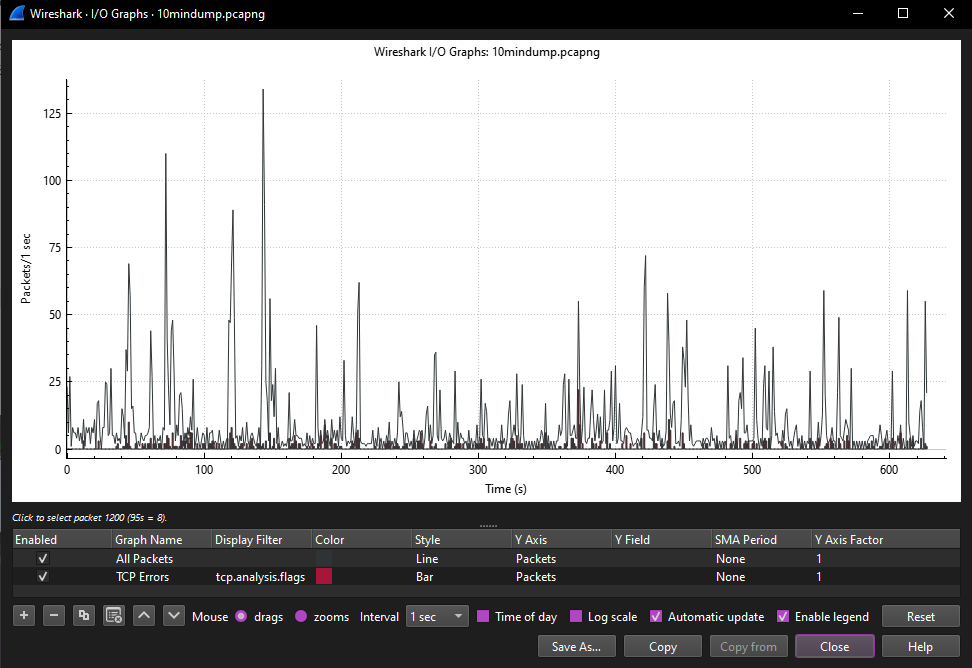


Рис. 9 – I/O Graphs

1. По оси x это время, а по оси y это то что мы выберем в параметре, например bytes

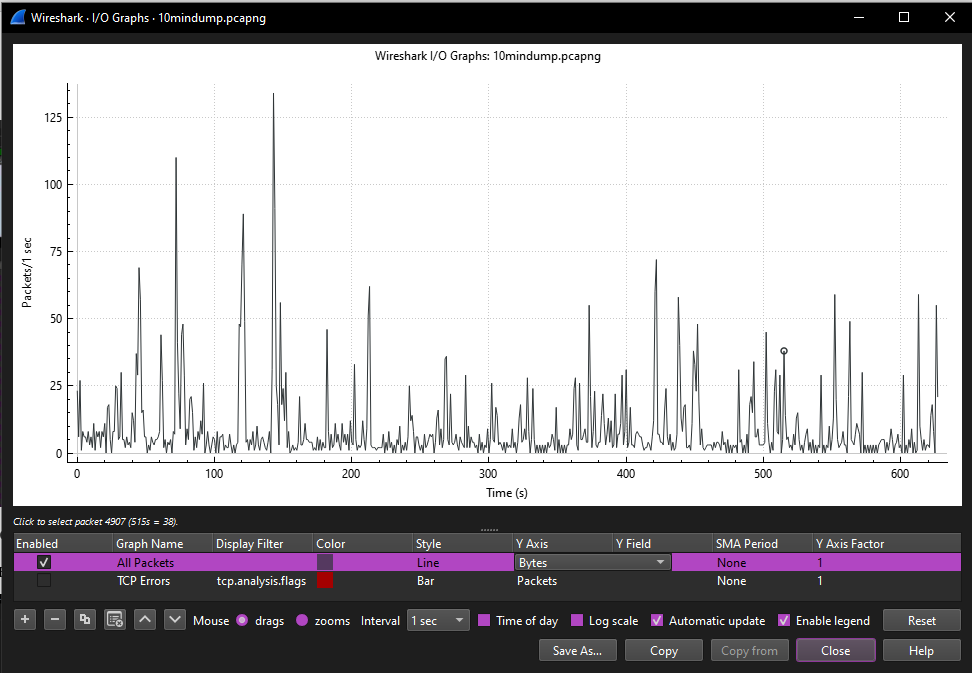


Рис. 10 – фильтр по байтам

1. Также в этом инструменте можно отображать сразу несколько графиков, например модно использовать DNS протокол

