Министерство образования и науки Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего профессионального 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"

ТЕМА РАБОТЫ:

Изучения средств мониторинга и анализа сетевого трафика. Сниффер Wireshark (Ethreal)

Выполнил:

студент гр. ПРИ-120

Парахин К.В.

Принял:

Доцент кафедры ИСПИ

Курочкин С.В.

Владимир 2022 г.

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 задания:

Для начала установим программу-сниффер Wireshark и выберем из предложенного списка беспроводную сеть.

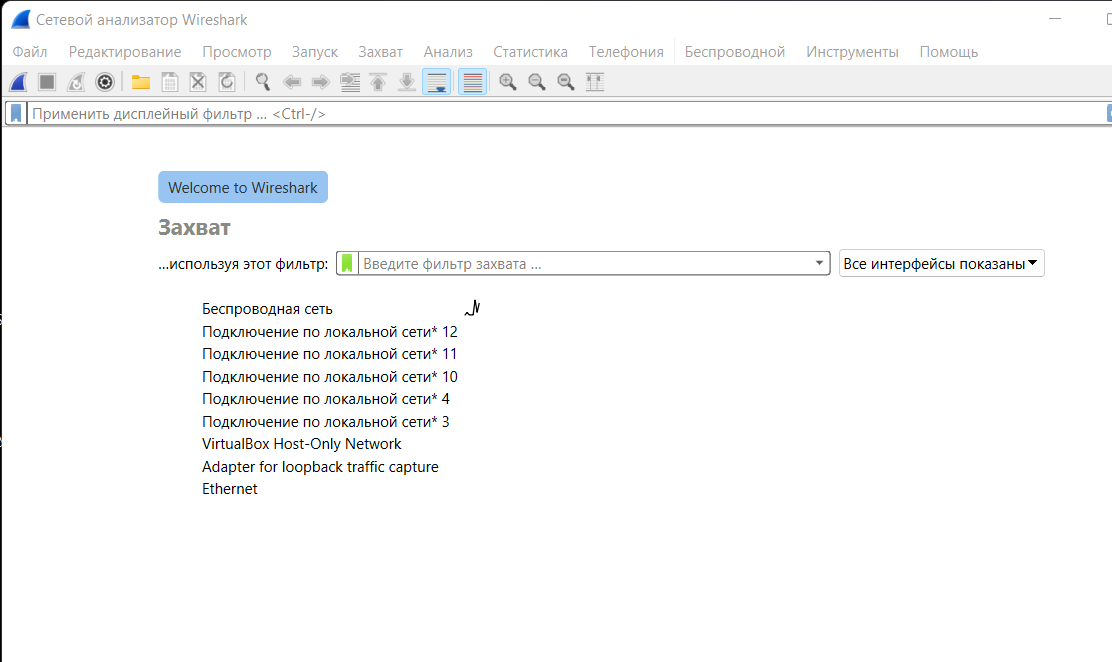


Рисунок 1. Скриншот установленной программы Wireshark

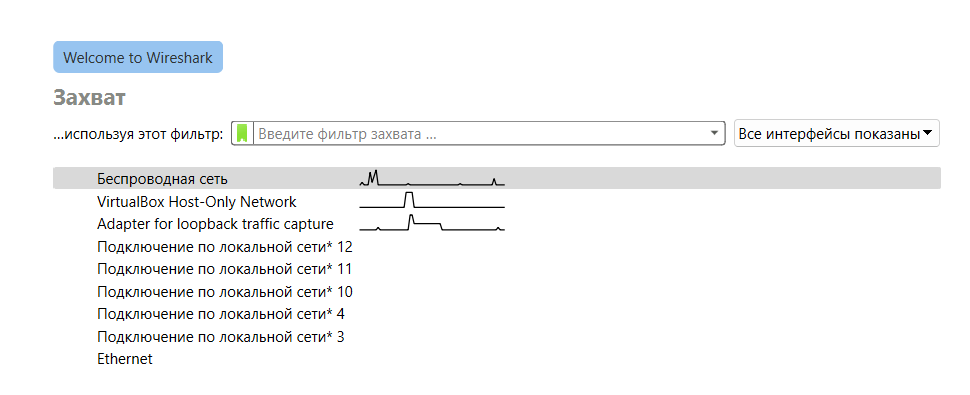


Рисунок 2. Скриншот выбора сети

Перейдем во вкладку «Опции Захвата»:

