Министерство образования Республики Беларусь

Учреждение образования

«Брестский государственный технический университет»

Кафедра ИИТ

Лабораторная работа №6

за 4 семестр

По дисциплине: «КСиС»

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

Выполнил:

Студент 1 курса

Группы ПО-6(1)

Лавренчик Д.О.

Проверил:

Бойко Д.О.

2022

Лабораторная работа №6

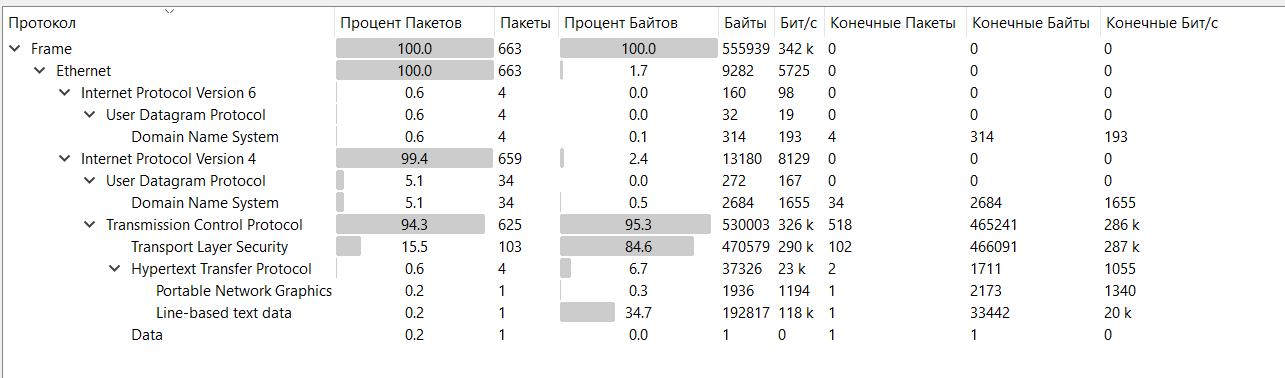
Анализ сетевого трафика и протоколов на базе WIRESHARK

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

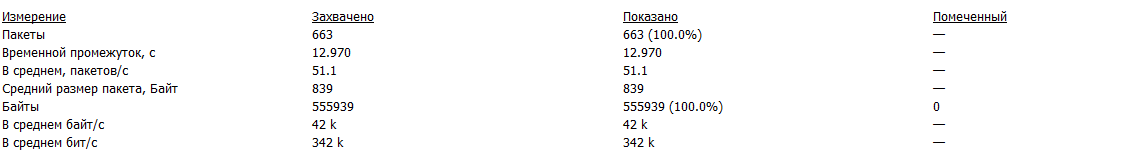
**Задание:**

1. Изучить краткие теоретические сведения по возможностям, приемам работы с программой Wireshark (файл [netWS.pdf](about:blank)).
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:

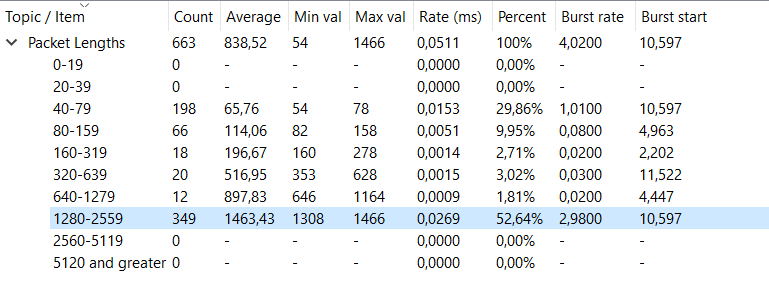
* процентное соотношение трафика разных протоколов в сети;



