Министерство образования Республики Беларусь

Учреждение образования

«Брестский государственный технический университет»

Кафедра ИИТ

Лабораторная работа №6

По дисциплине: «КСиС»

Тема: «Анализ сетевого трафика и протоколов на базе WIRESHARK»

Выполнил:

Студент 2 курса

Группы ПО-6

Осьмушников А.Ю.

Проверил:

Бойко М. О

Брест, 2022

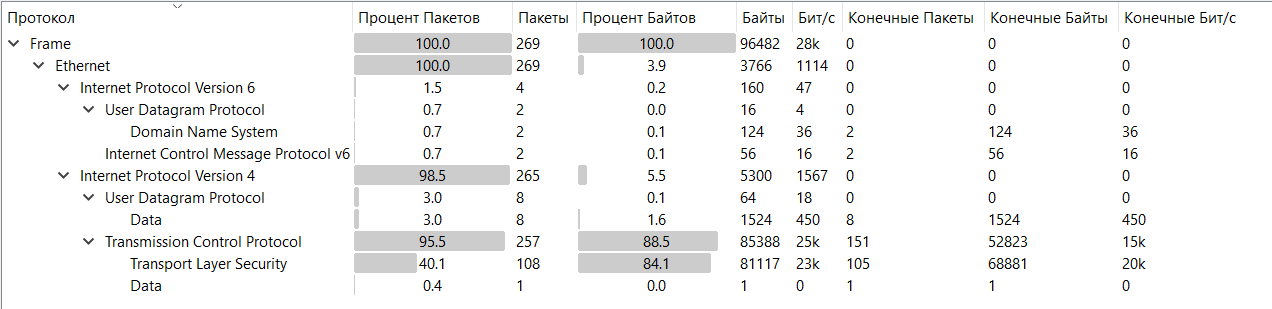
Лабораторная работа №6

Анализ сетевого трафика и протоколов на базе WIRESHARK

**Цель работы:** изучить типы фильтрации трафика, правила построения фильтров, приемы статистической обработки сетевого трафика в Wireshark.

**Задание:**

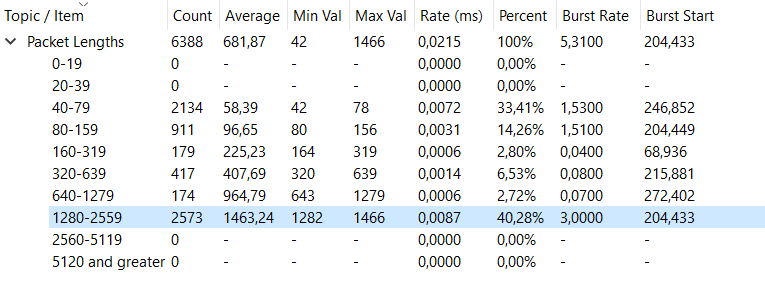
1. Изучить краткие теоретические сведения по возможностям, приемам работы с программой Wireshark.
2. Изучить: типы фильтрации трафика, правила построения фильтров, приемы статистической обработки сетевого трафика в Wireshark (материал приведен ниже).
3. Запустив Wireshark на захват, выполнить загрузку доступной в лабораторных условиях страницы (bstu.by, iit.bstu.by или др.). Остановить и сохранить захват. Для захваченных пакетов определить статистические данные:
   1. процентное соотношение трафика разных протоколов в сети;



