

Лабораторная работа №2.

«Основы фильтрации трафика в Wireshark»

Теоретические основы

Существует множество инструментальных средств, предоставляющих необходимые возможности для выполнения мониторинга сети и анализа сетевого трафика. Одним из таких средств является пакет Wireshark, представляющий собой программный анализатор протоколов. Анализатор протоколов переводит сетевой адаптер в режим «беспорядочного» приема кадров, записывает в свой буфер кадры сетевого трафика, по запросам пользователя выводит на экран те или иные кадры из буфера и посредством декодера протоколов предоставляет пользователю информацию о значениях полей заголовка протокола и содержимое его блока данных.

Целью данной работы является приобретение навыков фильтрации сетевого трафика в сегменте локальной сети с помощью программного анализатора протоколов Wireshark.

Запустите Wireshark и разверните главное окно приложения на весь экран (для удобства работы). Перед выполнением захвата сетевого трафика необходимо настроить параметры захвата или проконтролировать установленные значения некоторых из них так, чтобы собранная информация адекватно соответствовала решаемой задаче анализа трафика.

На экране монитора в программе Wireshark вы увидите несколько панелей с отображением сетевых пакетов, только что записанных в буфер. Общий вид окна приложения представлен на рис. 1. Пользовательский интерфейс программы содержит следующие компоненты:

- меню команд и панель инструментов;
- фильтр отображения пакетов;
- список пакетов в буфере;
- панель отображения декодера протоколов;
- панель отображения пакета в шестнадцатеричном коде и символах ASCII.

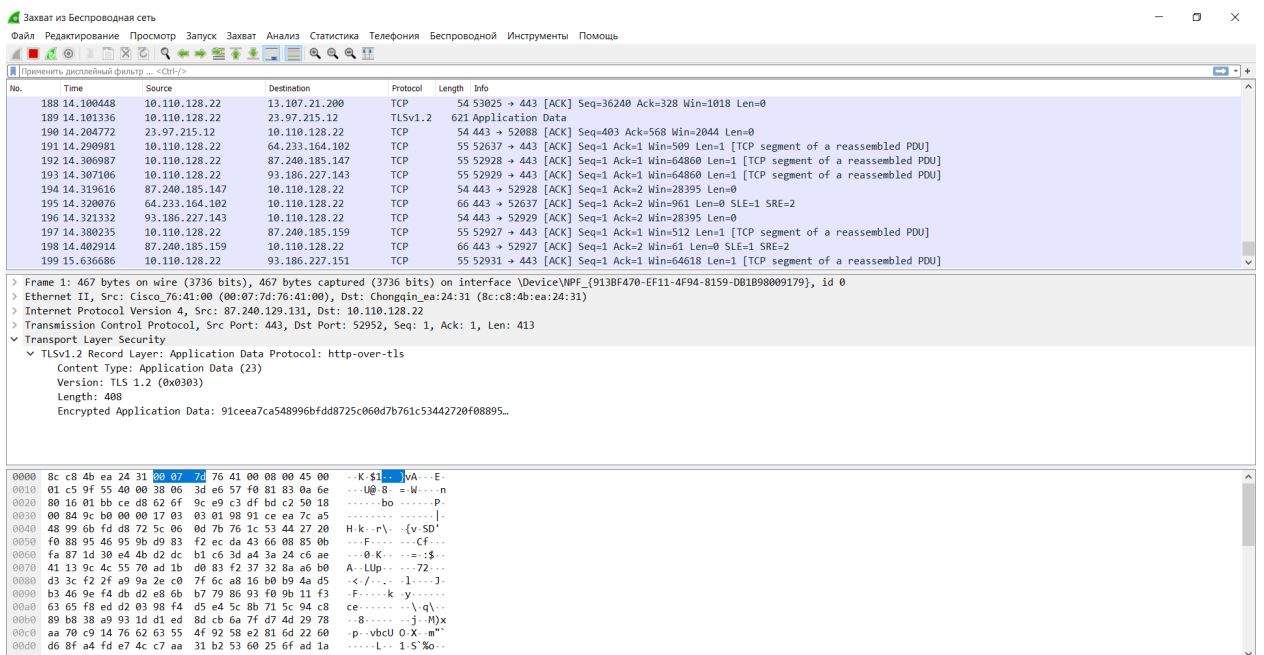


Рис. 1. Общий вид приложения Wireshark

Фильтрация

С помощью фильтра отображения можно быстро убрать «мусор». Выражение фильтрации может представлять собой просто название протокола, который присутствует в пакете на том или ином уровне вложенности.