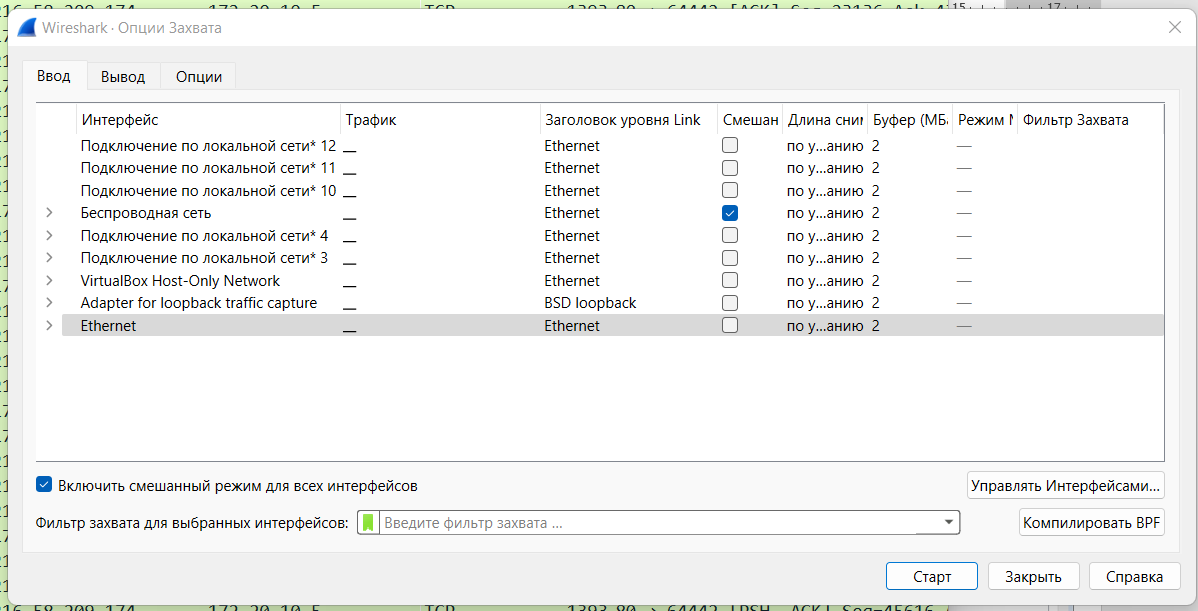


Рисунок 3. Скриншот установки галочки на той сети, пакеты которой хотим перехватить

Перейдём на вкладку «Опции»:

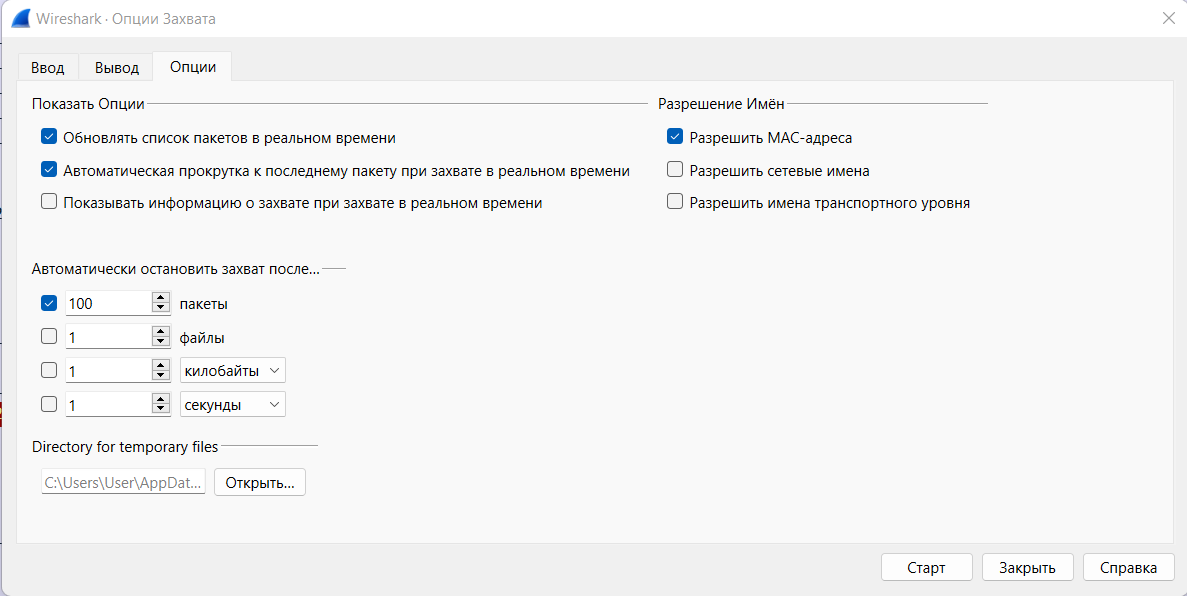


Рисунок 4. Скриншот выставления параметра автоматической остановки захвата после того, как будет перехвачено 100 пакетов

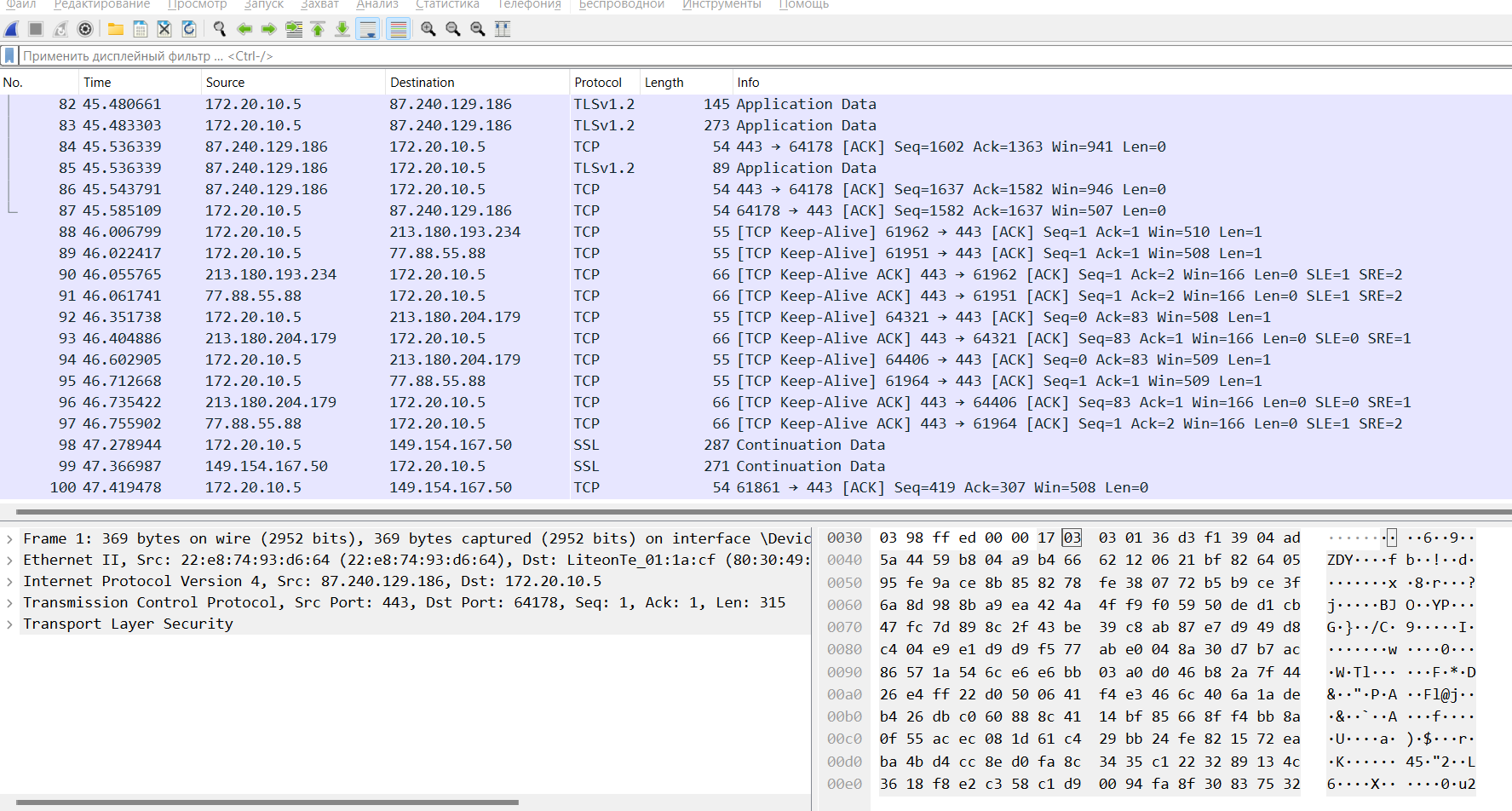


Рисунок 5. Скриншот запуска захвата после перехвата 100 пакетов

меню «Статистика/Длина пакетов» можно видеть 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).

