МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«Санкт-Петербургский национальный исследовательский университет  
информационных технологий, механики и оптики»

Лабораторная работа №5

Выполнил студенты группы М3204:  
Наскальнюк Никита Андреевич

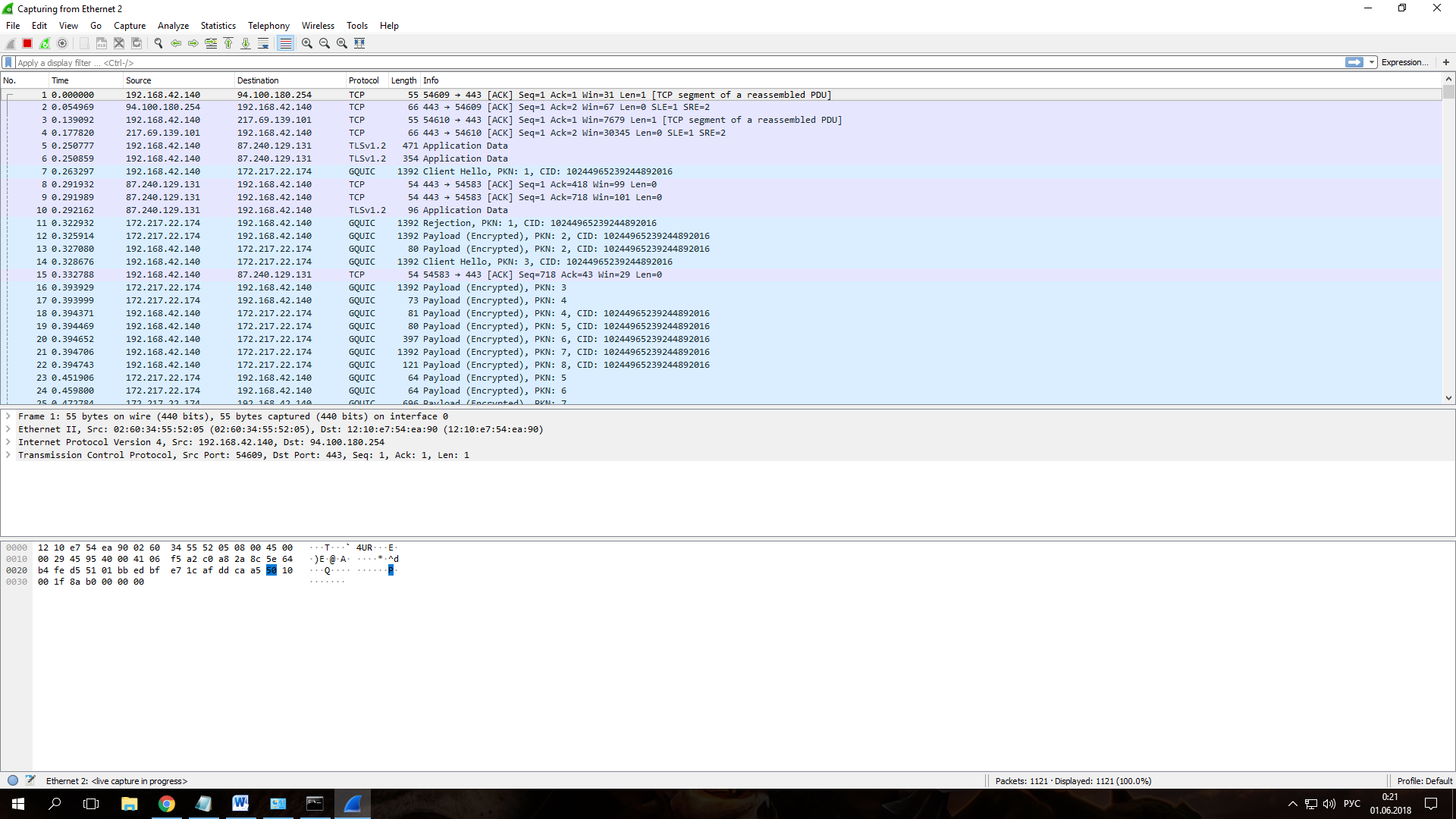
САНКТ-ПЕТЕРБУРГ  
2018

## ***Цель работы***

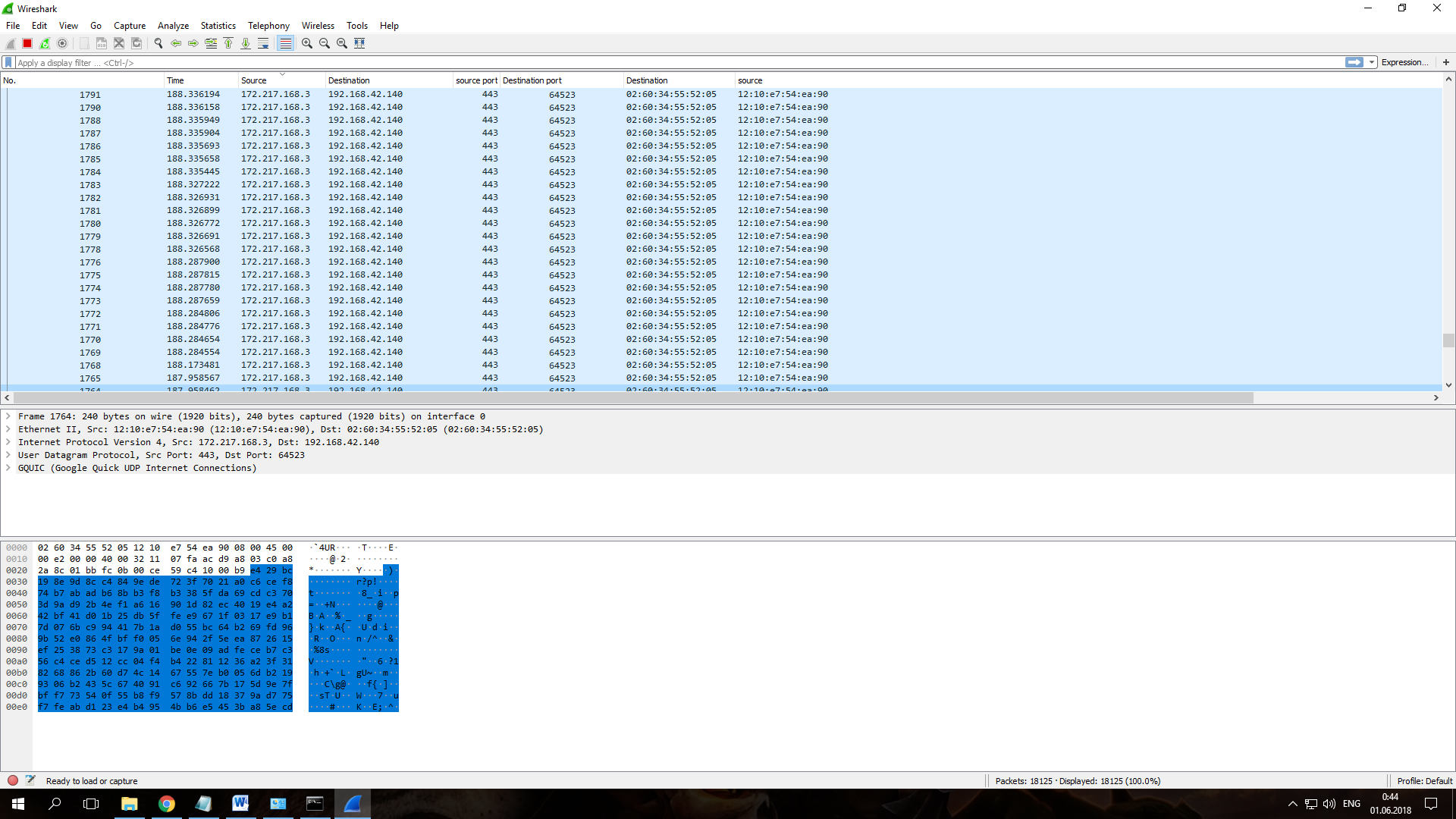
Формирование навыков по использованию основных программных инструментов анализа сетевого трафика.