1. Фильтр по протоколу

Достаточно в строке фильтра ввести название протокола и нажать ввод. На экране останутся пакеты, которые относятся к искомому протоколу. Например: `arp` — для отображения пакетов протокола ARP, `tcp` — для отображения пакетов, в которых присутствует заголовок протокола TCP.

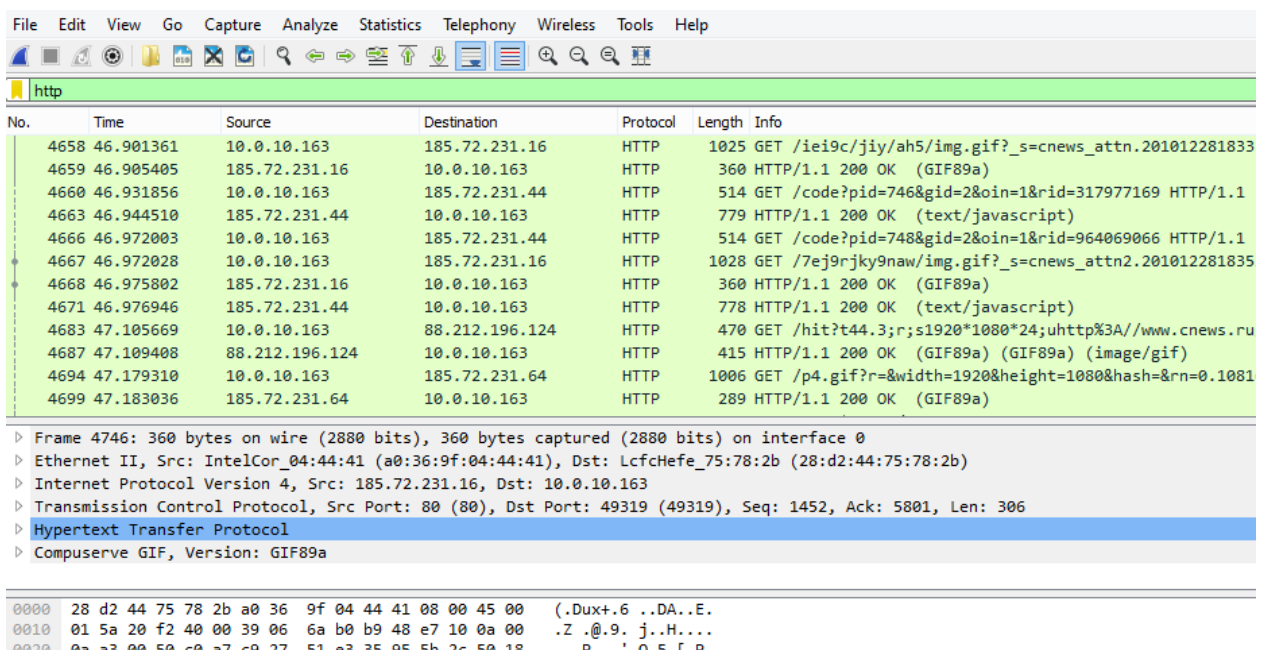
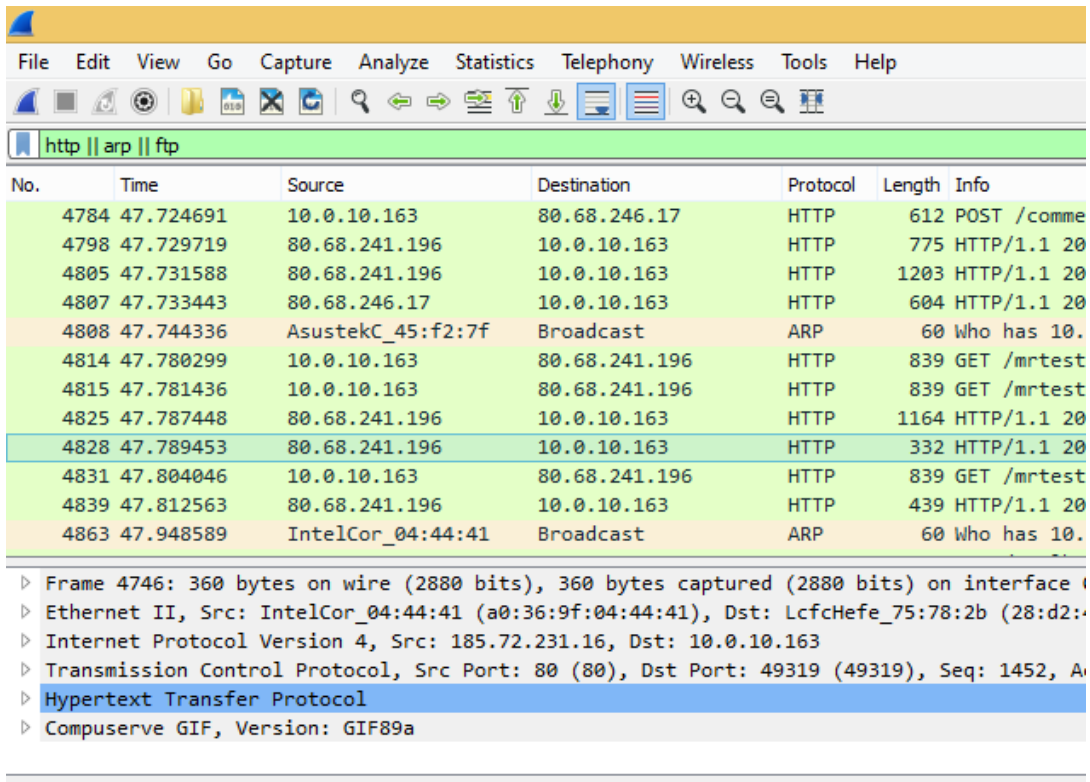


