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 2 курса

Группы ПО-4(1)

Иваненко И. Л.

Проверил:

Савицкий Ю. В.

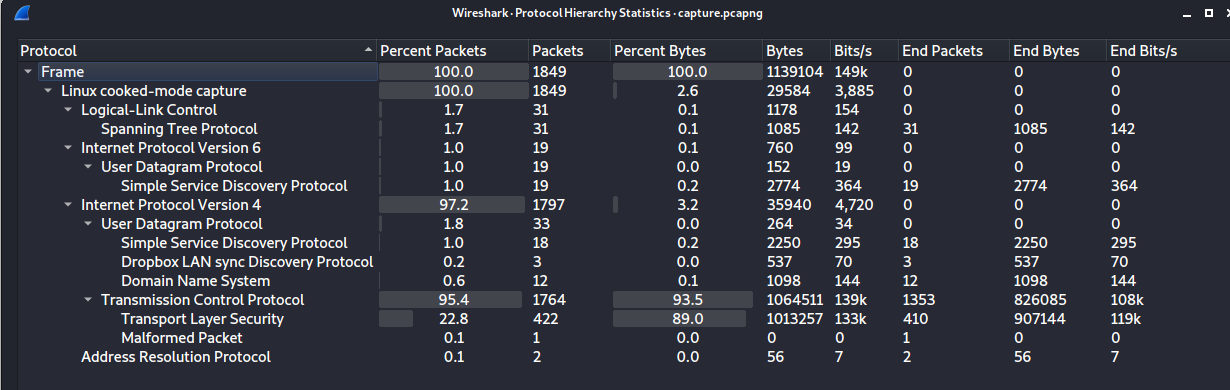
2021

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:

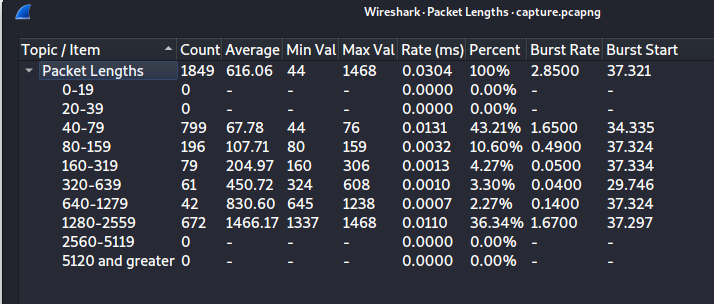
1) процентное соотношение трафика разных протоколов в сети;

2) среднюю скорость кадров/сек;

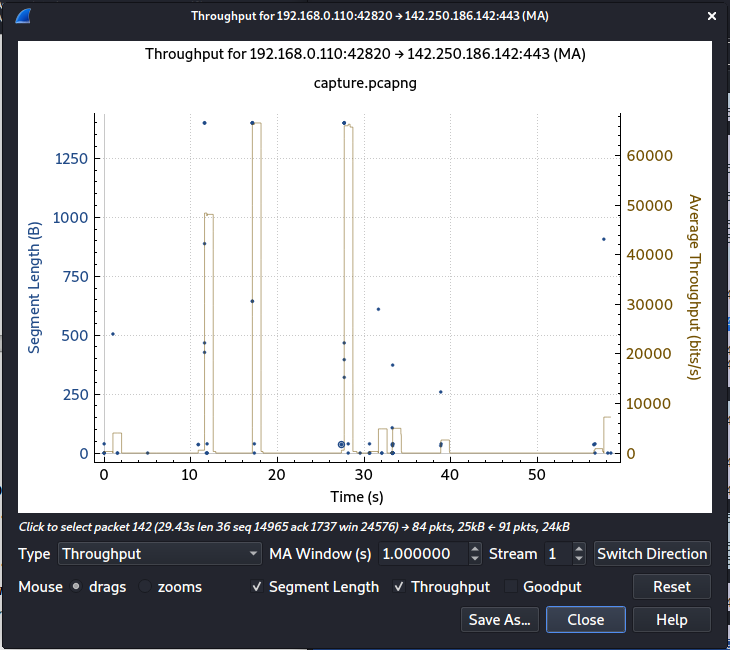
3) среднюю скорость байт/сек;