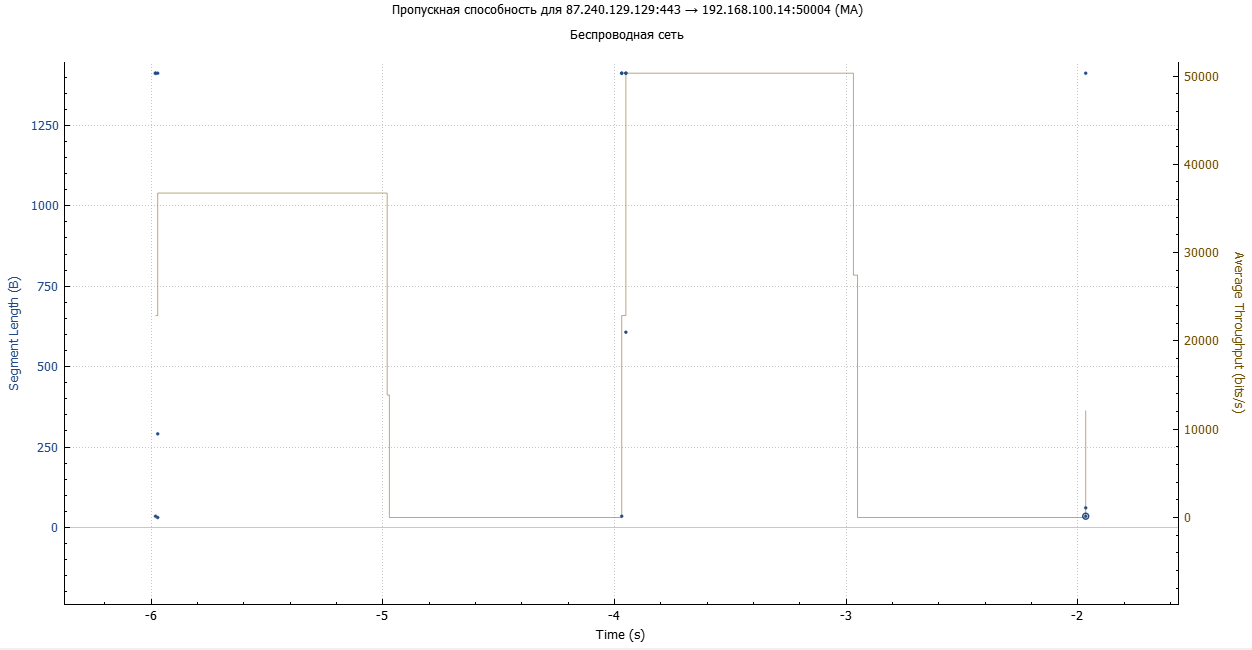
* 1. среднюю скорость кадров/сек и среднюю скорость байт/сек;



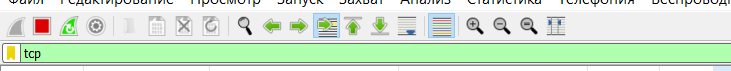
* 1. минимальный, максимальный и средний размеры пакета;