Рис. 2. Фильтр по протоколу

2. Составной фильтр

Если буфер захвата необходимо отфильтровать по нескольким протоколам, то необходимо перечислить все желаемые протоколы и разделить их знаком || (или or). Например:

arp || http || icmp



| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------|-------------------|---------------|----------|--------|-------------|
| 4784 | 47.724691 | 10.0.10.163 | 80.68.246.17 | HTTP | 612 | POST /comme |
| 4798 | 47.729719 | 80.68.241.196 | 10.0.10.163 | HTTP | 775 | HTTP/1.1 20 |
| 4805 | 47.731588 | 80.68.241.196 | 10.0.10.163 | HTTP | 1203 | HTTP/1.1 20 |
| 4807 | 47.733443 | 80.68.246.17 | 10.0.10.163 | HTTP | 604 | HTTP/1.1 20 |
| 4808 | 47.744336 | AsustekC_45:f2:7f | Broadcast | ARP | 60 | Who has 10. |
| 4814 | 47.780299 | 10.0.10.163 | 80.68.241.196 | HTTP | 839 | GET /mrtest |
| 4815 | 47.781436 | 10.0.10.163 | 80.68.241.196 | HTTP | 839 | GET /mrtest |
| 4825 | 47.787448 | 80.68.241.196 | 10.0.10.163 | HTTP | 1164 | HTTP/1.1 20 |
| 4828 | 47.789453 | 80.68.241.196 | 10.0.10.163 | HTTP | 332 | HTTP/1.1 20 |
| 4831 | 47.804046 | 10.0.10.163 | 80.68.241.196 | HTTP | 839 | GET /mrtest |
| 4839 | 47.812563 | 80.68.241.196 | 10.0.10.163 | HTTP | 439 | HTTP/1.1 20 |
| 4863 | 47.948589 | IntelCor_04:44:41 | Broadcast | ARP | 60 | Who has 10. |

| Frame 4746: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface 0 |
|---|
| Ethernet II, Src: IntelCor_04:44:41 (a0:36:9f:04:44:41), Dst: LcfcHefe_75:78:2b (28:d2:75:78:2b) |
| Internet Protocol Version 4, Src: 185.72.231.16, Dst: 10.0.10.163 |
| Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49319 (49319), Seq: 1452, Ack: 1453, Win: 0, Len: 0 |
| Hypertext Transfer Protocol |
| CompuServe GIF, Version: GIF89a |