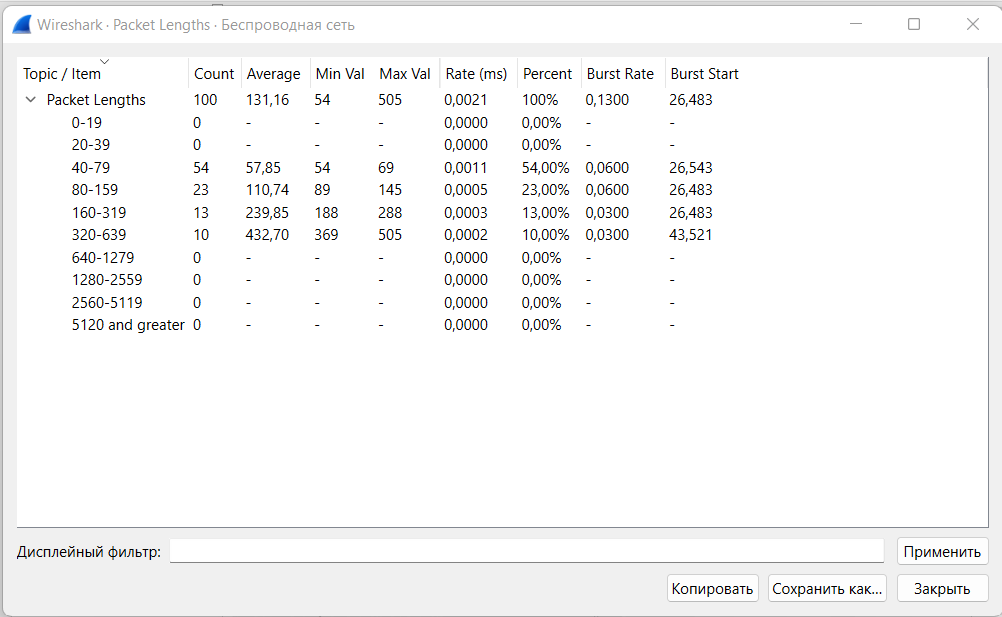


Рисунок 6. Скриншот вывода статистики

Перейдём во вкладку «Опции Захвата» и установим значение пакетам (равно 20 единицам)

