Лабораторная работа №3

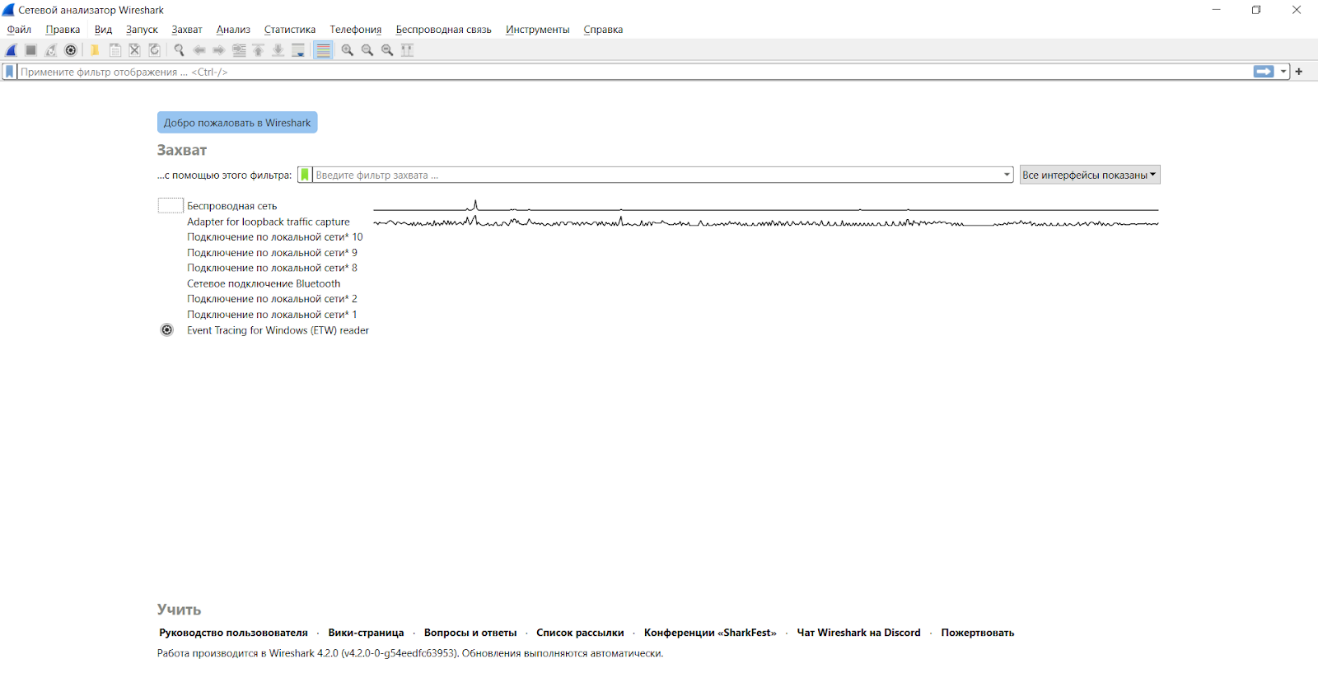
Wireshark - очень крутая программа, она позволяет смотреть на все пакеты которые проходят через хост. Через неё можно увидеть типы данных, ошибки при их передаче, а также при некотором умении вычислить личерскую программу, или майнер.

Программа имеет большую базу фанатов, хороший справочник и встроенный русский язык