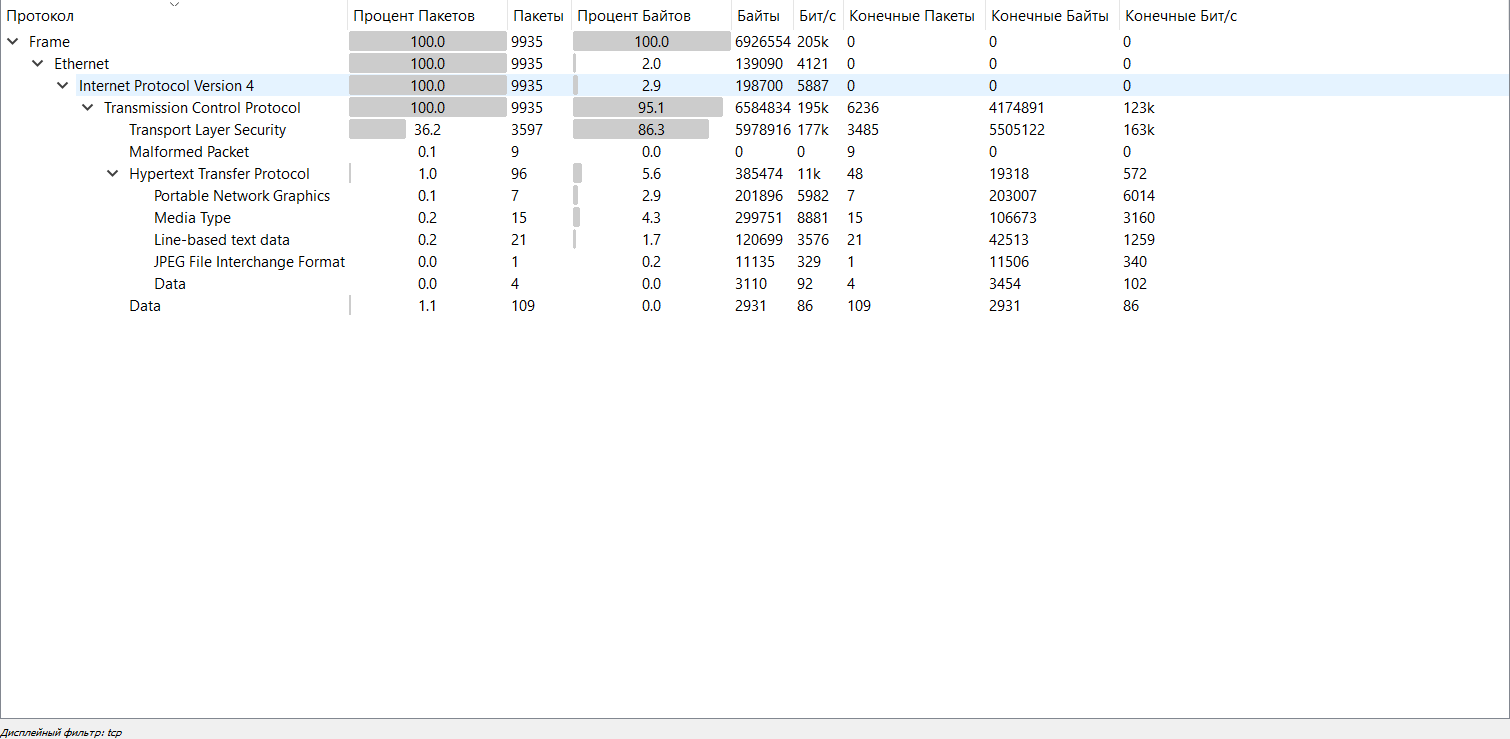


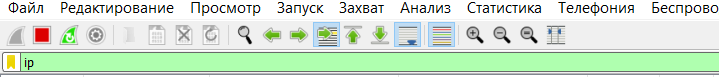
* 1. степень использования полосы пропускания канала (загрузку сети);