## ***Перечень используемого оборудования и ПО***

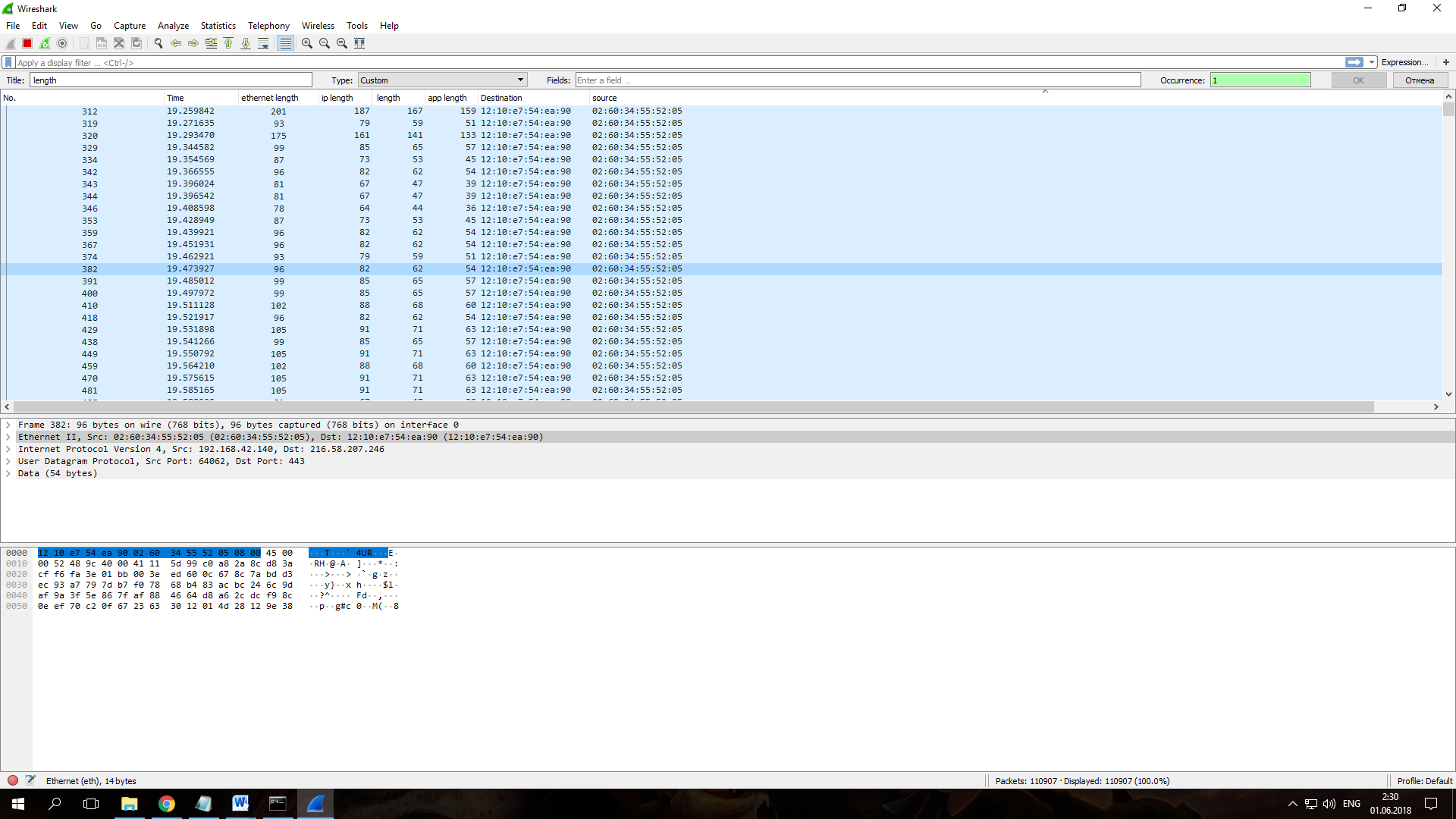
1) Персональный компьютер с ОС Windows, OC Linux или ОС Mac