Рис.3. Составной фильтр

3. Фильтр по IP-адресу

В зависимости от направления трафика фильтр будет немного отличаться. Например, мы хотим отфильтровать по IP адресу отправителя нашего компьютера:

ip.src==10.0.10.163

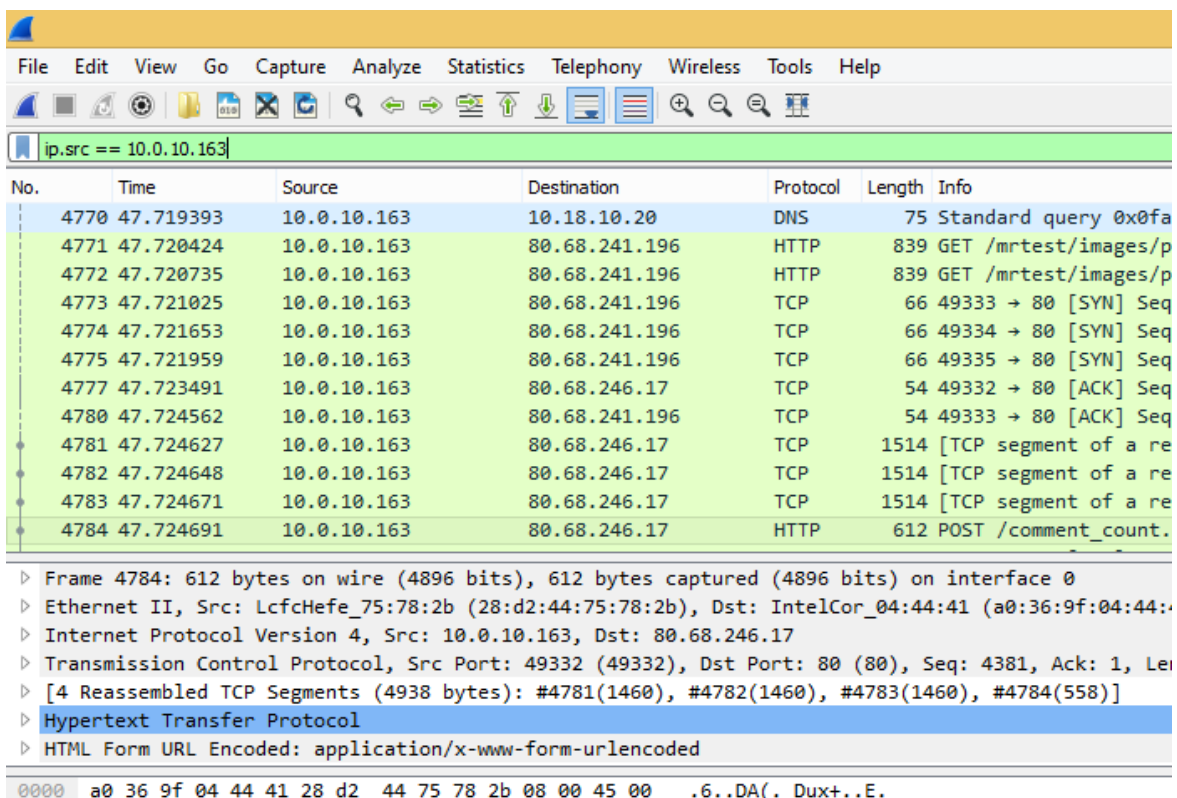


Рис.4. Фильтр по IP-адресу

По получателю фильтр будет выглядеть `ip.dst == x.x.x.x`, а если хотим увидеть пакеты в независимости от направления трафика, то достаточно ввести:

`ip.addr==50.116.24.50`

В случае если нам необходимо исключить какой то адрес из поля отбора, то необходимо добавить `!=`. Пример:

`ip.src!=80.68.246.17`

Более сложные выражения фильтрации строятся с помощью зарезервированных слов, обычно представляющих собой названия полей заголовков того или иного протокола, логической операции и конкретного значения в шестнадцатеричном или десятичном виде.