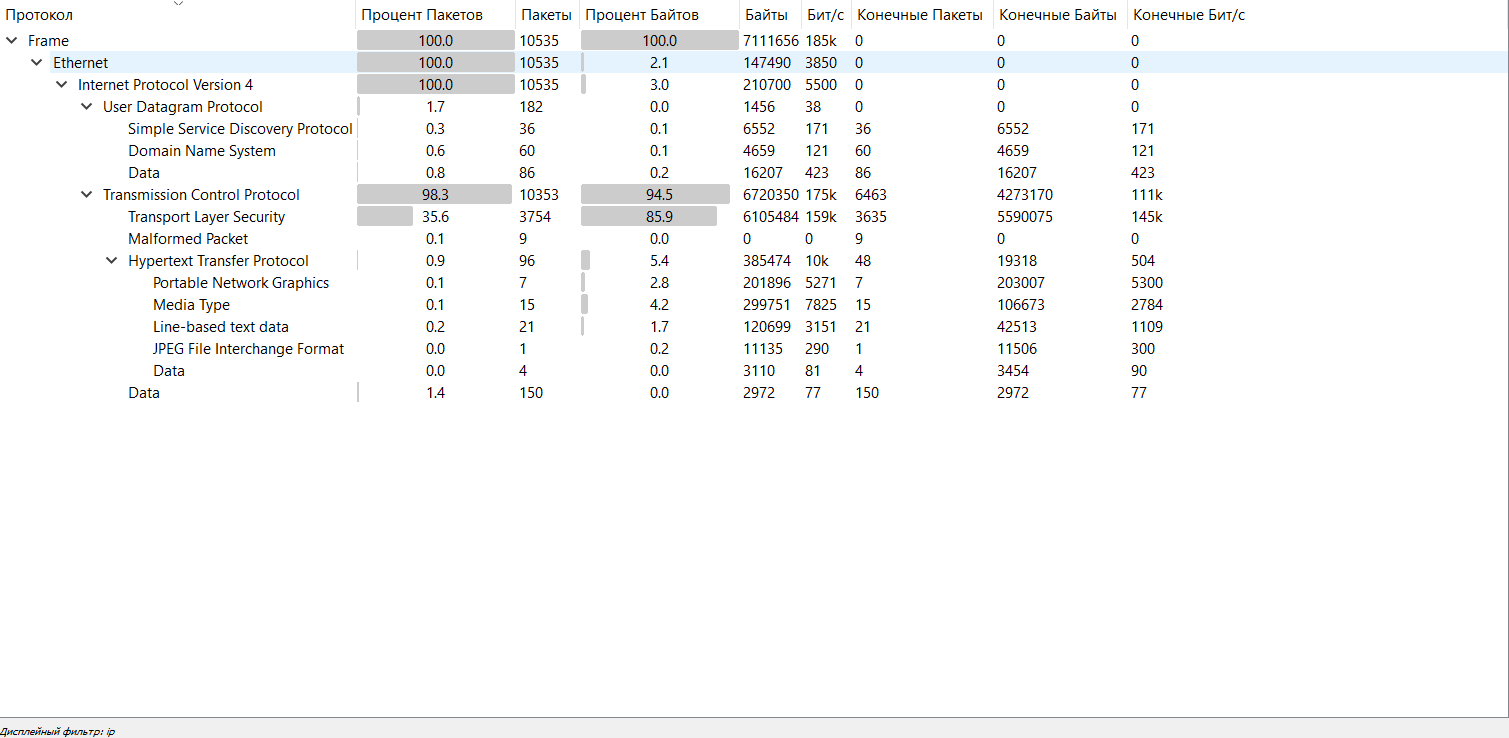


1. Отфильтровать в захвате IP пакеты. Определить статистические данные:
   1. процентное соотношение трафика разных протоколов стека tcp/ip в сети;

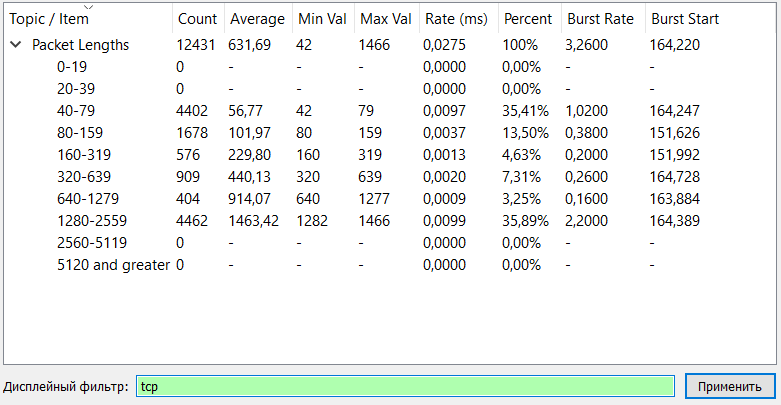


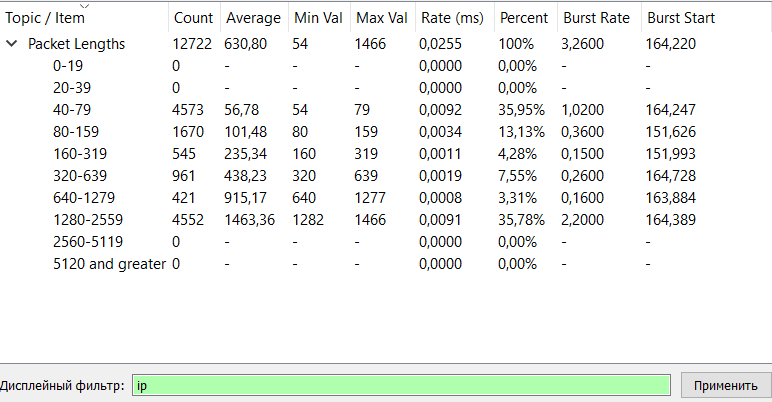






* 1. средний, минимальный, максимальный размеры пакета;



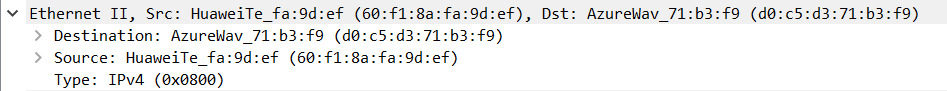


На примере любого IP-пакета указать структуры протоколов Ethernet и IP.

Отметить поля заголовков и описать их и интерпретировать их значения.