Скачиваем с официального сайта и запускаем

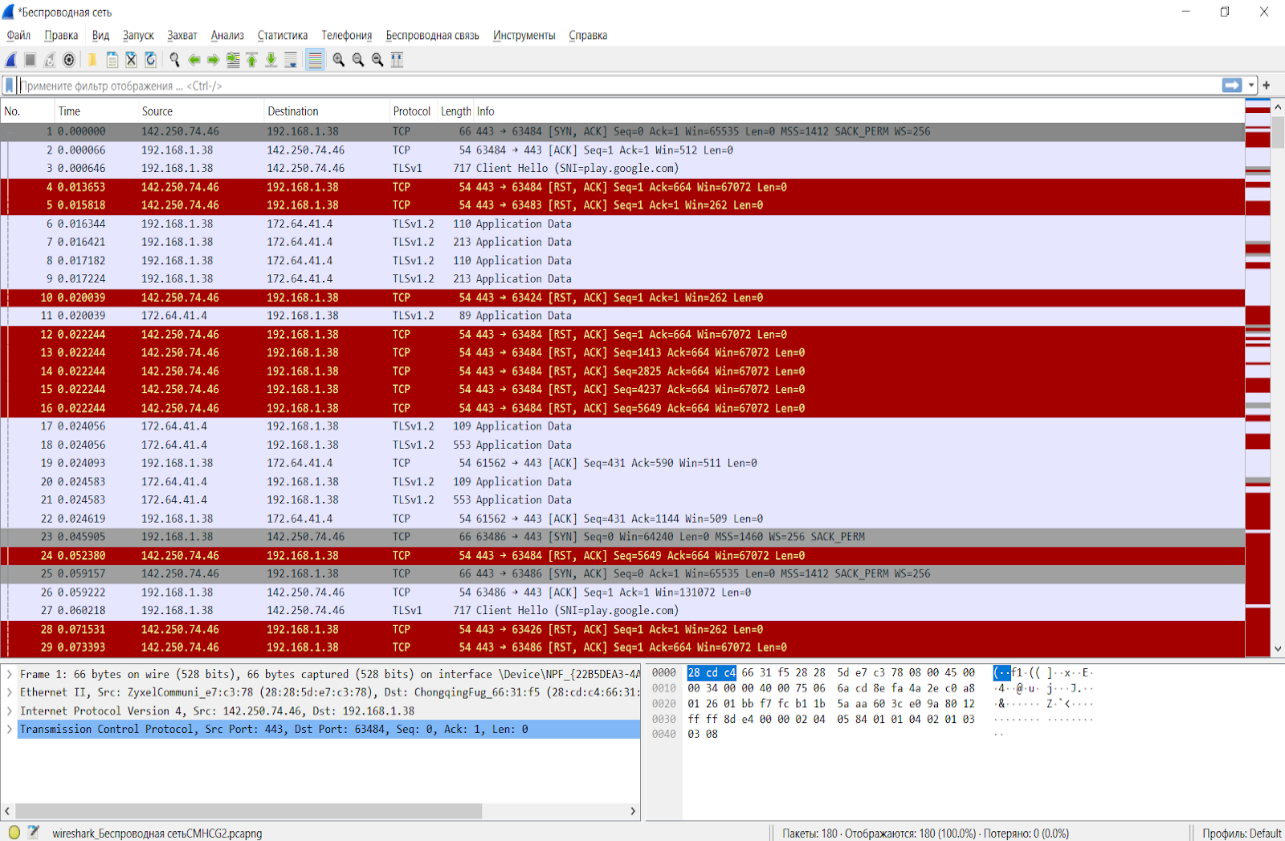
Потребует скачать Ncap, его тоже скачиваем

В итоге запускаем приложение и попадаем в главное меню



В приложении есть много вариантов захвата, но нас интересует именно беспроводная сеть - wifi

Выбираем её и попадаем сюда



Захват пакетов начинается автоматически, поэтому можно его отключить нажав на панели красный квадрат( у меня он уже нажат, т.к я остановил захват)

Сама программа работает так, что она записывает все пакеты которые через нее проходят, создает файл, и дальше можно либо работать с этим файлом, либо начать запись заново.

Можно работать с файлами из других устройств

В программе есть различные колонки

No или № показывает номер группы пакетов, отсчёт начинается с 1

Time - время получения пакета, ведёт отсчёт от 0

Source - ip отправителя пакета

Destination - адрес отправленного пакета

Protocol - Протокол по которому передаются пакеты - udp, tsp, http и.т.д

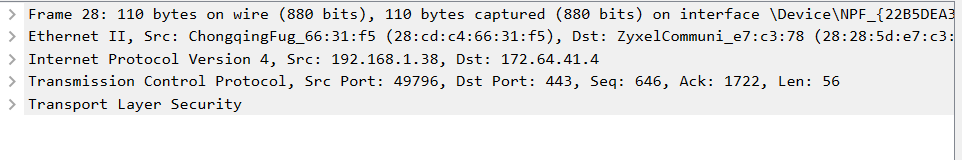
Length - длина пакета в байтах

Info - дополнительная информация

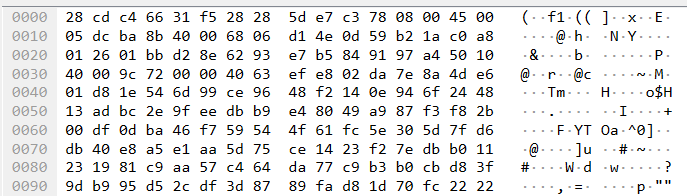
Если требуется отсортировать по порядку колонку, просто нажмите на название.