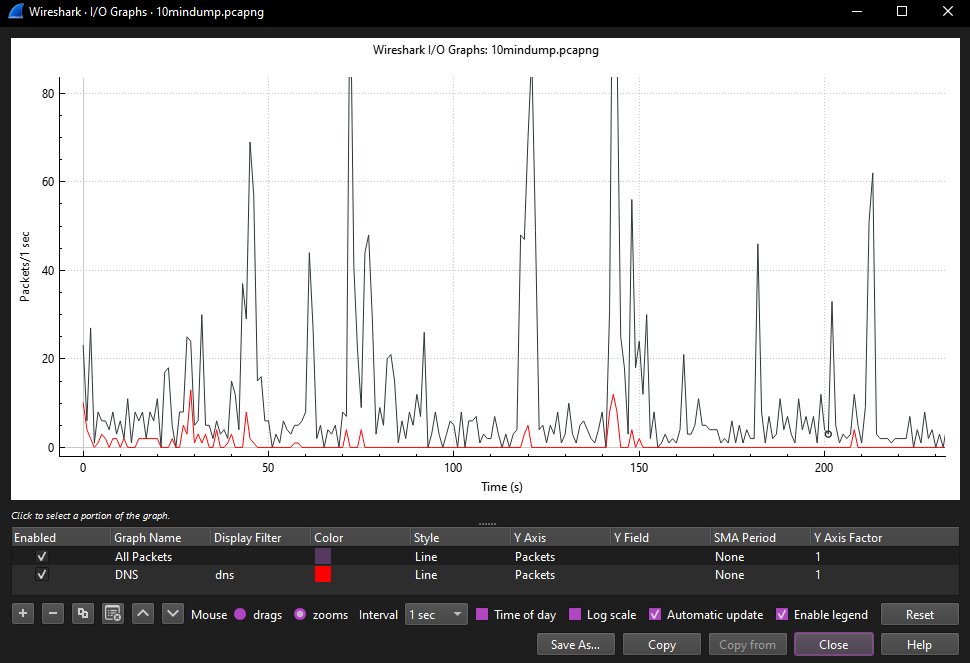


Рис. 11 – отображение DNS протокола

1. Можно посмотреть весь трафик роутера, также добавим отдельный график

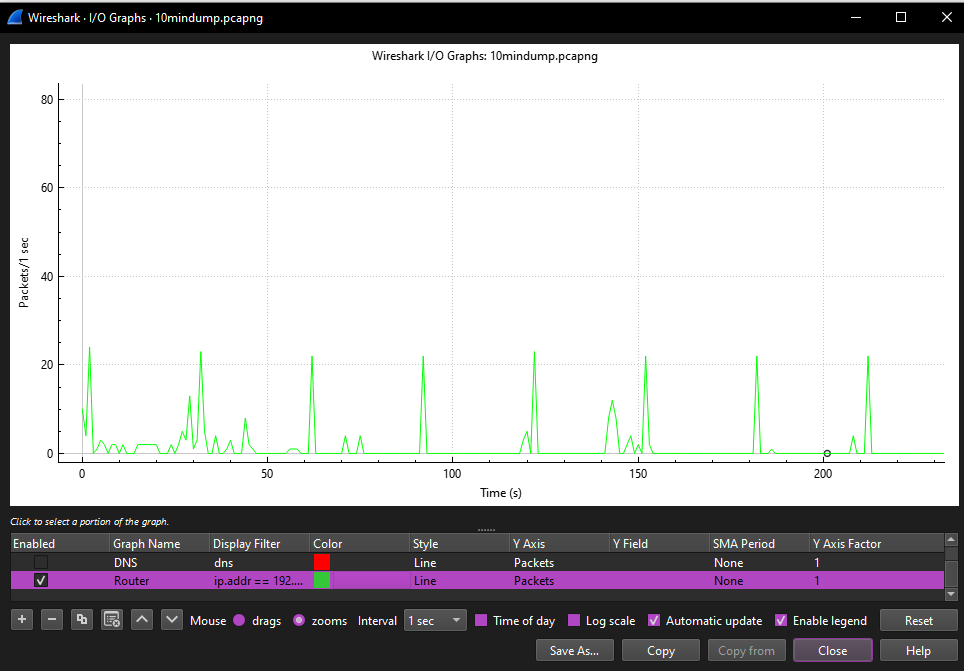


Рис. 12 – трафик роутера на графике