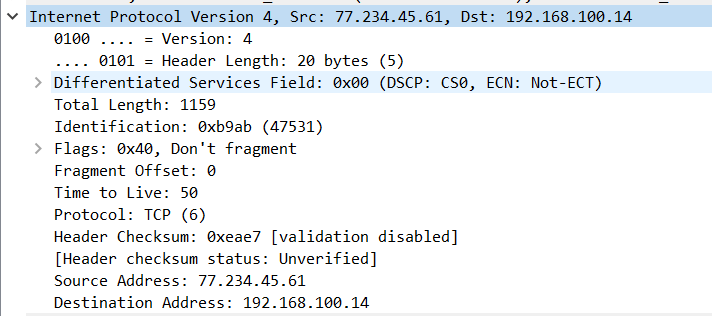
* Структура протокола Ethernet





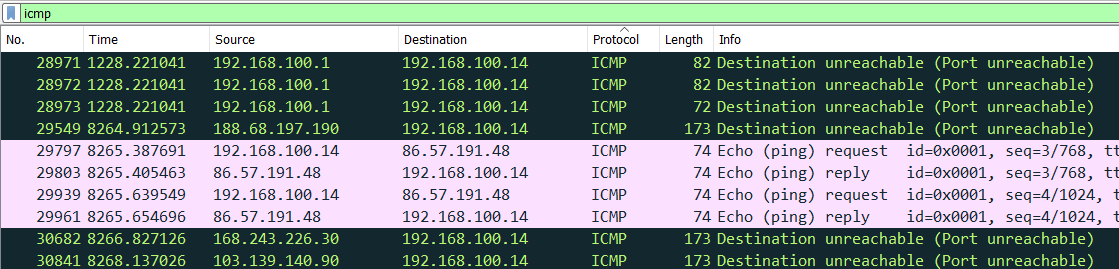
|  |
| --- |
| *Ethernet II* - Это кадр протокола Ethernet. |
| *Source: HuaweiTe\_fa:9d:ef (60:f1:8a:fa:9d:ef)* - Физический адрес устройства отправителя,  (60:f1:8a:fa:9d:ef), производитель сетевой карты – компания Huawei |
| *Destination: AzureWav\_71:b3:f9 (d0:c5:d3:71:b3:f9)* – Физический адрес устройства получателя AzureWav\_71:b3:f9, DNS имя устройства - d0:c5:d3:71:b3:f9 |
| *Type: IPv4 (0x0800)* – На сетевом уровне используется протокол IPv4. |

* Структура протокола IP

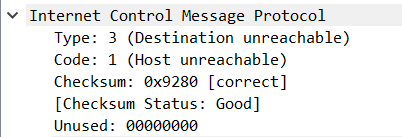


|  |
| --- |
| *Internet Protocol Version 4* - Это пакет протокола IPv4. |
| *Src: 77.234.45.61 (77.234.45.61)* - Сетевой адрес устройства отправителя 77.234.45.61, DNS имя устройства отправителя 77.234.45.61. |
| *Dst: (192.168.100.14)* – Сетевой адрес устройства получателя, 192.168.100.14. |
| *Time to live: 50* – Максимально возможное количество сетевых устройств, которые могут обработать и передать пакет дальше по сети. |
| *Protocol: TCP (6)* – На транспортном уровне используется протокол TCP. Значение, этого поля позволяет устройству определить, какому протоколу транспортного уровня следует дальше передать полученное PDU. |

1. Запустив Wireshark на захват, выполнить команду ping для IP адреса соседней рабочей станции в лаборатории (предварительно определив ее адрес с помощью ipconfig). Сохранить результат. Сформировав нужный фильтр, отфильтровать пакеты, относящиеся к выполнению команды ping. На базе полученных пакетов и значений их полей интерпретировать результат работы утилиты ping. Описать все протоколы, используемые утилитой. Составить диаграмму взаимодействия машин при работе утилиты *ping*. Примечание. Данная утилита использует протокол ICMP (RFC 792 и RFC 960).
   1. Фильтр перехваченных пакетов:



* 1. Интерпретация основных полей протокола ICMP:



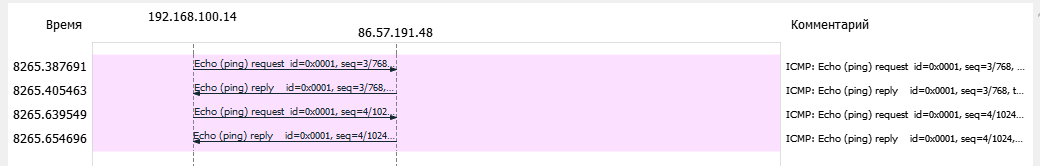
*Type: 3 (Destination unreachable)* - тип сообщения ICMP.