Чуть выше есть фильтр, туда можно вбить интересующие вас параметры - протокол или нужный ip

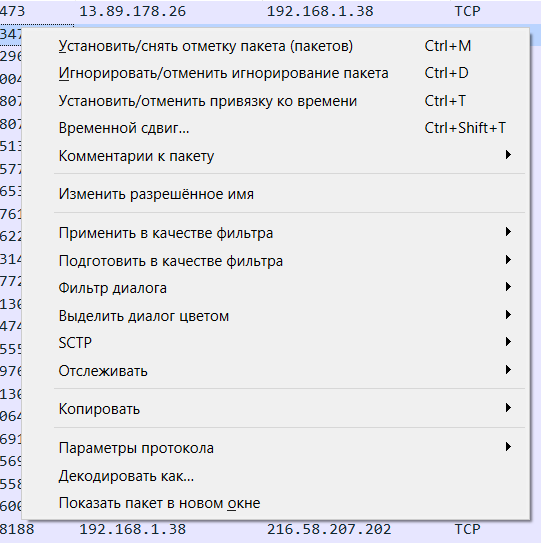
снизу справа расположено контекстное окно, при нажатии на группу пакетов там появится полная информация о них



Справа внизу расположен просмотр пакетов



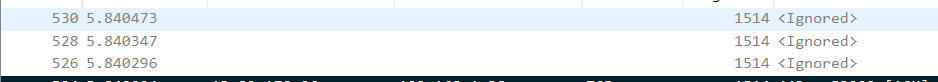
По нажатию правой кнопкой мыши будет открыто меню



Отметка пакета перекрашивает цвет в черный

https://lh7-us.googleusercontent.com/7I9sLxWBwcSe5Uh8Un6VcQknqW8llO-VkyBDJrGkcoxrN4aWqXh8yvlHShAGPTHaANDp42W79LAMTEM4J1acg6_fNeHdA0aA_saC0pVx8xUvjr0TnDnoQnI5cGB4bNSSzrk7WAqRymKaR3fWsaSPTG8

Игнорирование пакета перекрашивает его в серый и деактивирует



Привязка по времени устанавливает и убирает привязку

https://lh7-us.googleusercontent.com/s_5s1_K45q8vnsCzz2l4MGA4LSChF_DbvIwYVTLxTaAkjpdS4fWwXFElpS1Ib3NG_1-zB_QKJbK_QVL187RqENioxeu6qNKaZmH2c7ashi_qu-M9K27mzltzVnrkKujgaKDyA4sf-DTSNVygSKk5dbs

Временной сдвиг смещает пакеты по времени

Комментарий к пакету это комментарий

Дальше идут различные точечные выделения и покраска

Далее идёт основное меню

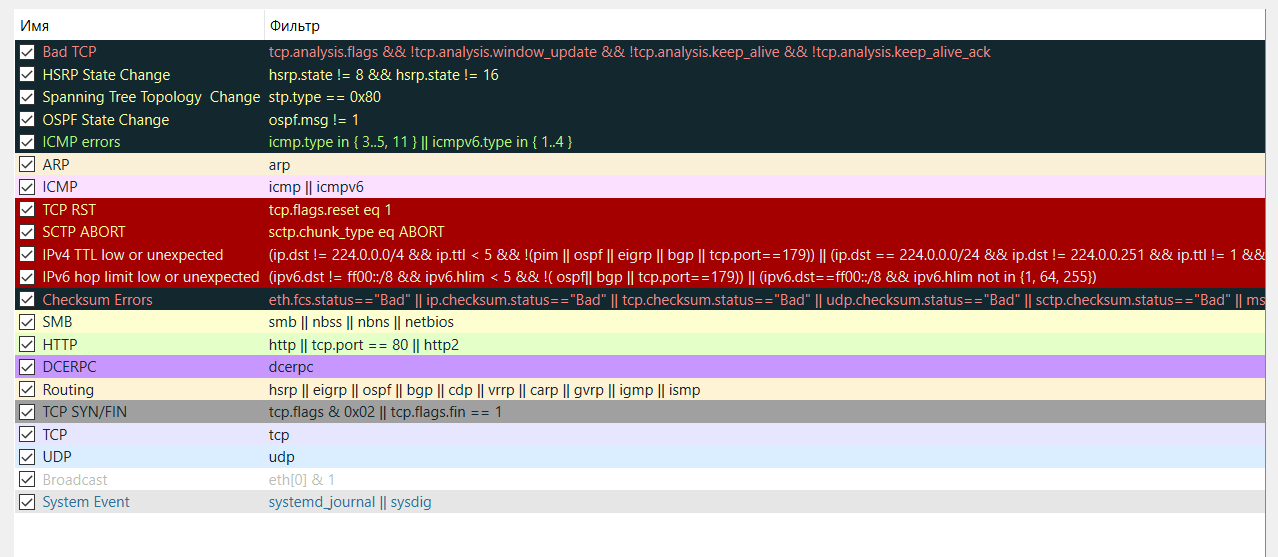
https://lh7-us.googleusercontent.com/LRTXz0Pf8RrofPYww5so68HsRfQVWWZKfRCAo8g0ufhiglUq8t5b16XOQP1JS6ElRuh7rwhZN8_F7Oo_0jjXTwLwt3luALp6WPRaiwsBSmTNt_ChqbbM2DUThja1SK55yHWRZbMi2d8tjcc3t8dw4yY