2) ПО Wireshark 

*Рис. 1. “Список доступных интерфейсов для захвата”*



*Рис.2.”Отображение по адресам”*



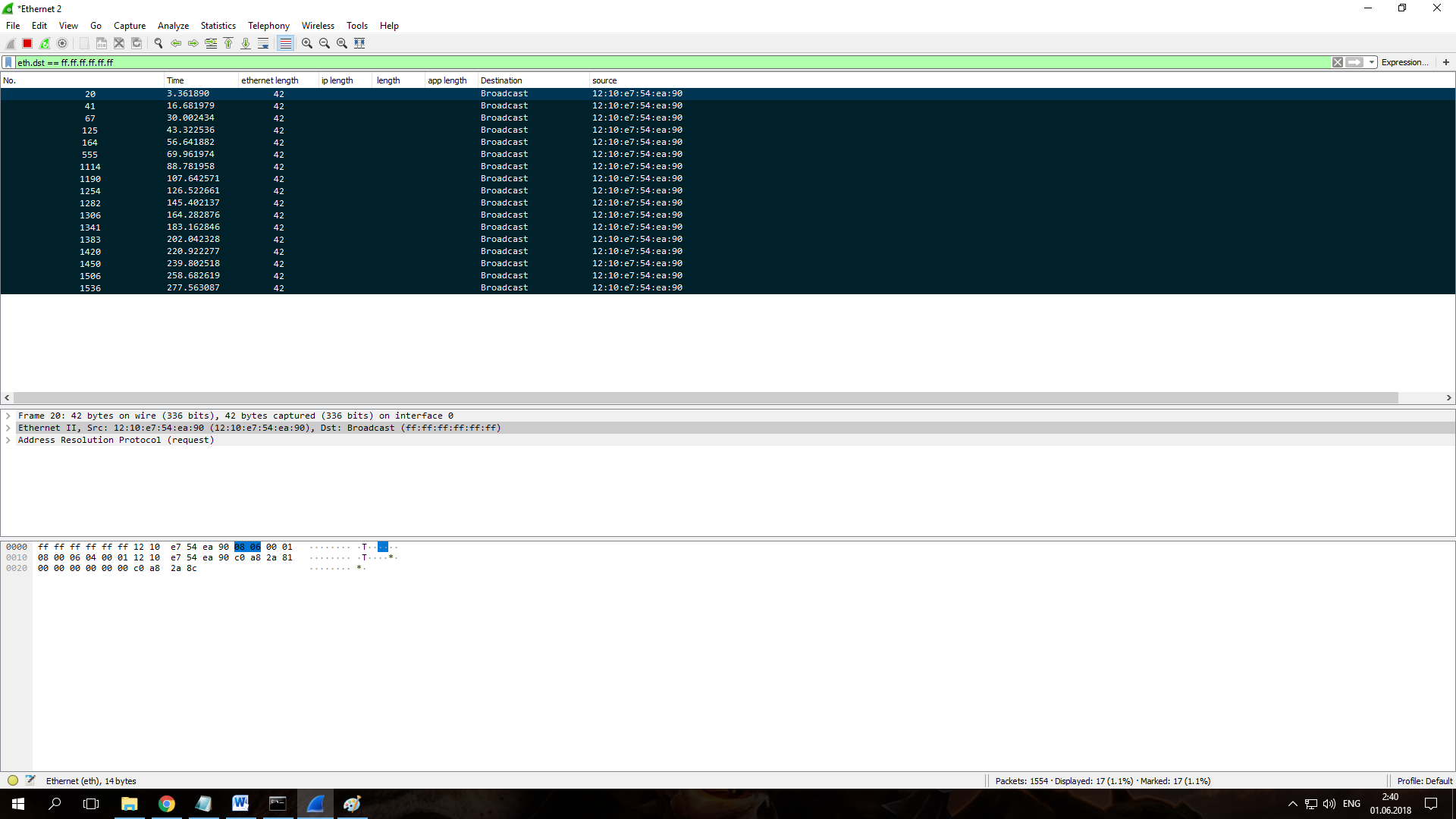
*Рис. 3. “Отображение по длинам”*