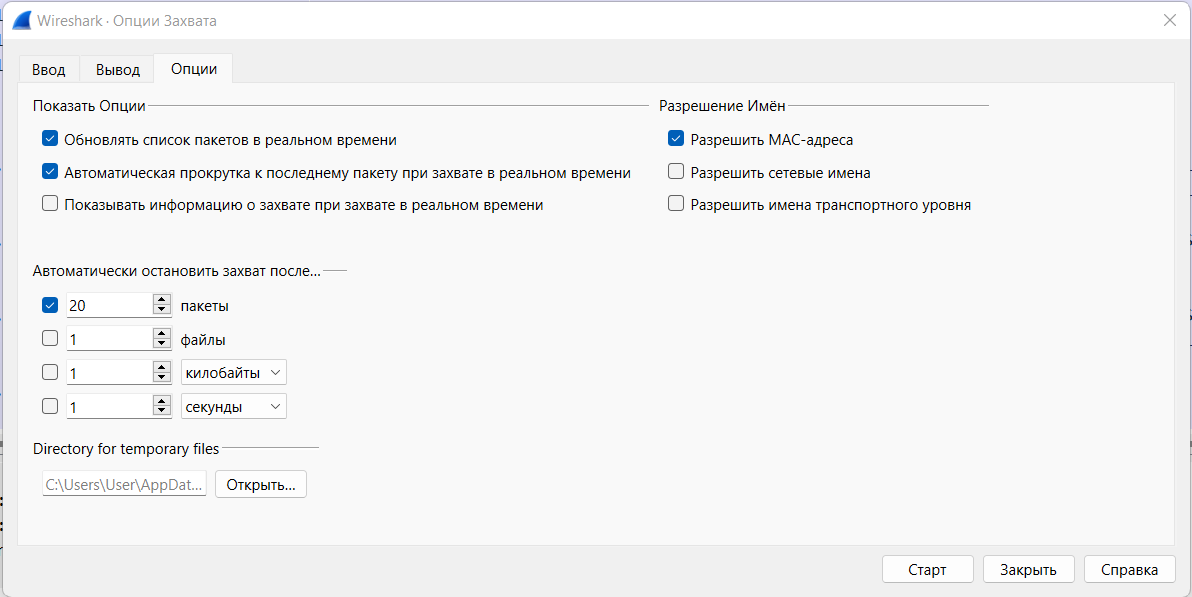


Рисунок 7. Скриншот установки значения автоматической остановки захвата после двадцати пакетов

На следующем рисунке в среднем окне отображается информация о пакетах, а в нижнем MAC адреса.