Запуск, остановка, рестарт, смена захвата.

Открыть, сохранить, закрыть, перезагрузить файл захвата.

Переходы по пакетам

Цвет пакетов настраивается во вкладке вид, там его к слову можно и отключить



Например чёрный цвет означает сообщение о ошибке или изменении, красный это прекращение работы или ресет, остальные же более спокойные цвета означают виды запросов.

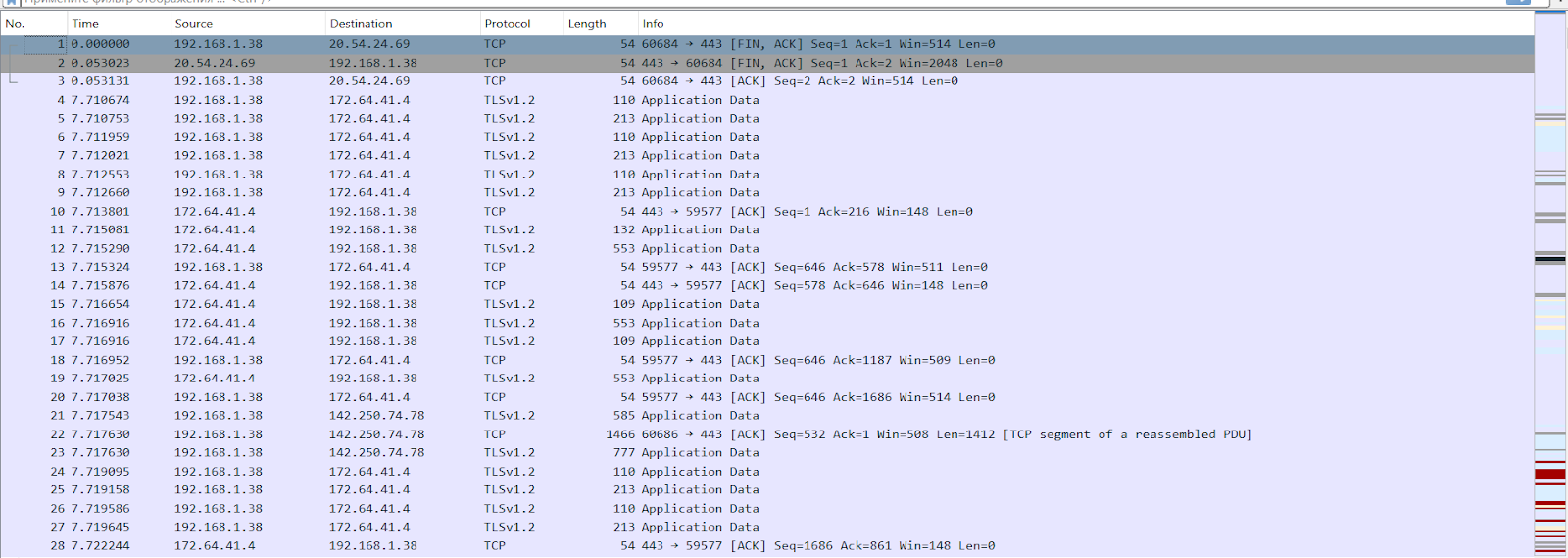
Также есть функции работы с ip-телефонией, статистикой и анализом.

Касательно работы программы.