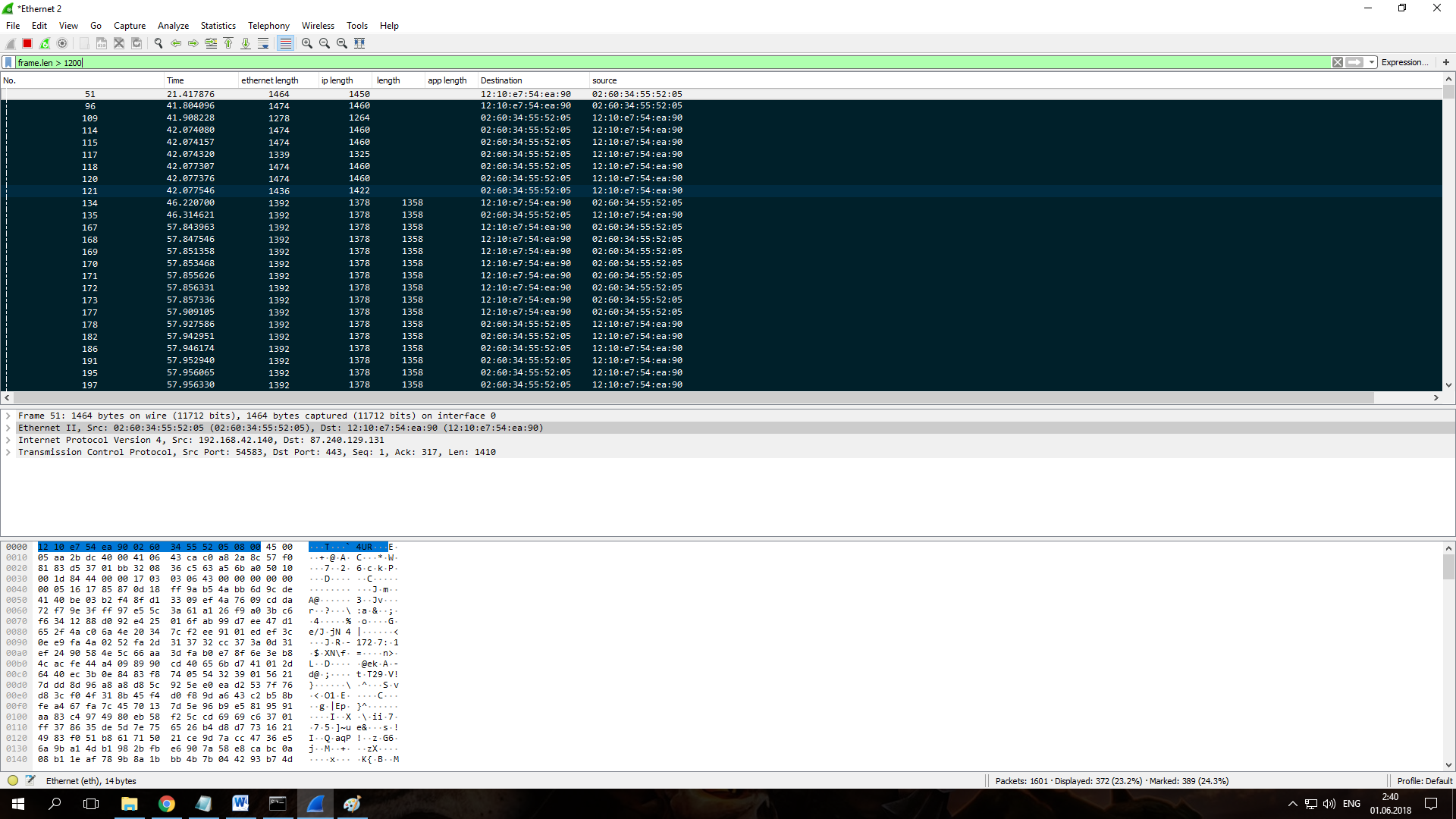
Таблица 1 – Длины протоколов

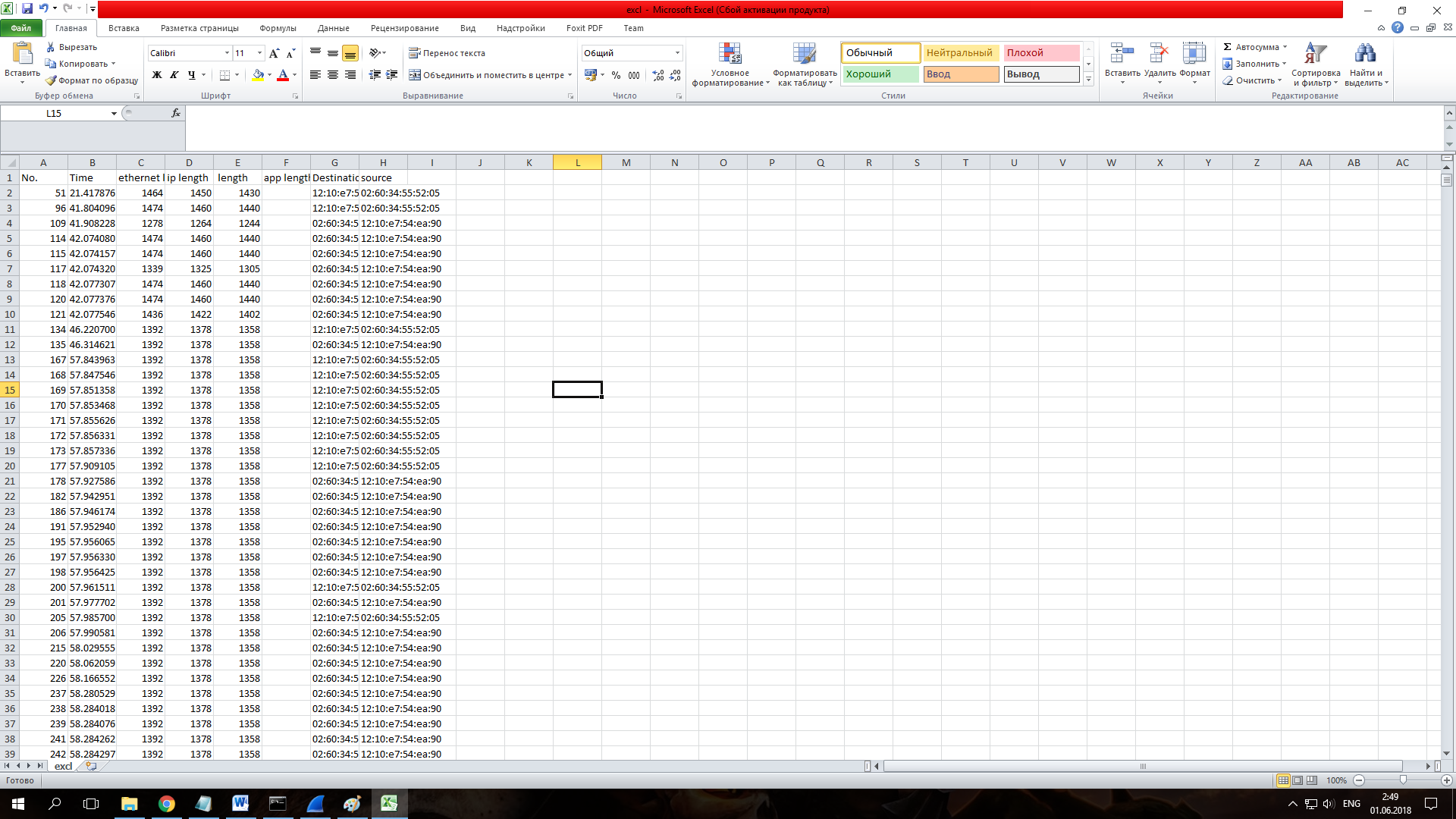
|  |  |  |
| --- | --- | --- |
| **№** | **Параметр** | **Значение** |
| 1 | Длина протокола канального уровня |  |
| 2 | Длина протокола сетевого уровня |  |
| 3 | Длина протокола транспортного уровня |  |