1. Откроем dump http

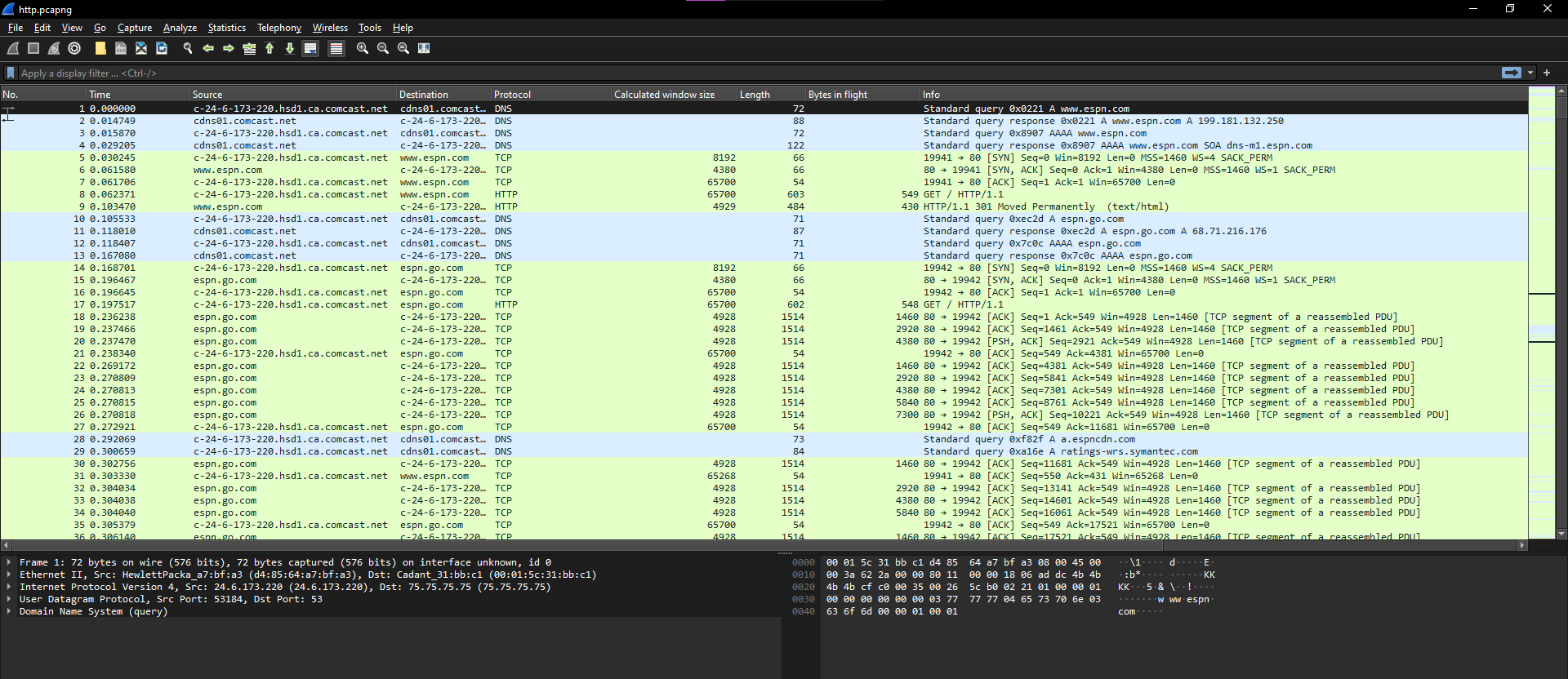


Рис. 13 – файл http

1. Откроем в нем инструмент I/O Graphs и отфильтруем по 184.0.0.0.8 и не 184.0.0.0/8

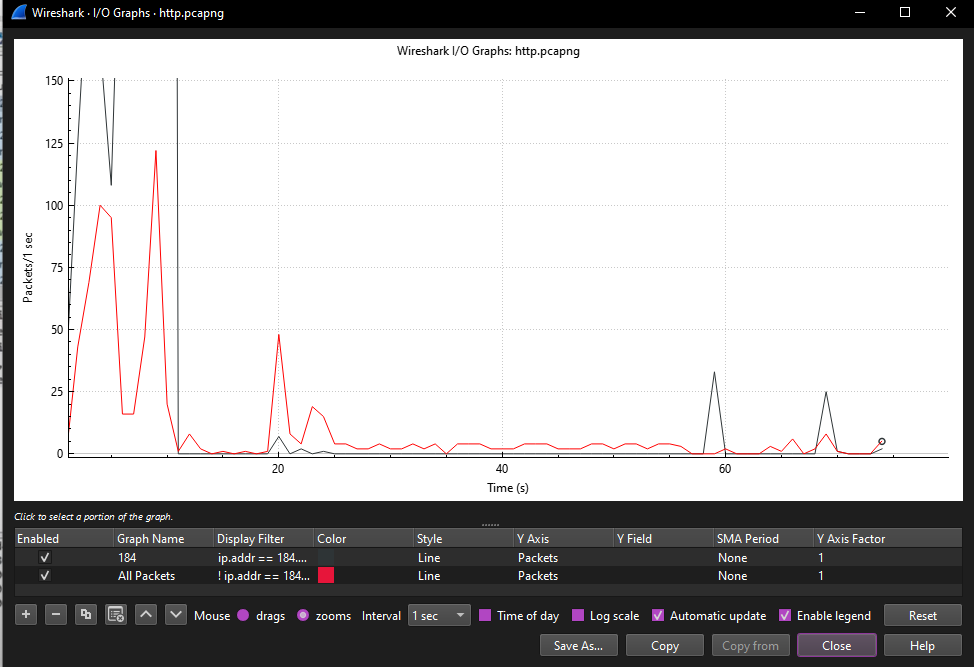


Рис. 14 – i/o graphs

Тест: 