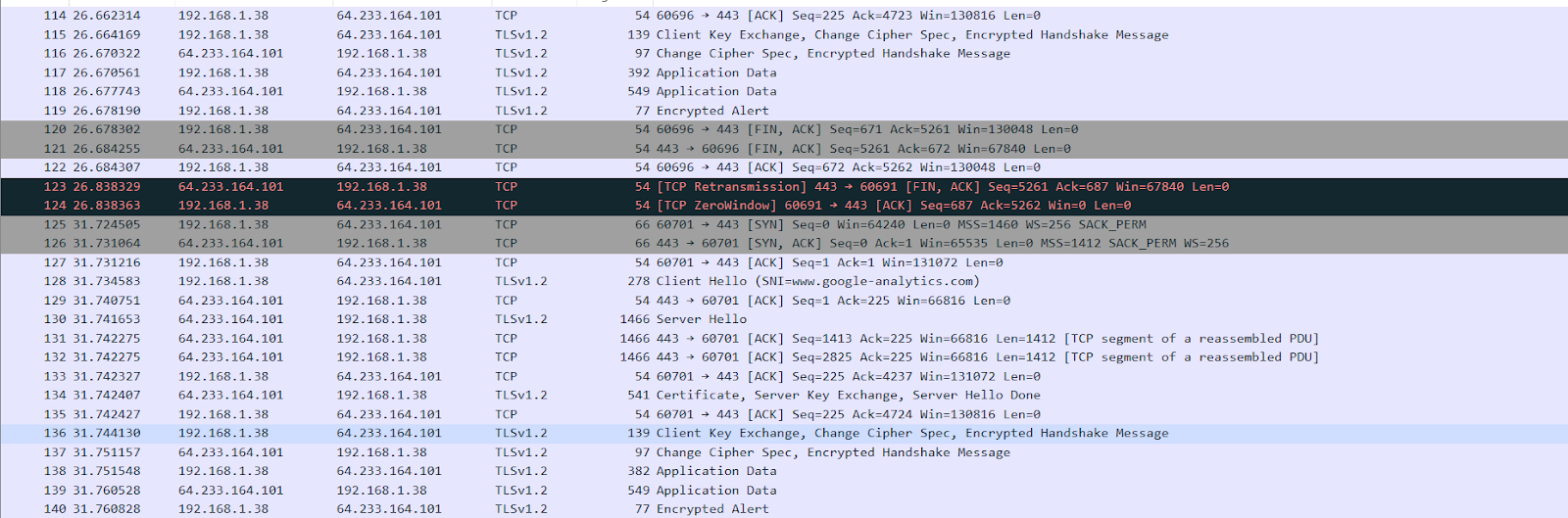
Запущу захват на одну минуту

Справа можно увидеть колонну с ивентами.

