МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

“БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ”

**КАФЕДРА ИИТ**

ОТЧЁТ

по лабораторной работе №6

**«Анализ сетевого трафика и протоколов на базе WireShark»**

Выполнил:

Студент 2 курса

группы ПО-9

Харитонович Захар Сергеевич

Проверил:

Савицкий Ю. В.

Брест 2023

**Вариант 1**

**Цель работы:** приобретение навыков анализа сетевого трафика компьютерных сетей; изучение структуры сетевых протоколов различных уровней.

**Ход работы**

1. Изучить краткие теоретические сведения по возможностям, приемам работы с программой Wireshark (файл netWS.pdf).

2. Изучить: типы фильтрации трафика, правила построения фильтров, приемы статистической обработки сетевого трафика в Wireshark.

3. Запустив Wireshark на захват, выполнить загрузку страницы <https://www.google.ru>

4. Остановить и сохранить захват. Для захваченных пакетов определить статистические данные:

• процентное соотношение трафика разных протоколов в сети;

UDP – 97.73% пакетов

DNS – 2.27% пакетов

• среднюю скорость - 59.964 пакетов/сек;

• среднюю скорость – 34243.594 байт/сек;

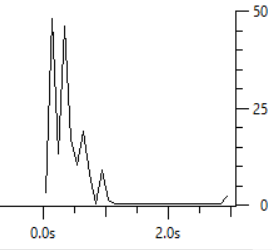
• минимальный, максимальный и средний размеры пакета;

минимальный – 24 байта

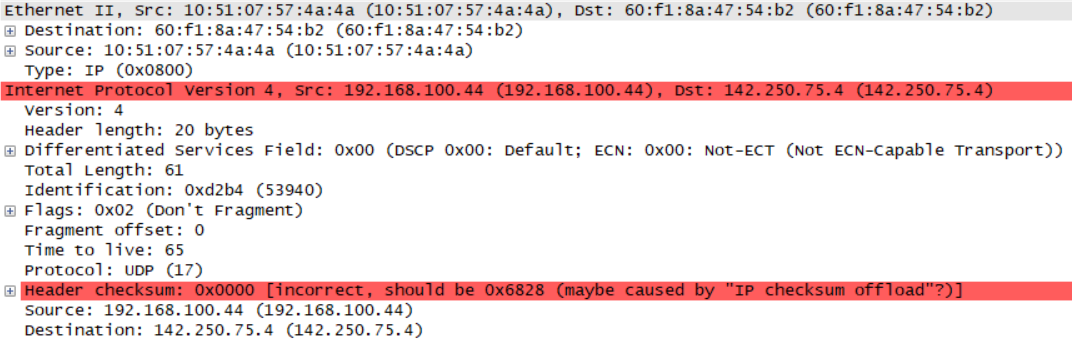
максимальный – 1357 байт

средний – 571.068 байт

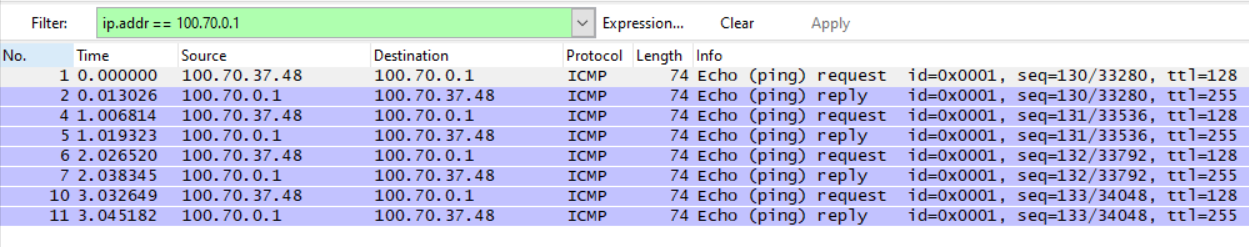
• степень использования полосы пропускания канала (загрузку сети)



5. На примере третьего захваченного IP-пакета указать структуры протокола канального уровня (протокола Ethernet 802.3, Wi-Fi 802.11, либо другого, используемого в вашей конфигурации) и протокола IPv4.