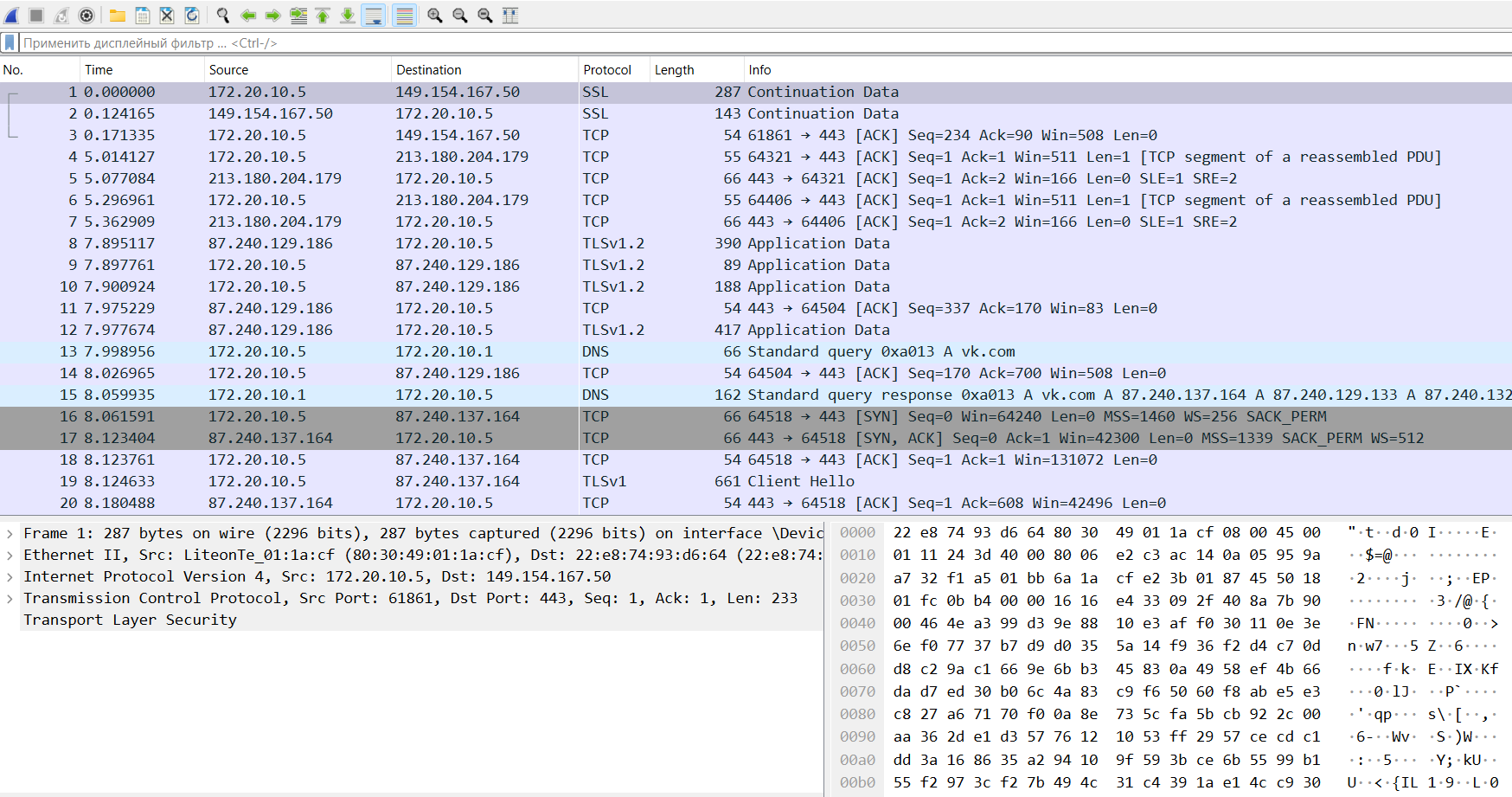


Рисунок 8. Скриншот захвата 20 пакетов

Перейдём во вкладку «Статистика», далее в меню «Иерархия протоколов»:

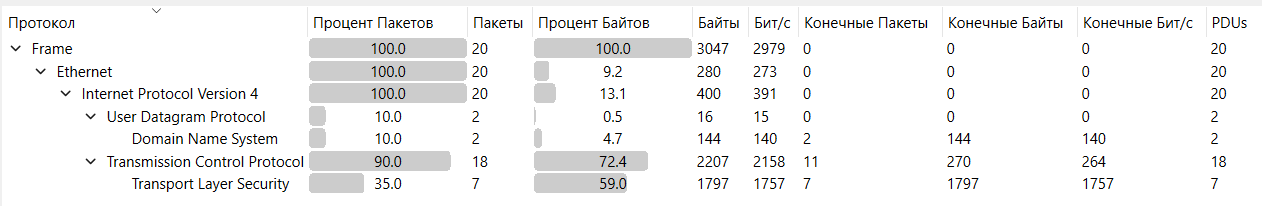


Рисунок 9. Скриншот статистики

Анализ ARP протокола:

ARP протокол - сетевой протокол, предназначенный для преобразования IP-адресов (адресов сетевого уровня) в MAC-адреса (адреса канального уровня) в сетях TCP/IP.



Рисунок 10. Скриншот применения фильтра для arp-протокола

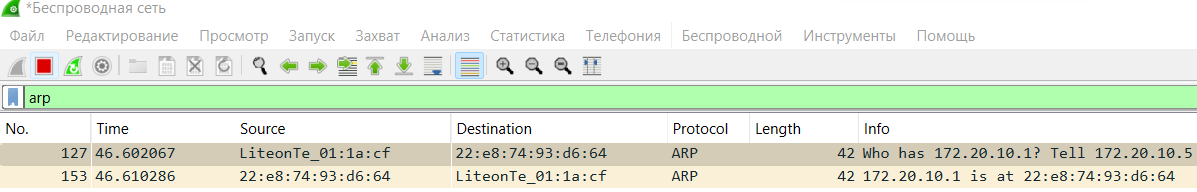


Рисунок 11. Скриншот имеющихся arp-протоколов

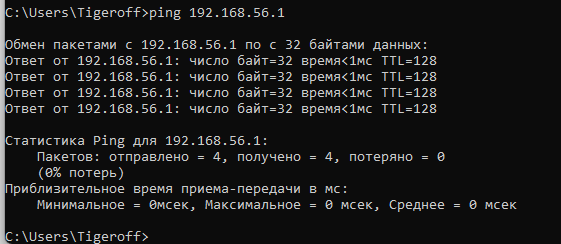


Рисунок 12. Скриншот создания запроса на обмен пакетами

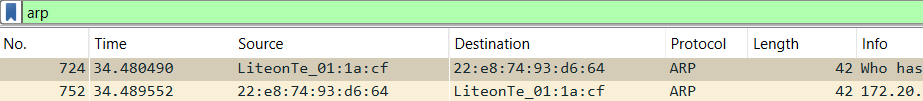


Рисунок 13. Скриншот результата запроса

Просмотрим ARP-кеш при помощи команды arp -a. В результате выполнения команды будет известно, что в кеше хранится 7 записей, а также мы сможем наблюдать IP и MAC адреса машин.