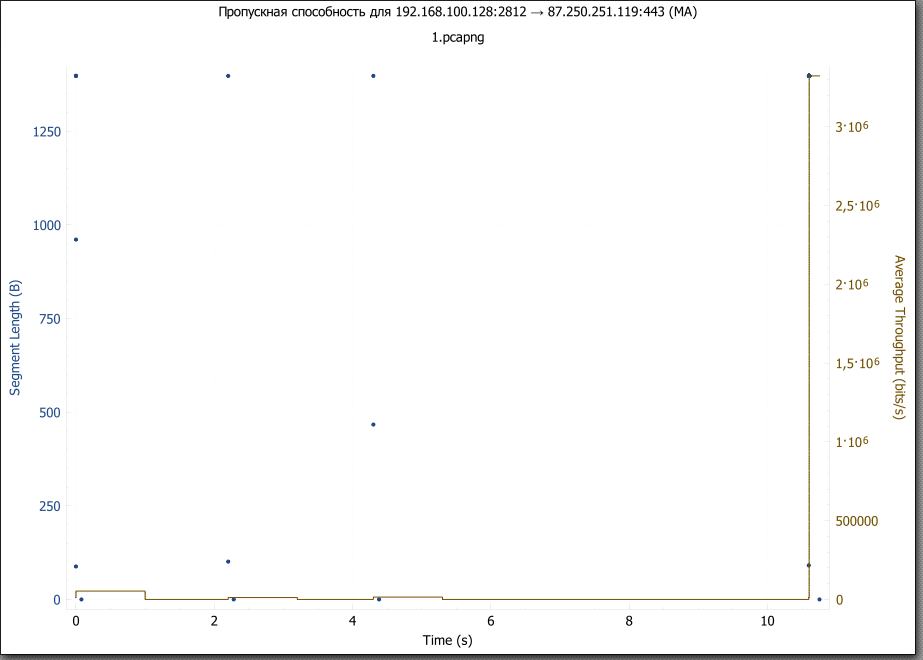
* среднюю скорость кадров/сек;
* среднюю скорость байт/сек;



* минимальный, максимальный и средний размеры пакета;

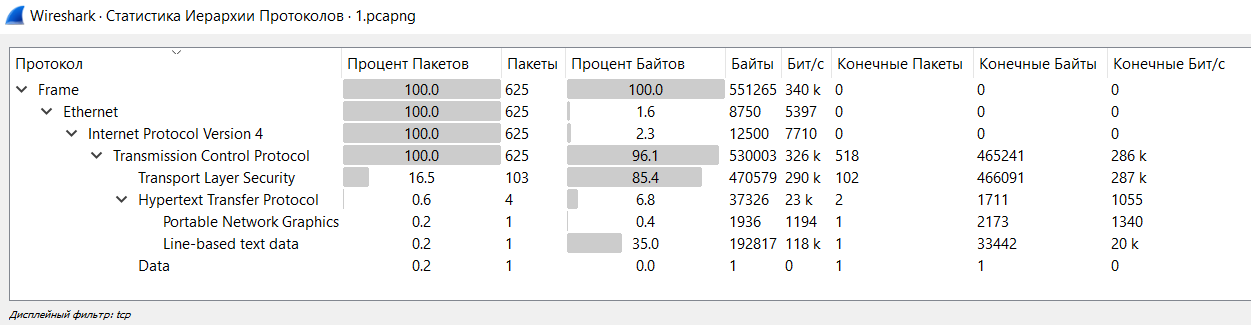


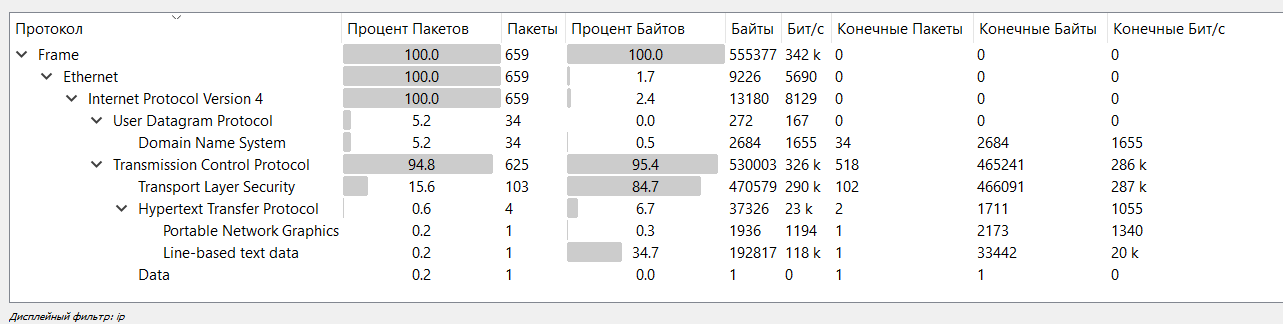
* степень использования полосы пропускания канала (загрузку сети).



