Конспект занятия на тему

**«Программа для** **мониторинга трафика «WIRESHARK»**

Выполнил педагог дополнительного образования

СП ЦЦОД «IT-куб» г. Балашова МБУДО Центра «Созвездие»

Шурыгин Михаил Романович

**Цель** – сформировать представление у школьников 10-11 классов о работе с программой мониторинга «WIRESHARK».

**Задачи**:

- развить с концентрацию внимания;

- научить распознавать трафик (входящий и исходящий);

- развить внимательность при разборе трафика;

- научить пользоваться программой wireshak.

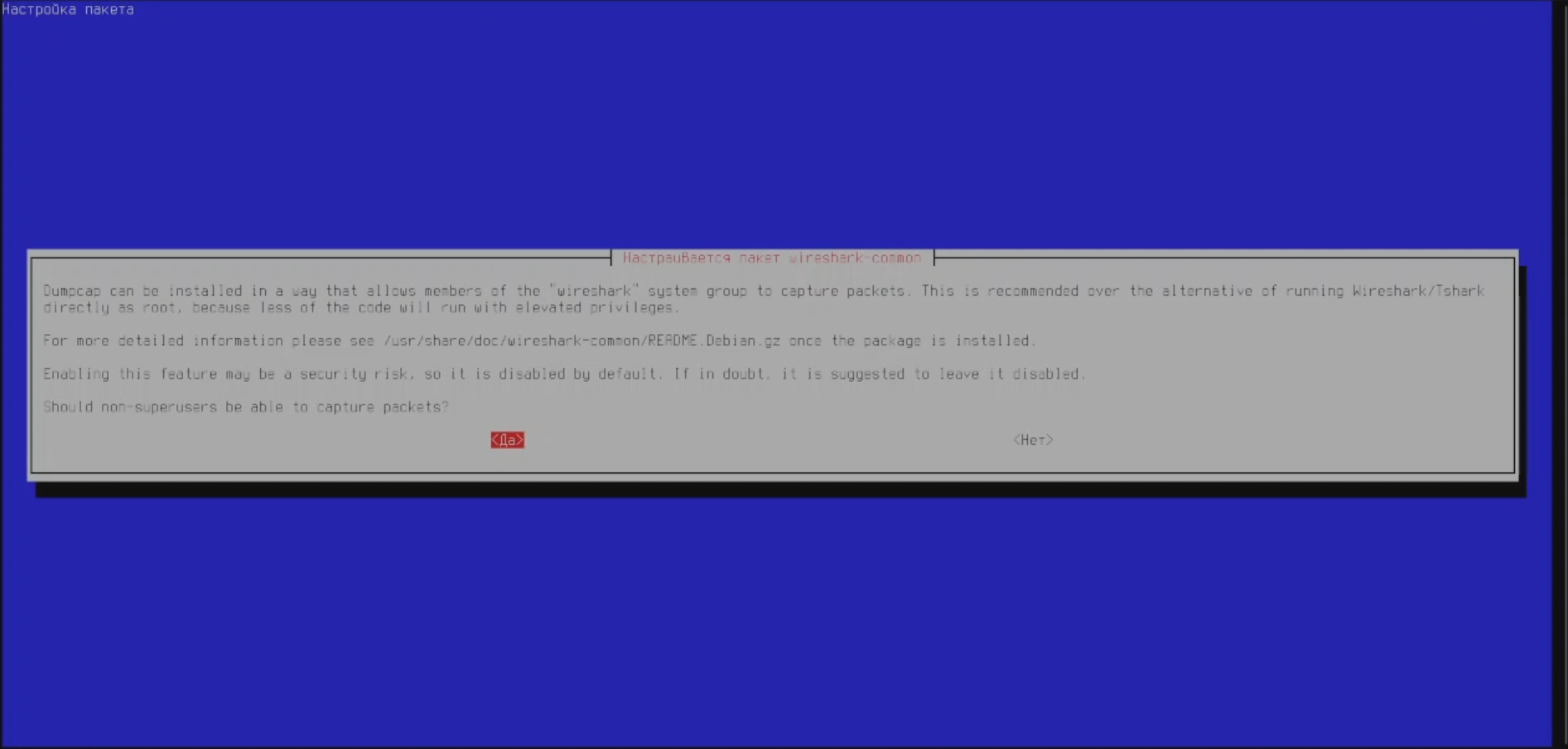
1.Сегодня познакомимся с программой для мониторинга трафика - «wireshark», но сначала ее нужно установить.