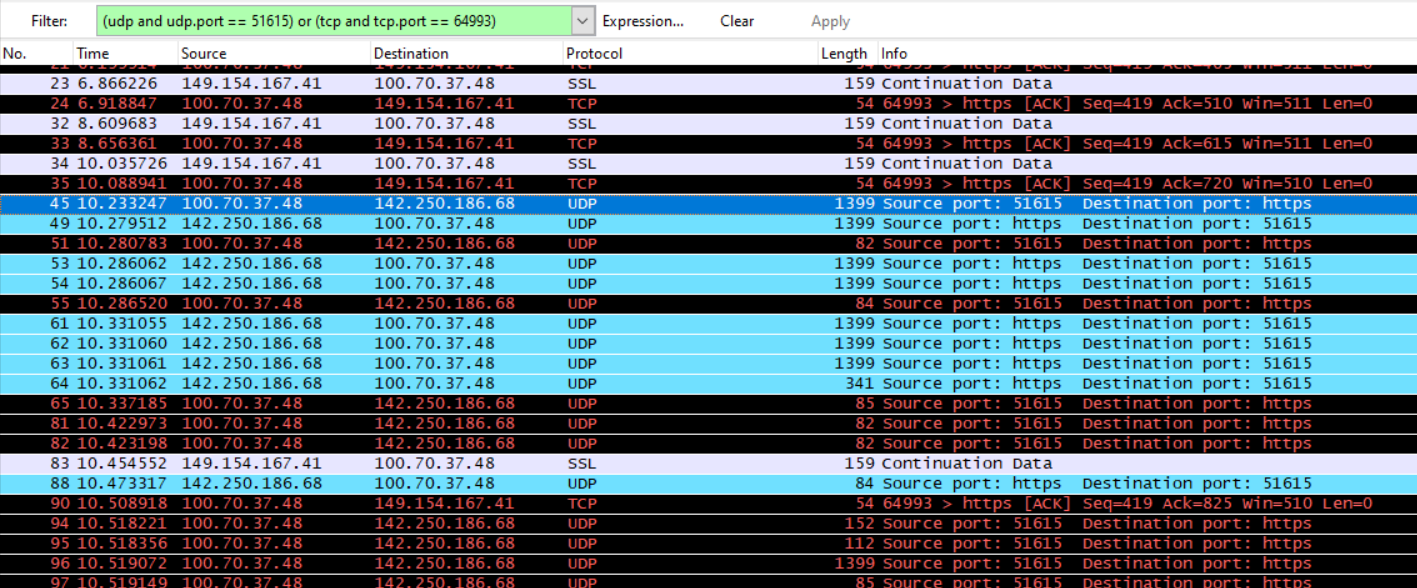


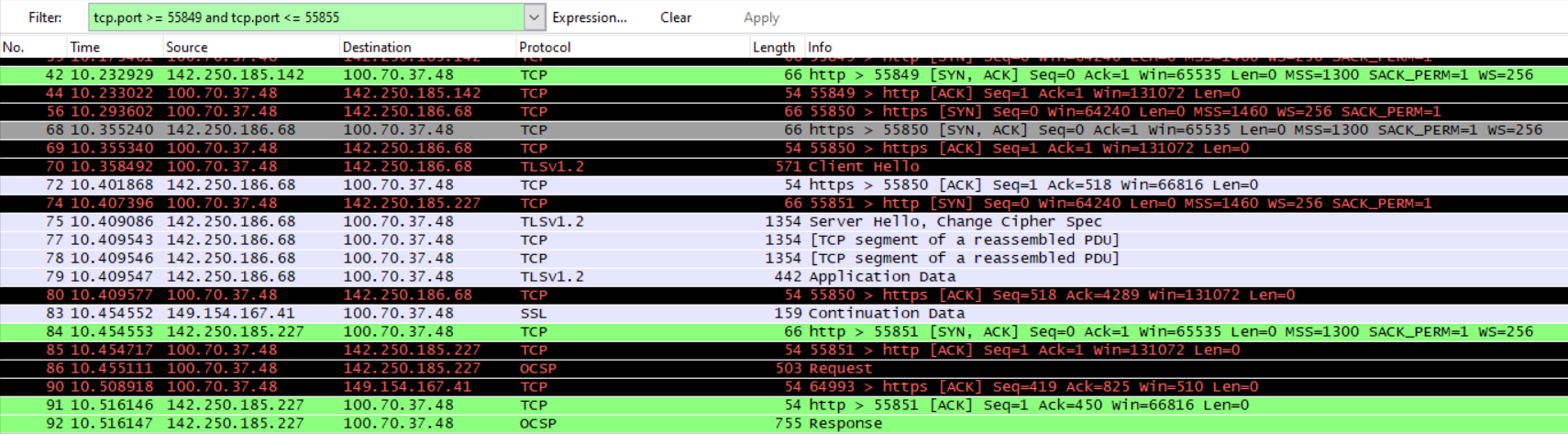
6. Запустив Wireshark на захват, выполнить команду ping для IP адреса компьютера. Сохранить результат. Сформировав нужный фильтр, отфильтровать пакеты, относящиеся к выполнению команды ping.



7. Сформировать не менее 3-х сложных фильтров захвата с использованием полей протоколов, операторов сравнения (таблицы 1 и 2 из файла netWS.pdf) и логических операторов; каждый раз перезапуская захват, для каждого фильтра захватить соответствующие пакеты.

