Министерство образования Республики Беларусь

Учреждение образования

«Брестский государственный технический университет»

Кафедра ИИТ

Лабораторная работа №6

за 4 семестр

По дисциплине: «КCиС»

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

Выполнила:

Студентка 2 курса

Группы ПО-6 (2)

Данилюк Д. Б.

Проверил:

Бойко Д.О.

Брест, 2022

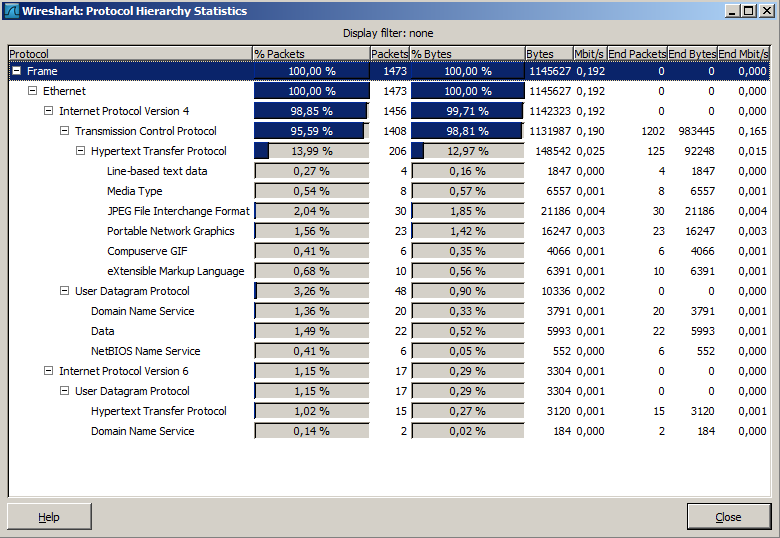
Лабораторная работа №6

Анализ сетевого трафика и протоколов на базе WIRESHARK

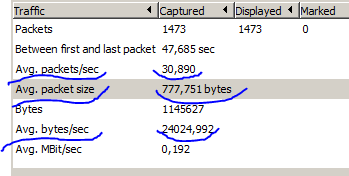
**Задание на лабораторную работу:**

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;

Минимальный

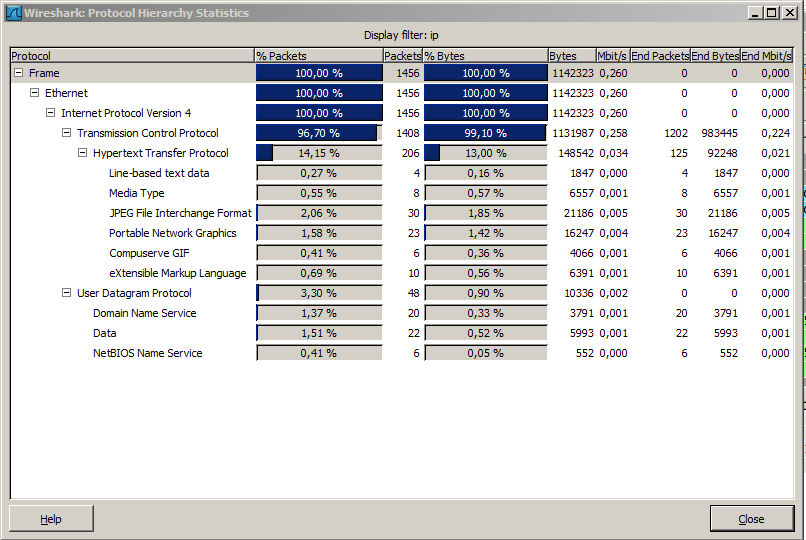


Максимальный



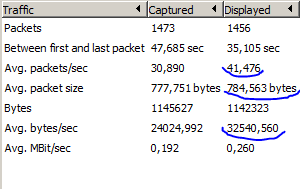
1. Отфильтровать в захвате IP пакеты. Определить статистические данные:

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



* средний, минимальный, максимальный размеры пакета.