Перед установкой wireshark нужно обновить список репозиториев в Ос Astra Linux Орел



Далее устанавливаем wireshark командой apt install wireshark

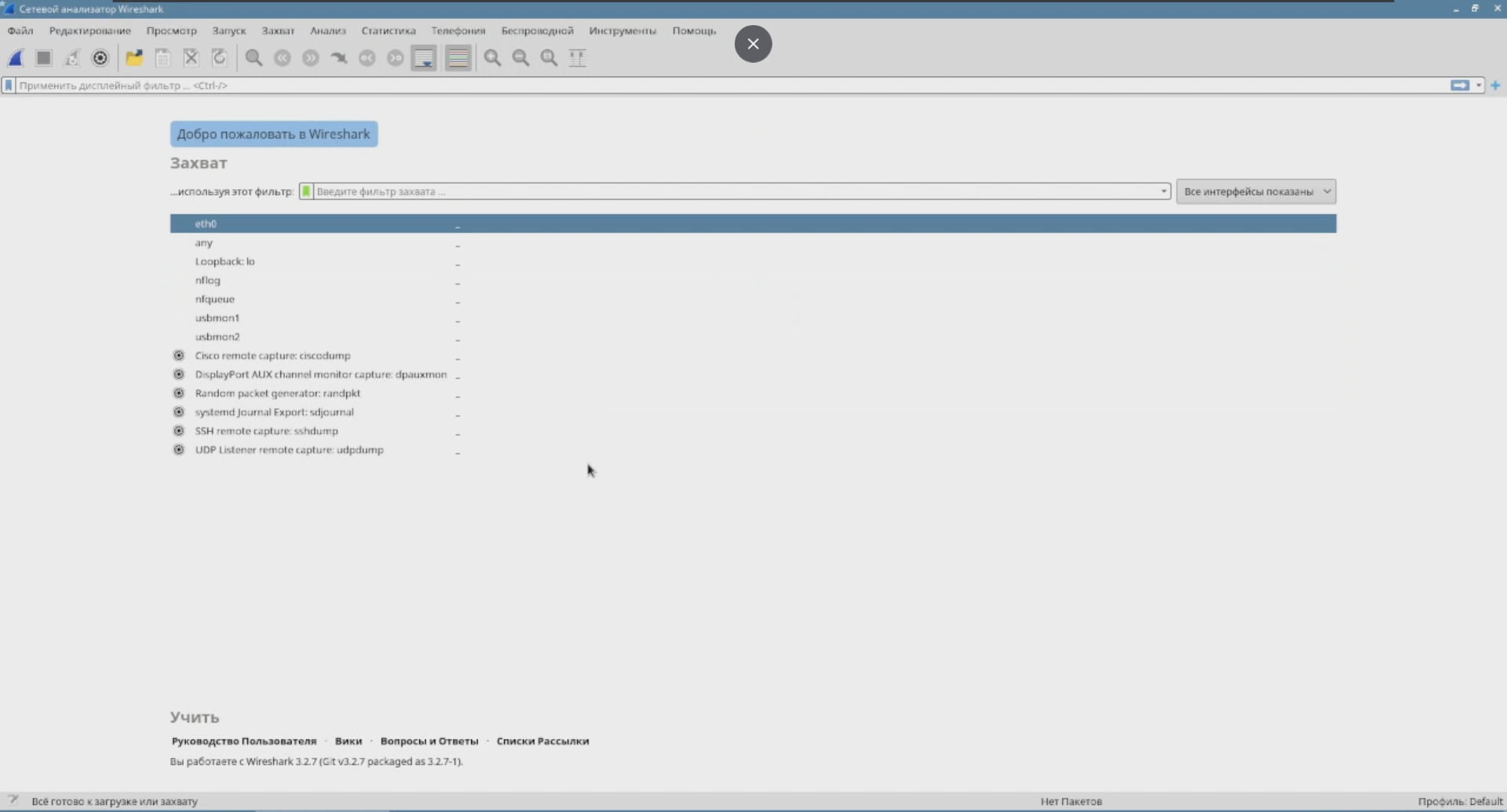


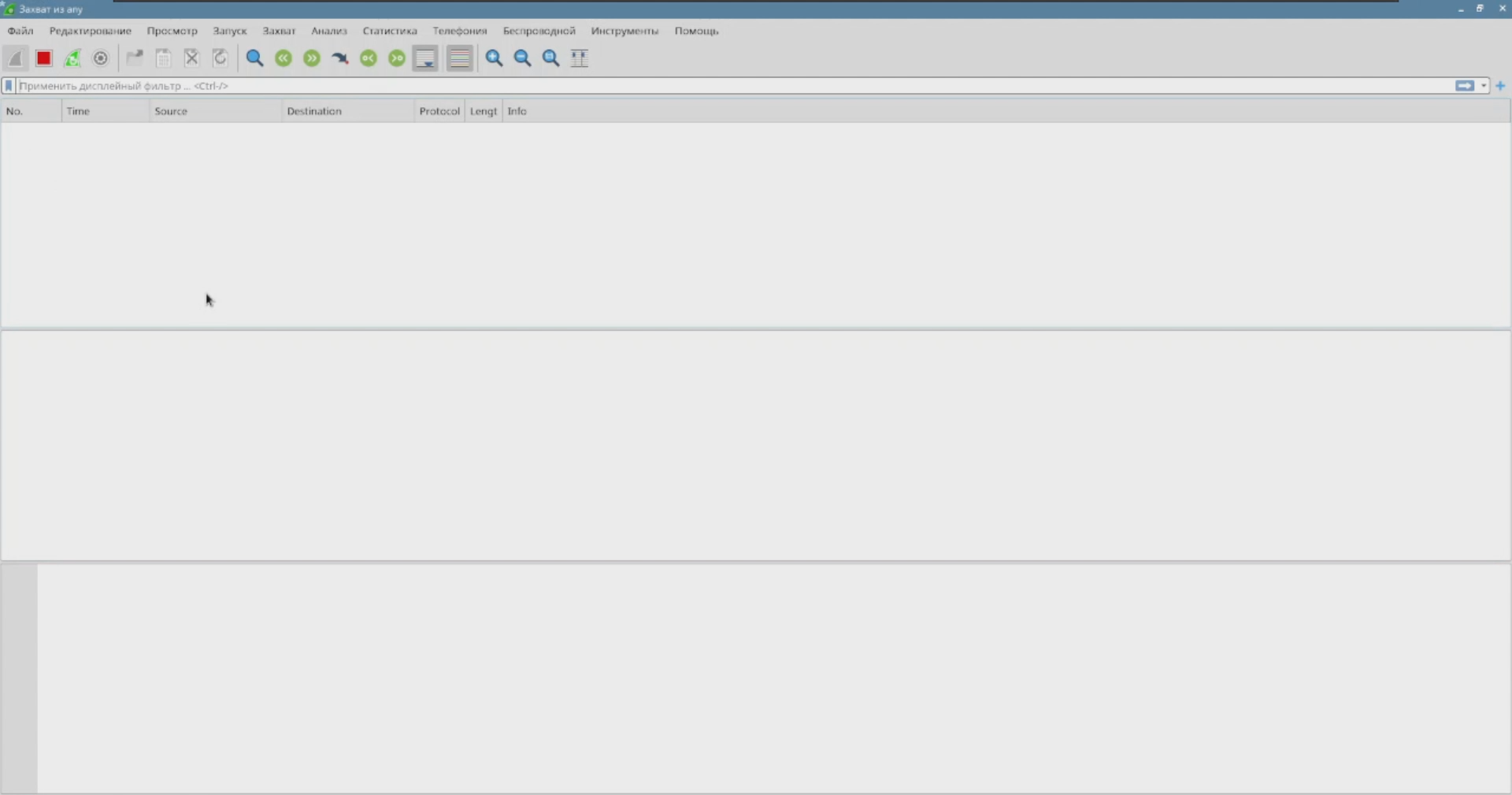
На рисунке при установке нас спрашивают разрешить ли программе захватывать пакеты из сети