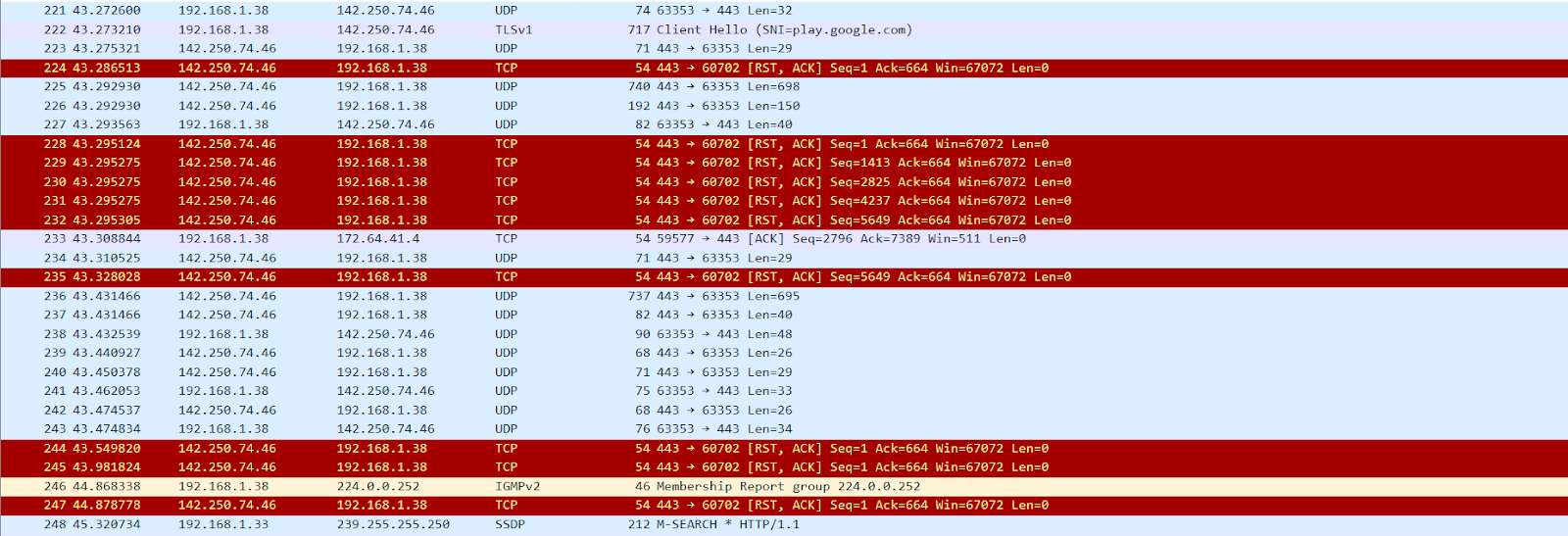
Начало



Середина



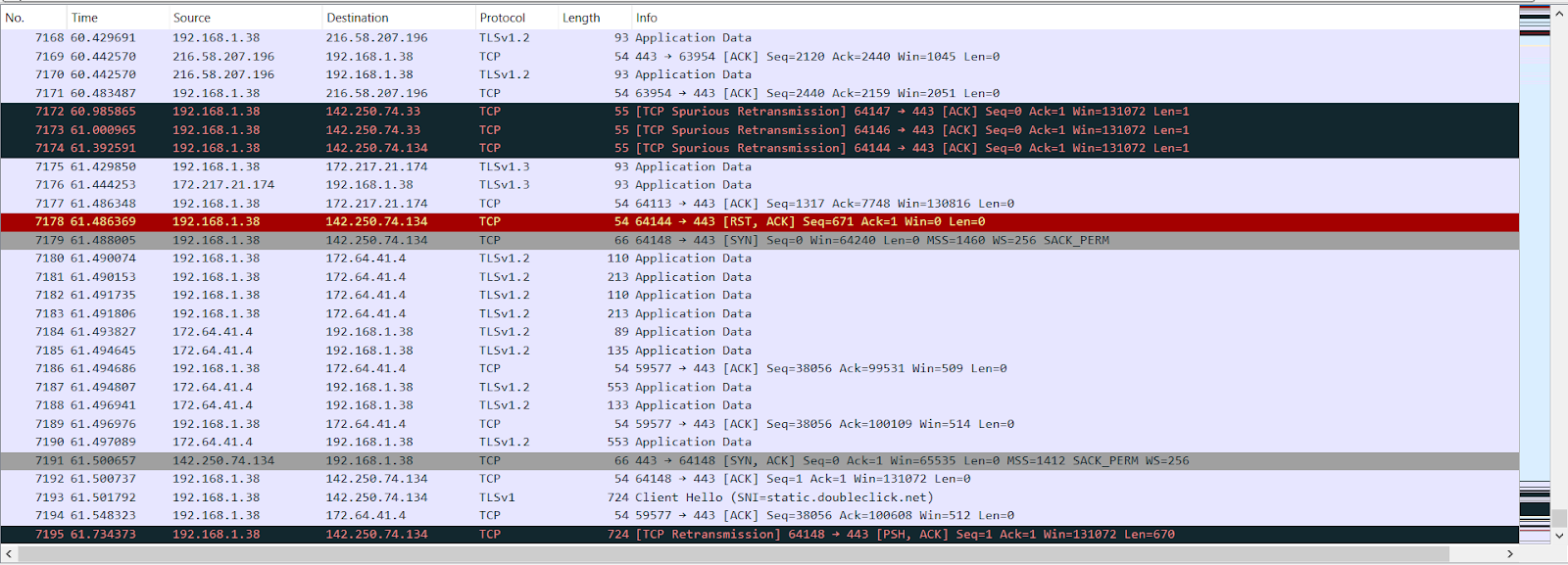
Конец



Так выглядит программа с захватом в состоянии простоя компьютера( когда ничего не происходит и открыт интернет)

Пачек пакетов всего 250 за минуту и всё довольно стабильно

Однако если мы допустим откроем видео на Youtube, то всё полетит.