Средняя скорость кадров/сек и средняя скорость байт/сек, средний размер пакета:



Минимальный:  
Максимальный:

Возьмём следующий пакет:

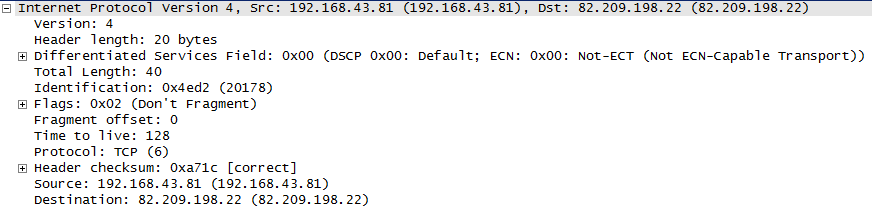


Структура протокола Ethernet



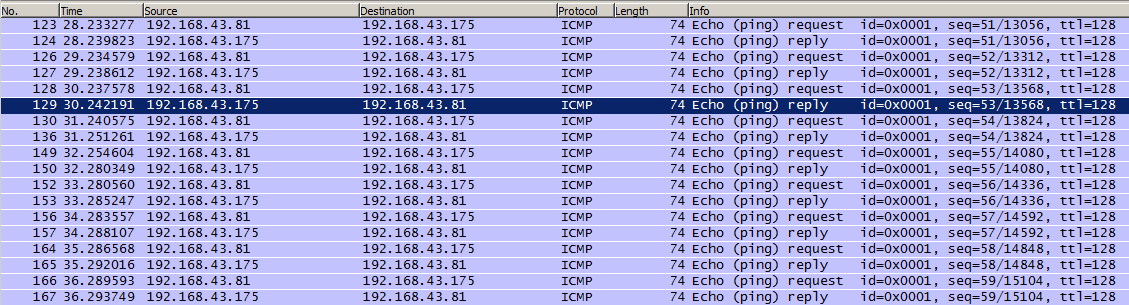
|  |
| --- |
| Ethernet II, - Это кадр протокола Ethernet. |
| Source: Apple\_7e:8f:da (58:b0:35:7e:8f:da) - Физический адрес устройства отправителя,  58:b0:35:7e:8f:da, производитель сетевой карты – компания Apple |
| Destination: 42:c6:2a:30:32:7a (42:c6:2a:30:32:7a) – Физический адрес устройства получателя 42:c6:2a:30:32:7a, DNS имя устройства - 42:c6:2a:30:32:7a |
| Type: IP (0x0800) – На сетевом уровне используется протокол IPv4. |

Структура протокола IP



|  |
| --- |
| Internet Protocol Version 4 - Это пакет протокола IPv4. |
| Src: 192.168.43.81 (192.168.43.81) - Сетевой адрес устройства отправителя 192.168.43.134, DNS имя устройства отправителя 192.168.43.134. |
| Dst: 82.209.198.19(82.209.198.22) – Сетевой адрес устройства получателя, 82.209.198.22. |
| Time to live: 128 – Максимально возможное количество сетевых устройств, которые могут обработать и передать пакет дальше по сети равняется 128. |
| 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. |

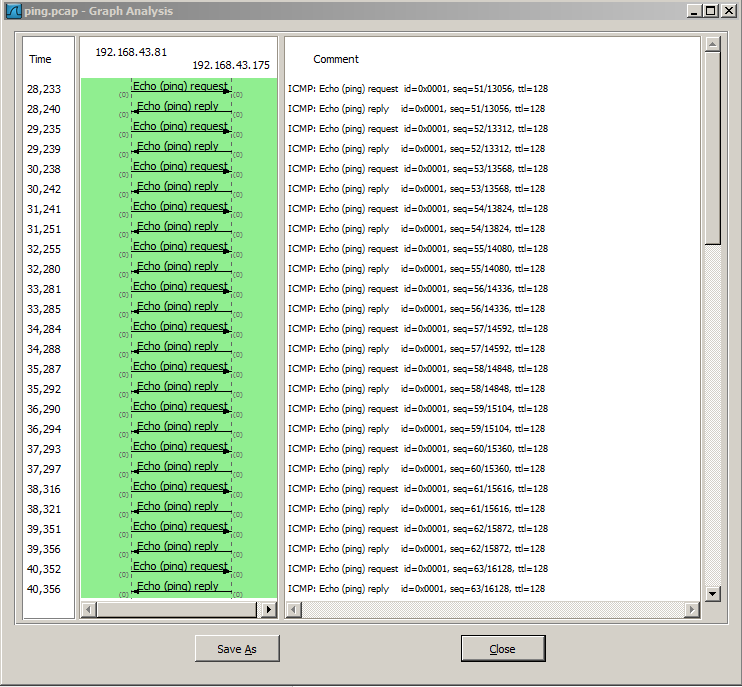
1. Запустив Wireshark на захват, выполнить команду ping для IP адреса соседней рабочей станции.