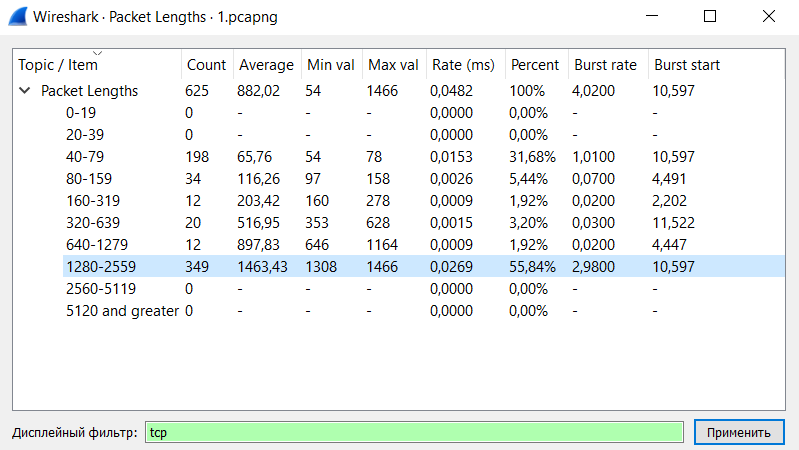
1. Отфильтровать в захвате IP пакеты. Определить статистические данные:

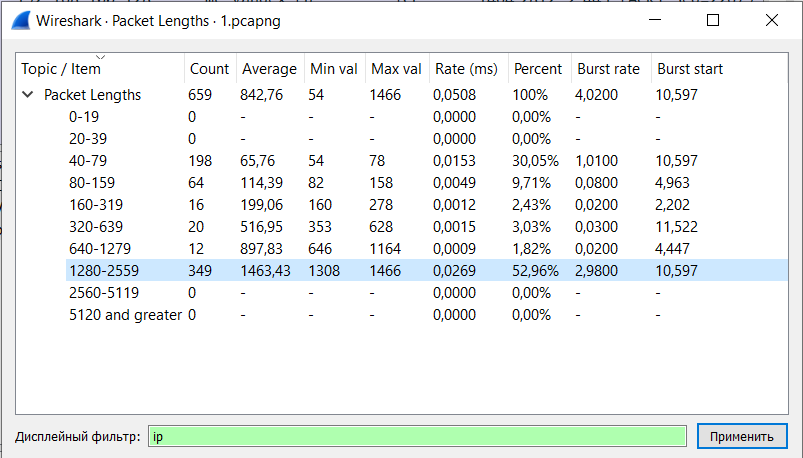
* процентное соотношение трафика разных протоколов стека tcp/ip в сети;





* средний, минимальный, максимальный размеры пакета.

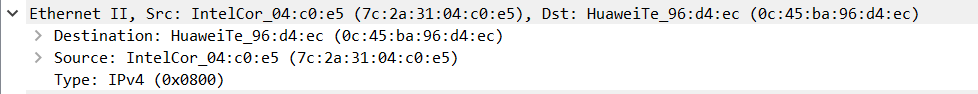


**

*На примере любого IP-пакета указать структуры протоколов Ethernet и IP. Отметить поля заголовков и описать их и интерпретировать их значения.*