4) минимальный, максимальный и средний размеры пакета;



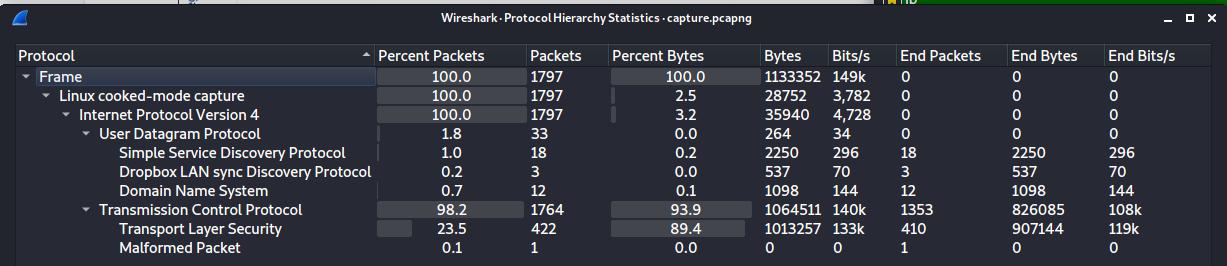
5) степень использования полосы пропускания канала (загрузку сети).

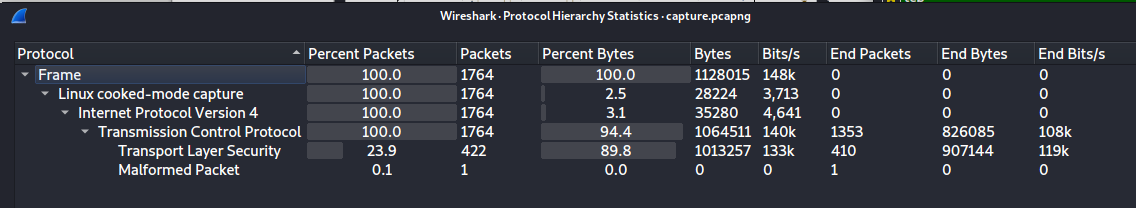


4.Отфильтровать в захвате IP пакеты. Определить статистические данные:

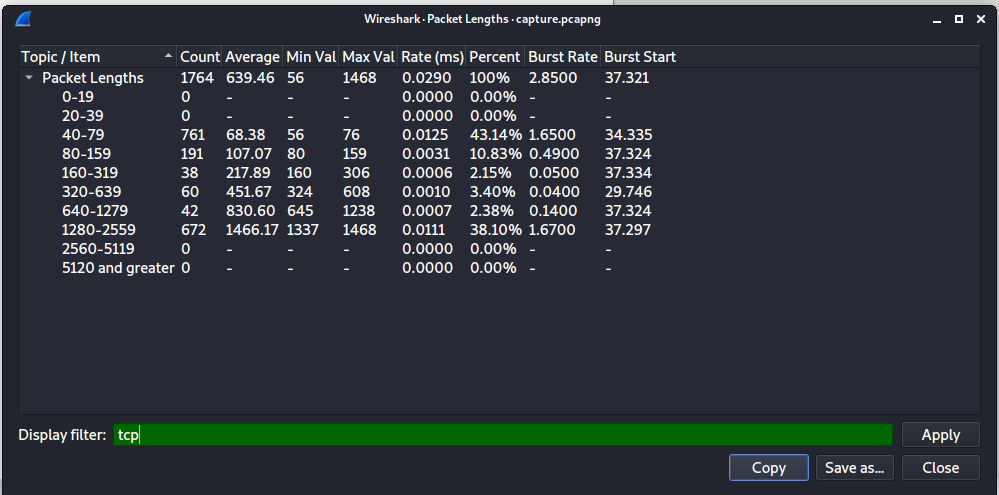
1) процентное соотношение трафика разных протоколов стека tcp/ip в сети;

ip filter

 tcp filter

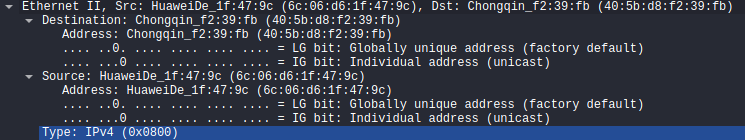


2) средний, минимальный, максимальный размеры пакета.