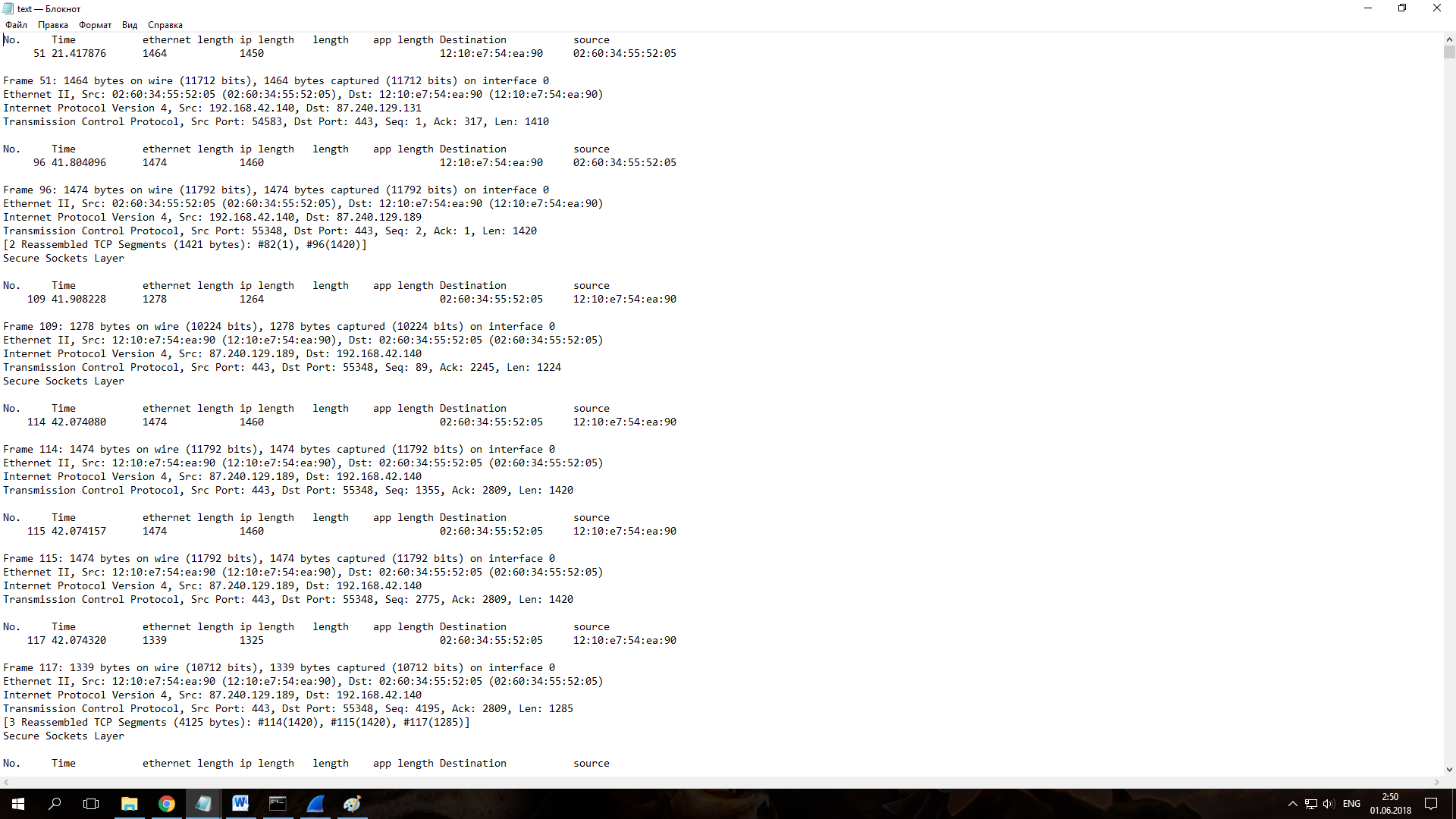
Таблица 2 – Фильтры отображения в wireshark