Code отражает причину отправки сообщения (1 - хост не достижим);3 –запрос , 1 – ответ.

*Checksum: 0x9280 [correct]* - контрольная сумма, вычисляется из части ICMP пакета.

*Data (103 bytes)* – поле данных.

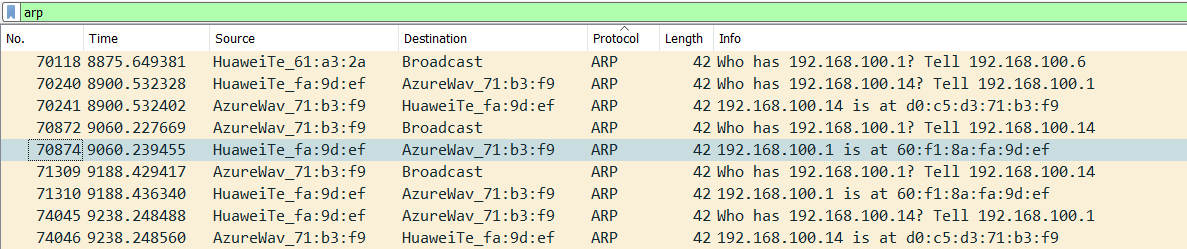
* 1. Диаграмма взаимодействия:



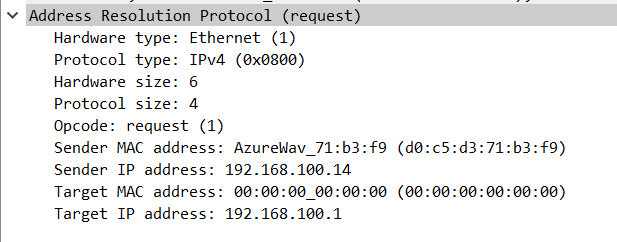
1. Выполнить анализ ARP-протокола по примеру из методических указаний.

Для успешного эксперимента предварительно очистим arp-кэш командой:

arp -d 192.168.1.5

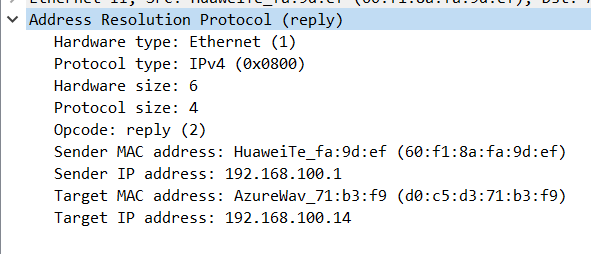


ARP-запрос:



Sender MAC address:  – MAC-адрес отправителя.  
Sender IP address: 192.168.100.14 (192.168.100.14) – IP-адрес отправителя.  
Target MAC address:  – MAC-адрес получателя.  
Target IP address: 192.168.100.1 (192.168.100.1) – IP-адрес получателя.

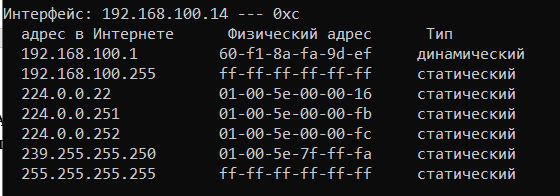
ARP-ответ:



Sender MAC address:  - целевое поле MAC-адреса получателя.  
Sender IP address: 192.168.100.1 (192.168.100.1) – IP-адрес получателя  
Target MAC address: - MAC-адрес исходного отправителя.  
Target IP address: 192.168.100.128 (192.168.100.128) - IP-адрес исходного отправителя.

Просмотрим ARP-кэш и сверим данные в нем с данными, которые мы узнали из анализа пакетов ARP-запрос/ответа:





**Вывод:** изучили типы фильтрации трафика, правила построения фильтров, приемы статистической обработки сетевого трафика в Wireshark.