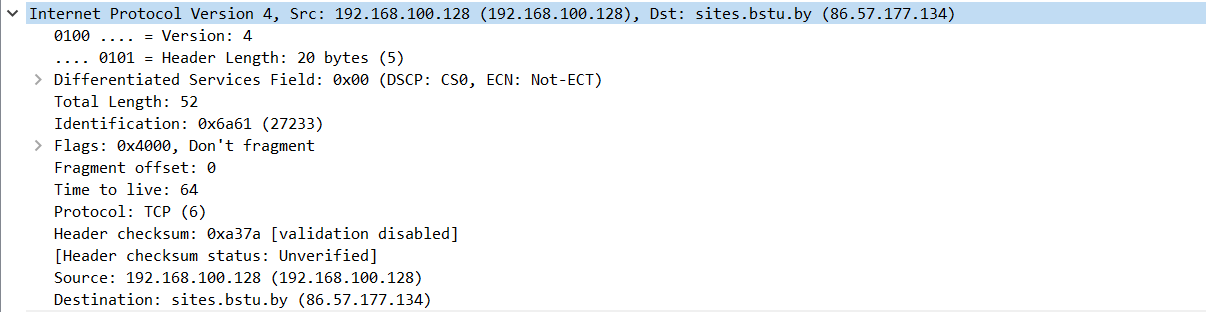


Структура протокола Ethernet



|  |
| --- |
| Ethernet II, - Это кадр протокола Ethernet. |
| Source: IntelCor\_04:c0:e5(7c:2a:31:04:c0:e5) - Физический адрес устройства отправителя,  7c:2a:31:04:c0:e5, производитель сетевой карты – компания Intel |
| Destination: HuaweiTe\_96:d4:ec (0c:45:ba:96:d4:ec) – Физический адрес устройства получателя HuaweiTe\_96:d4:ec, DNS имя устройства - 0c:45:ba:96:d4:ec |
| Type: IP (0x0800) – На сетевом уровне используется протокол IPv4. |

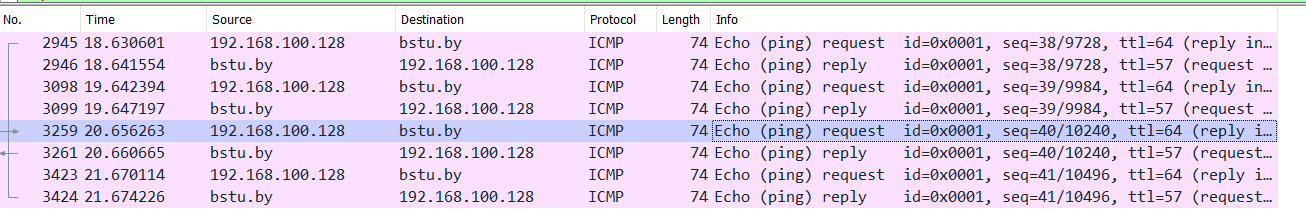
Структура протокола IP



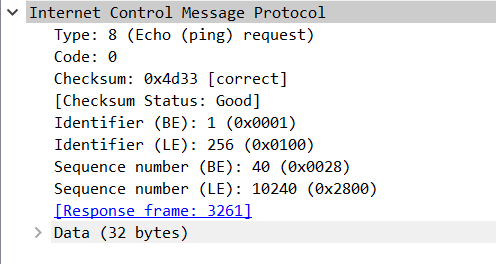
|  |
| --- |
| Internet Protocol Version 4 - Это пакет протокола IPv4. |
| Src: 192.168.100.128 (192.168.100.128) - Сетевой адрес устройства отправителя 192.168.100.128, DNS имя устройства отправителя 192.168.100.128. |
| Dst: sites.bstu.by(86.57.177.134) – Сетевой адрес устройства получателя, 86.57.177.134. |
| Time to live: 64 – Максимально возможное количество сетевых устройств, которые могут обработать и передать пакет дальше по сети равняется 64. |
| Protocol: TCP (6) – На транспортном уровне используется протокол TCP. Значение, этого поля позволяет устройству определить, какому протоколу транспортного уровня следует дальше передать полученное PDU. В данном случае – это протокол TCP. |

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).

Отфильтруем перехваченные пакеты:



Интерпретируем основные поля протокола ICMP:



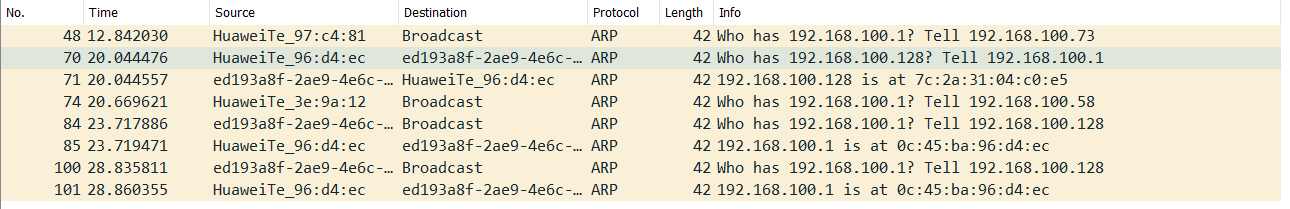
|  |
| --- |
| Type: 0 (Echo (ping) request)  - тип сообщения ICMP.  8 - Эхо-запрос (Echo Request), 0 - Эхо-ответ (Echo Replay). |
| Checksum: 0x4d33 [correct] - контрольная сумма, вычисляется из части ICMP пакета. |
| Data (32 bytes) – поле данных. |