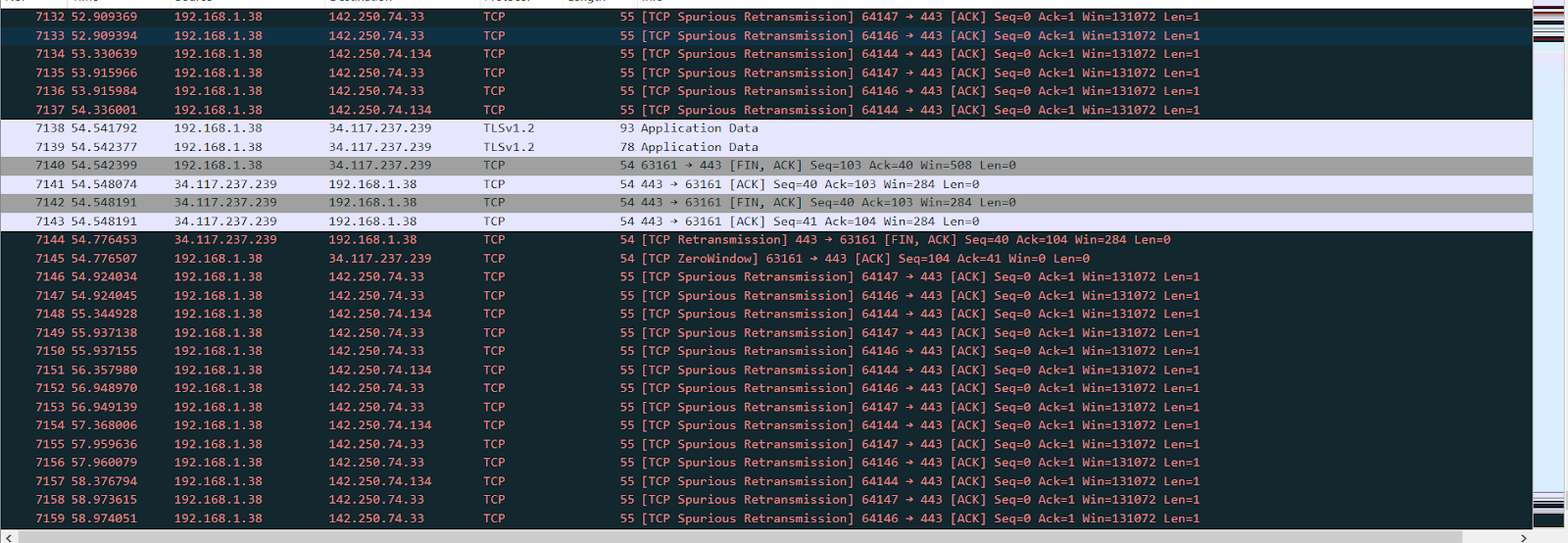


Количество пачек пакетов возросло до 7200

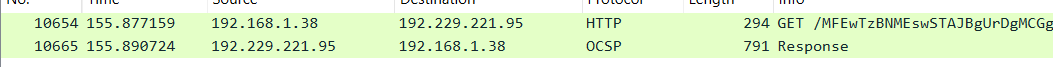
Также стоит заметить что трафик поставлялся поочередно

Сначала идут tcp, tlsv1, tlsv1.2 запросы, а потом идут QUIC запросы.