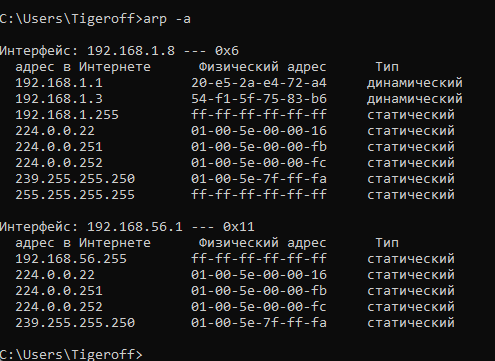


Рисунок 14. Скриншот выполнения команды arp -a

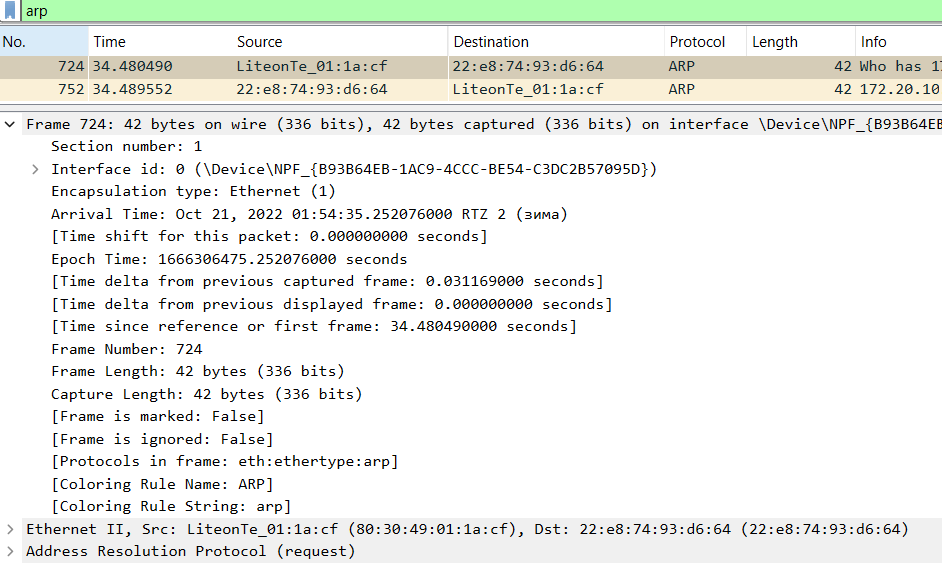


Рисунок 15. Скриншот просмотра детальной информации о пакете (строка Frame)

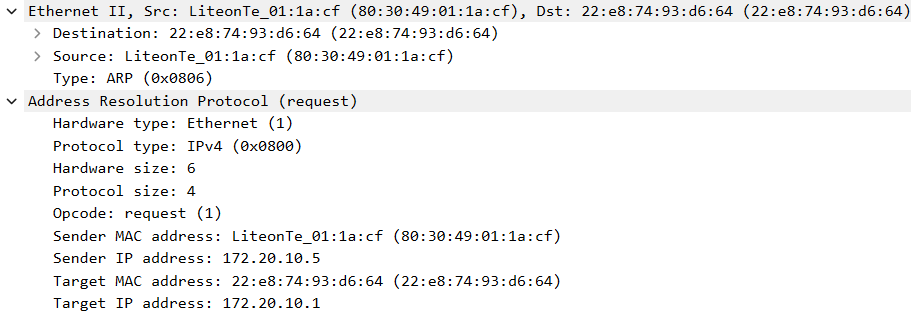


Рисунок 16. Скриншот просмотра детальной информации о пакете

(строки Enternet II и Address Resolution Protocol (request))

Анализ утилиты «Ping»:

*Ping* – утилита командной строки, которая нужна для проверки подключения к другому компьютеру на уровне IP. Принцип работы очень простой: команда ping ip отправляет серию небольших пакетов данных на указанное устройство, а затем показывает время ответа.

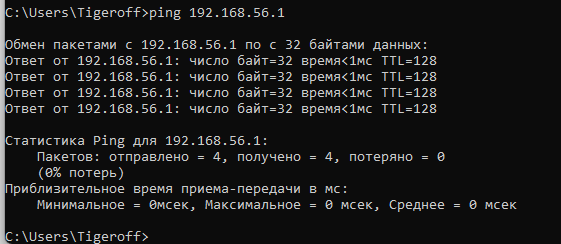


Рисунок 17. Пример вызова утилиты ping

Вывод

В результате выполнения работы я научился использовать сетевой анализатор (сниффер Wireshark) и анализировать сетевой трафик на примере протоколов ARP, IP и ICMP.