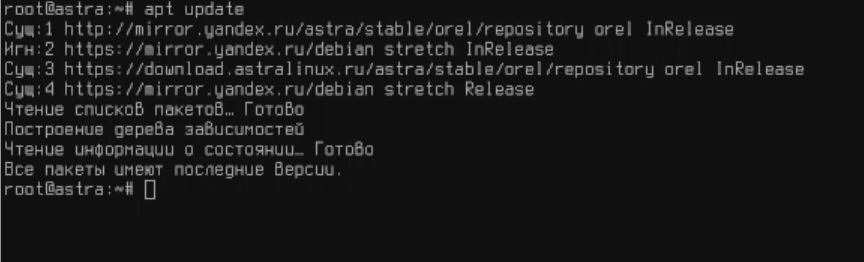
Запускаем wireshark



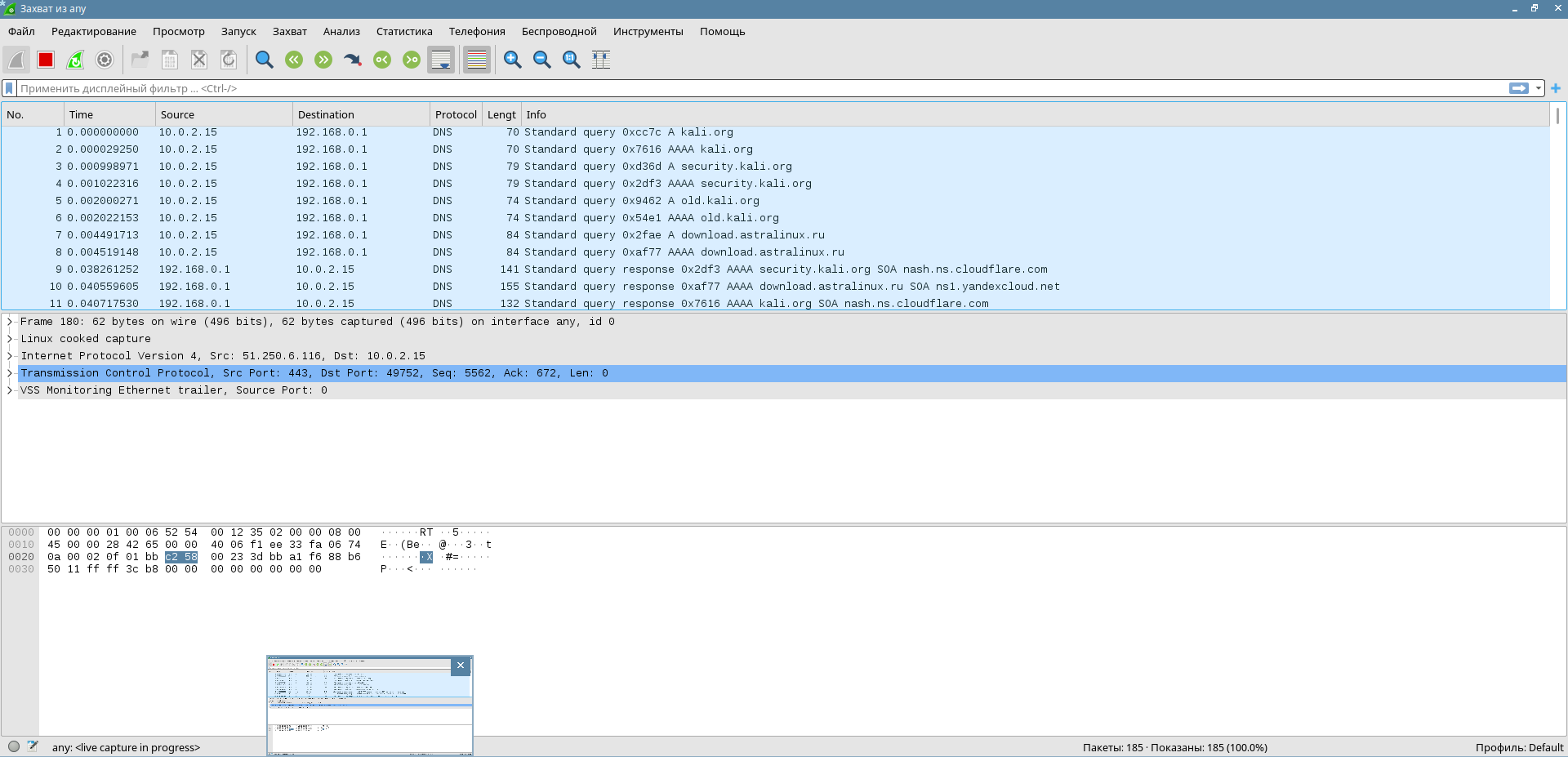
Попадаем в графический редактор

Тут нужно указать какой порт слушать программе, если их несколько можно выбрать 

Программа начала отслеживать пакеты

Для того чтобы увидеть пакеты через второй терминал обновляем репозитории

Получаем вывод программы



Time – время отправки пакета

Source – Источник

Destination – Адрес назначения

Protocol - протокол

Lengt – длина пакета

Info – информация о пакете

В информации о 1 ом пакете написано что это стандартный запрос буква А означает протокол ipv4 или же AAAA означает протокол ipv6

Контроль сетевого трафика позволяет установить, какое из рабочих мест нуждается в повышенной пропускной способности или увеличенном объеме трафика. Так же мониторинг нужен для проверки работоспособности сетевого оборудования или специального ПО, сбоев интернет-соединений, скачков в связи . Достаточно полезная утилита для системного администратора.