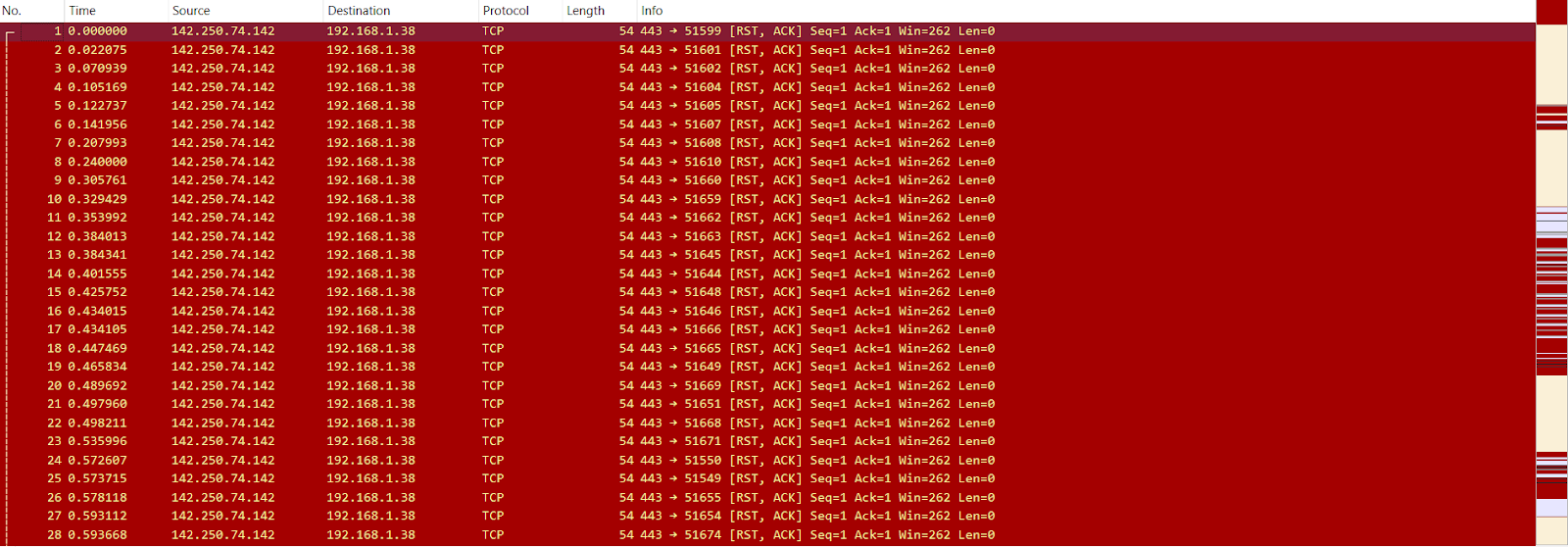
Также можно заметить скопления потерей пакетов

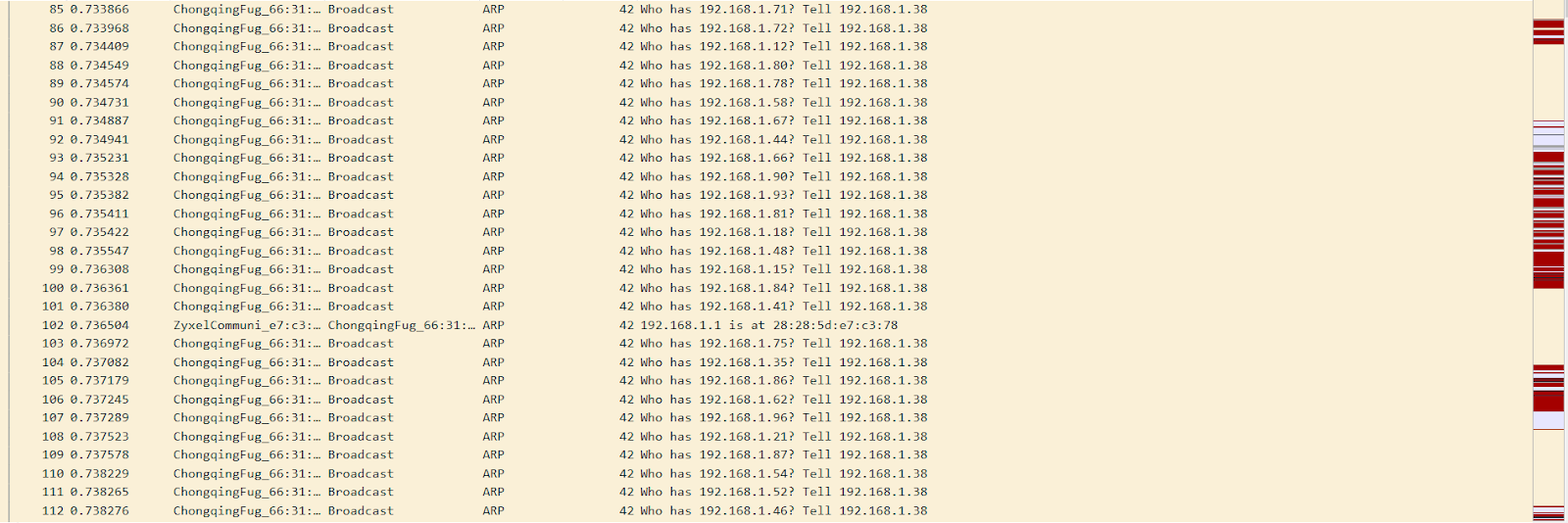


А вот и http протокол



Наконец пример работы с Advanced IP Scanner. Сканирование моей подсети.





Компьютер отправляет через широковещание огромное количество сообщений, однако так как в моей подсети только 4 устройства, он возвращает столь же огромное количество ошибок.