|  |  |  |
| --- | --- | --- |
| **№** | **Название фильтра** | **Фильтр в Wireshark** |
| 1 | Кадров Ethernet, отправляемых с сетевого интерфейса | eth.src == 70:1c:e7:f4:9d:bd |
| 2 | Кадров Ethernet, только принимаемых на сетевой интерфейс | eth.dst == 70:1c:e7:f4:9d:bd |
| 3 | Кадров Ethernet и отправляемых, и принимаемых сетевым интерфейсом | eth.src == 70:1c:e7:f4:9d:bd or eth.dst == 70:1c:e7:f4:9d:bd |
| 4 | Пакетов IP, только отправляемых с сетевого интерфейса | ip.src == 192.168.1.38 |
| 5 | Пакетов IP, только принимаемых на сетевой интерфейc | ip.dst == 192.168.1.38 |
| 6 | Пакетов IP и отправляемых, и принимаемых сетевым интерфейсом | ip.src == 192.168.1.38 or ip.dst == 192.168.1.38 |
| 7 | Сегментов TCP, только отправляемых с сетевого интерфейса – на порты 80, 443 (http, https) | (tcp.dstport == 80 || tcp.dstport == 443) && ip.src == 192.168.1.38 |
| 8 | Сегментов TCP, только принимаемых на сетевой интерфейс – с портов 80, 443 (http, https) | (tcp.srcport == 80 || tcp.srcport == 443) && ip.dst == 192.168.1.38 |
| 9 | Сегментов TCP и отправляемых, и принимаемых сетевым интерфейсом | (ip.dst == 192.168.1.38 || ip.dst == 192.168.1.38) && tcp |
| 10 | Датаграмм UDP, только отправляемых с сетевого интерфейса – на порт 53 (dns) | udp.dstport == 53 && ip.src == 192.168.1.38 |
| 11 | Датаграмм UDP, только принимаемых на сетевой интерфейс – с порта 53 (dns) | udp.srcport == 53 && ip.dst == 192.168.1.38 |
| 12 | Датаграмм UDP и отправляемых, и принимаемых сетевым интерфейсом | (ip.dst == 192.168.1.38 || ip.src == 192.168.1.38) && udp |
| 13 | Сообщений протокола arp | arp |
| 14 | Сообщений протокола icmp | icmp |
| 15 | Сообщений протокола dns | dns |
| 16 | Сообщений протокола http | http |



*Рис. 4. “Маркировка широковещательных кадров ethernet”* 

*Рис. 5. “Маркировка пакетов по размеру”* 

*Рис. 6. “Экспорт захвата в excel”* 

*Рис.7. “Экспорт захвата в txt”*

# Выводы

## Особенности процедуры анализа сетевого трафика

Данная процедура заключается в использовании фильтров, чтобы отображались необходимые пакеты, а также в отображении определенных столбцов, чтобы видеть только необходимые данные.

Для анализа используются сетевые и физические адреса, адреса портов (источник и получатель), длины кадров на разных уровнях и протоколы.

Результаты отображаются в виде таблицы, в которой обозначены искомые пакеты и поля информации об этих пакетах.

## Структура и функции программных инструментов анализа сетевого трафика

Программный инструмент анализа сетевого трафика имеет панель инструментов с кнопками и вкладками, предоставляющими доступ к его функциям, поле для ввода фильтра, таблицу в которой отражены выбранные пакеты, а также область внизу, в которой можно посмотреть более подробную информацию о конкретном пакете.

Функции: захват и остановка захвата трафика, использование фильтров, настройка отображения данных, сохранение и экспорт в файлы различных типов.

Start capturing packets - начать захват пакетов, которые в данный момент проходят через наш интерфейс.

Stop capturing packets - прекратить захват пакетов, которые в данный момент проходят через наш интерфейс.

Apply filter - отображает только те пакеты, которые удовлетворяют введенному нами фильтру.

Edit->Preferences->Columns - позволяет настроить столбцы, в которых будут отображаться данные о пакетах.

File->SaveAs - сохранение захваченных пакетов в какой-либо тип данных

File->ExportSpecifiedPackets - экспорт в специфические типы данных (txt, excel, csv и т.д.)