**

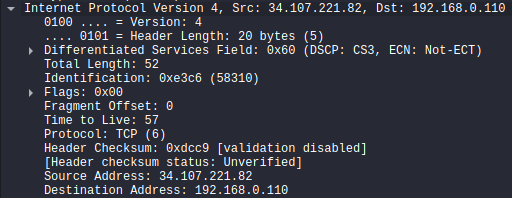
*На примере любого IP-пакета указать структуры протоколов Ethernet и IP. Отметить поля заголовков и описать их и интерпретировать их значения.*

Ethernet II — кадр протокола Ethernet.

Destination: Chongqin\_f2:39:fb (40:5b:d8:f2:39:fb) — физический адрес устройства-получателя , 40:5b:d8:f2:39:fb — MAC адрес

Source: HuaweiDe\_1f:47:9c (6c:06:d6:1f:47:9c) — физический адрес устройства-отправителя, 6c:06:d6:1f:47:9c — MAC адрес.

Type: IPv4 — на сетевом уровне используется протокол Ipv4



Src — сетевой адрес устройства-отправителя

Dst — сетевой адрес устройства-получателя

Differentiatd Services Field — Задается класс обслуживания, а также уведомления о перегрузке.

Total Length — длина всей дейтаграммы.

Identification — позволяет хосту-получателю определить, какому пакету принадлежат полученные им фраменты.

Flags — резервный бит, MF, DF.

Fragment Offset — положение пакета фрагмениа в исходном пакете.

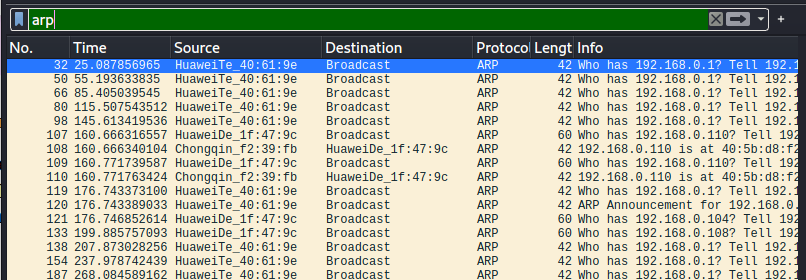
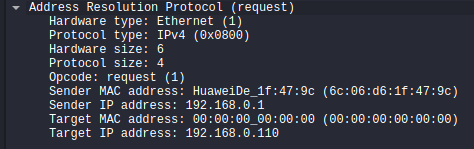
Time to Live — счетчик, ограничивающий время жизни пакета.

Protocol — сообщает, какому протоколу транспортного уровня нужно передать этот пакет.

5. 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).

arp -d 192.168.88.254

Фильтр захвата:

Рассмотрим ARP-запрос:

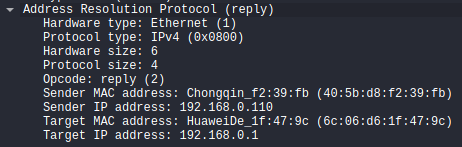
Sender MAC address — MAC-адрес отсправителя

Sender IP address — IP-адрес отпавителя

Target MAC address — MAC-адрес получателя

Target IP address — IP-адрес получателя

Рассмотрим ARP-ответ:

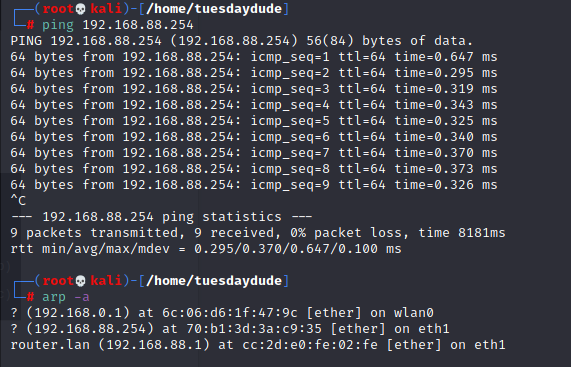


Sender MAC address — целевое поле MAC-адреса получателся

Sender IP address — IP-адрес получателся

Target MAC address — MAC-адрес исходного отправителя

Target IP address — IP-адрес исходного отправителя

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