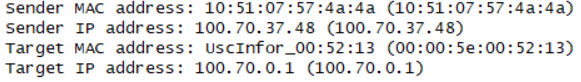




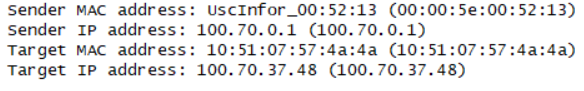


8. Выполнить анализ ARP-протокола по примеру из методических указаний.

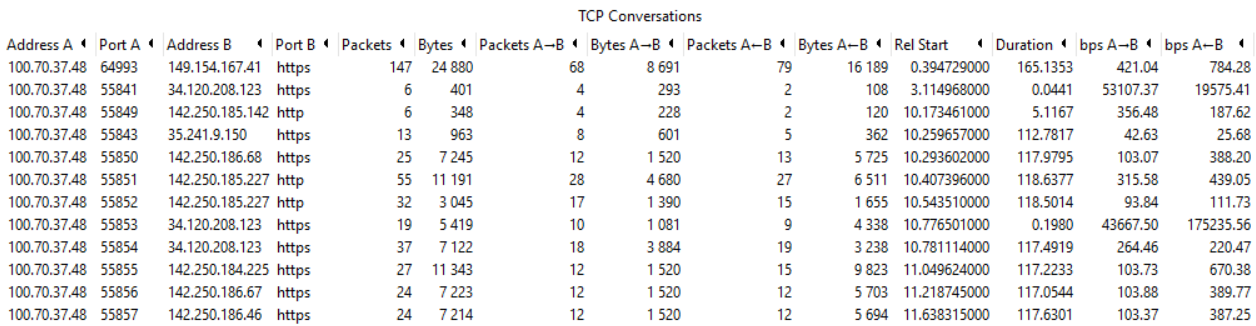
Запрос



Ответ



9. Выполнить анализ TCP-сеансов по примеру из методических указаний



**Вывод:** приобретены навыки анализа сетевого трафика компьютерных сетей; изучены структуры сетевых протоколов различных уровней.