Диаграмма взаимодействия:

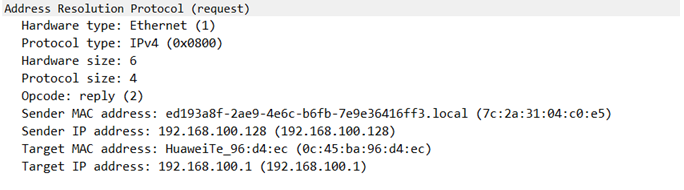


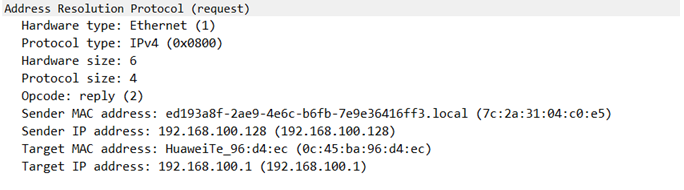
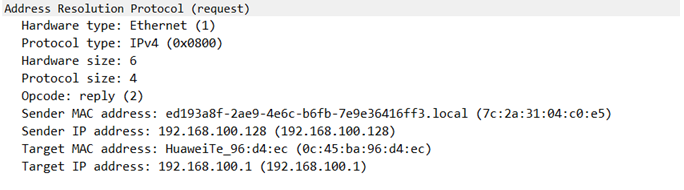
1. Выполнить анализ ARP-протокола по примеру из методических указаний.

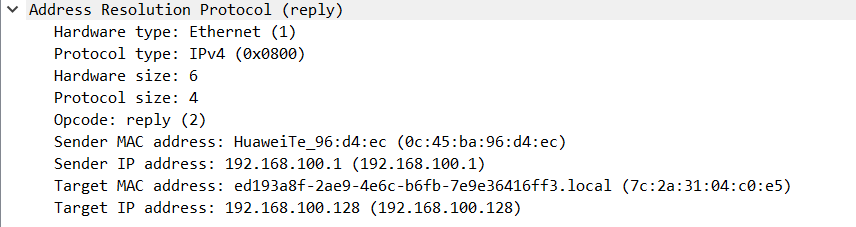
Очистим arp-кэш командой:  
arp –d 192.168.100.128  
Фильтр захвата будет иметь следующий вид:  
arp

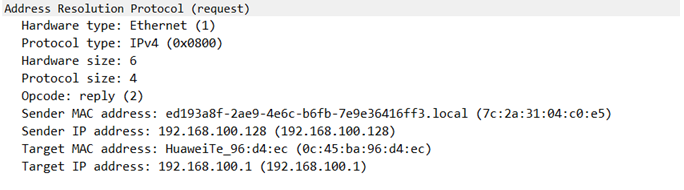
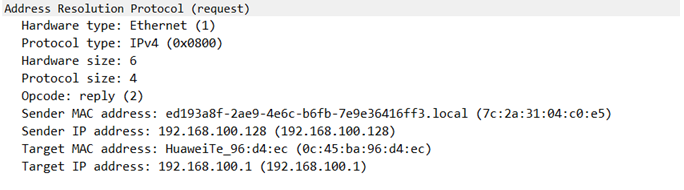


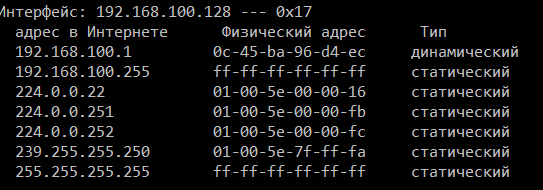
Рассмотрим ARP-запрос:



Sender MAC address:  – MAC-адрес отправителя.  
Sender IP address: 192.168.100.128 (192.168.100.128) – IP-адрес отправителя.  
Target MAC address: – MAC-адрес получателя.  
Target IP address: 192.168.100.1 (192.168.100.1) – IP-адрес получателя.  
Рассмотрим 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: изучил типы фильтрации трафика, правила построения фильтров, приемы статистической обработки сетевого трафика в Wireshark.