Отфильтруем перехваченные пакеты:

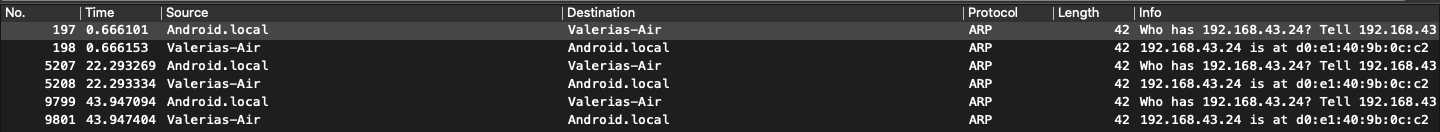
Интерпретируем основные поля протокола ICMP:

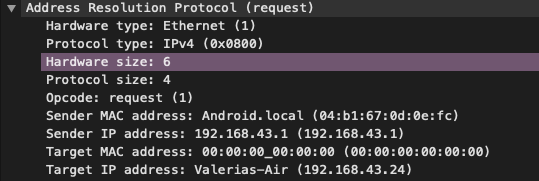
|  |
| --- |
| Type: 0 (Echo (ping) request)  - тип сообщения ICMP.  8 - Эхо-запрос (Echo Request), 0 - Эхо-ответ (Echo Replay). |
| Checksum: 0x5522 [correct] - контрольная сумма, вычисляется из части ICMP пакета. |
| Response time: 4,550 ms - время отклика. |
| Data (32 bytes) – поле данных. |

Диаграмма взаимодействия



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

Очистим arp-кэш командой:  
arp –d 192.168.43.195   
Фильтр захвата будет иметь следующий вид:  
arp   
Обратимся к другой машине, пропинговав ее. Получим следующий результат.

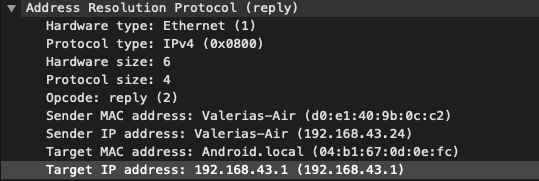
Рассмотрим ARP-запрос:

Sender MAC address: Apple\_7e (58:b0:35:7e:8f:da) – MAC-адрес отправителя.

Sender IP address: 192.168.43.81 (192.168.43.81) – IP-адрес отправителя.

Target MAC address: HonHaiPr\_d2:90:45 (c0:14:3d:d2:90:45) – MAC-адрес получателя.

Target IP address: 192.168.43.195 (192.168.43.195) – IP-адрес получателя.  
Рассмотрим ARP-ответ:



Sender MAC address: HonHaiPr\_d2:90:45 (c0:14:3d:d2:90:45) - целевое поле MAC-адреса получателя.

Sender IP address: 192.168.43.195 (192.168.43.195) – IP-адрес получателя

Target MAC address: Apple\_7e (58:b0:35:7e:8f:da) - MAC-адрес исходного отправителя.

Target IP address: 192.168.43.81 (192.168.43.81) - IP-адрес исходного отправителя.

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

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

Вывод: научились выполнять анализ сетевого трафика.