- a. `!=` (ne)— не равно
- b. `>` (gt)— больше
- c. `<` (lt)— меньше
- d. `>=` (ge)— больше или равно
- e. `<=` (le)— меньше или равно
- f. `&&` — логическое «И» (AND)

Пример: `(ip.dst==10.0.0.1) AND tcp.flags.syn;`

4. Фильтр по времени захвата и номера кадра

Для того чтобы захватить все кадры, начиная с некоторого момента, выполните команду `frame.time_relative`. Например, выделим кадры, захваченные после 5 секунд после начала захвата:

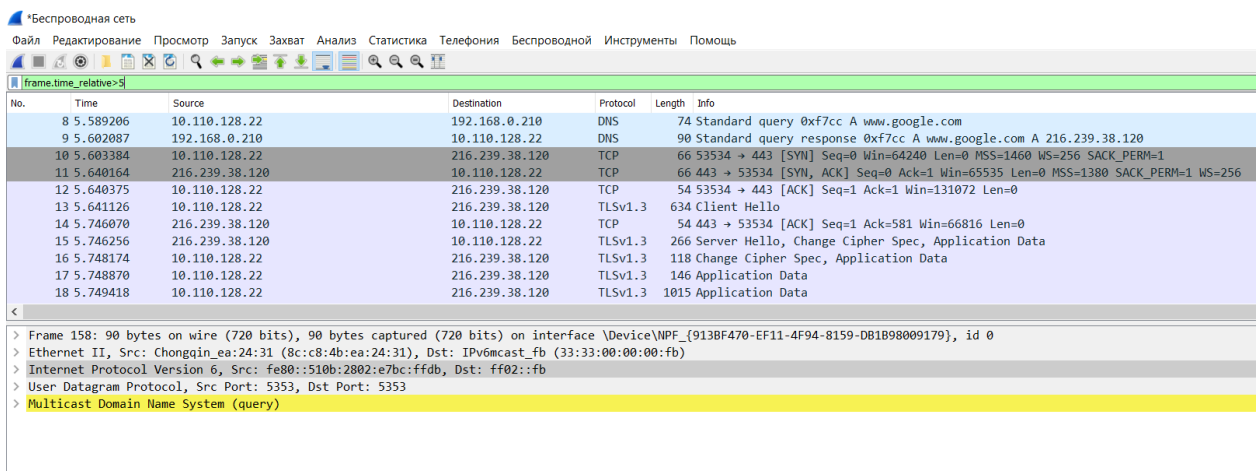


Рис.5. Фильтр по времени захвата

Для того чтобы сделать фильтр по номеру кадра, выполните команду `frame.number`. Например, выделим кадры с 300 до 500:

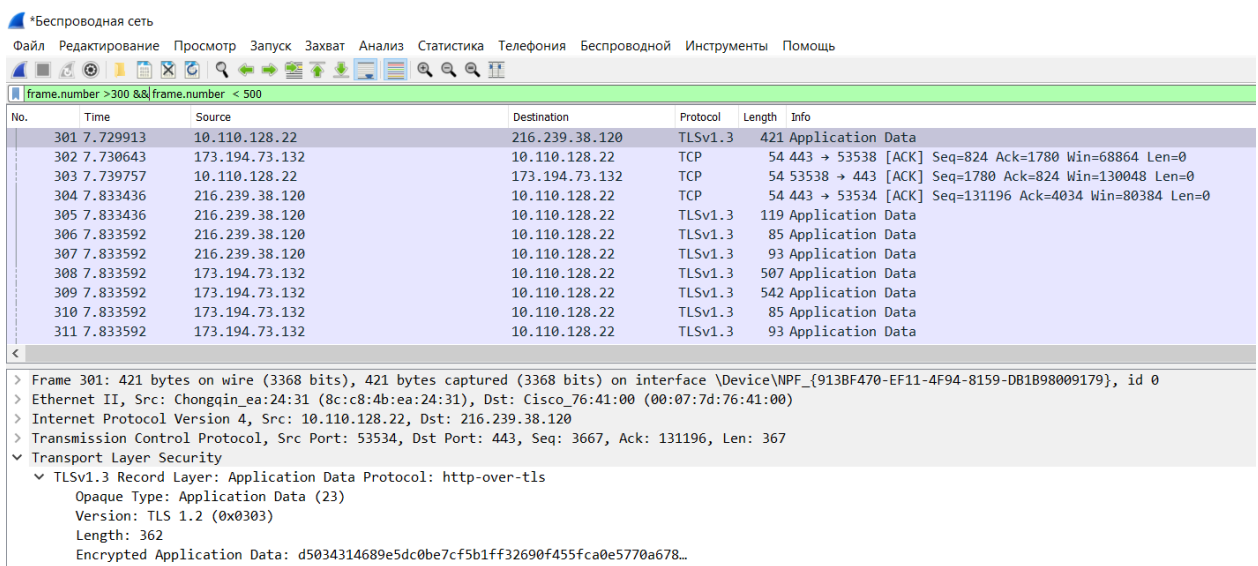


Рис. 6. Фильтр по номеру кадра.

5. Элементы статистики

Для простейшего анализа статистики захваченных кадров можно воспользоваться элементом меню «Statistics» (Статистика). Чаще всего используют такие его элементы: «Summary» (Свойства захвата файла), «Conversations» (Диалоги), «Packet Lengths» (Длина пакетов), «IO Graphs» (График ввода/вывода).

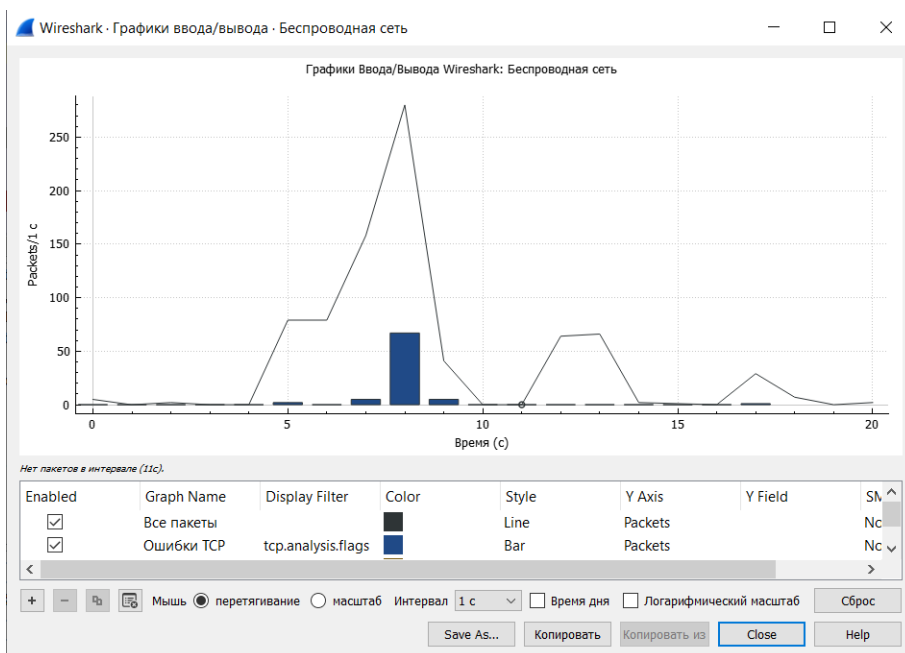


Рис.7. Графики ввода/вывода

Wireshark · Свойства Файла Захвата · Беспроводная сеть

—

□

×

Подробности

Файл

Имя:

C:\Users\holme\AppData\Local\Temp\wireshark_Беспроводная сеть_20200907112557_a08944.pcapng

Длина:

460 kB

Хэш (SHA256):

77c50091b8b184d8c40b4850a5615417f67c599e7930189bd15412e1aaa52199

Хэш (RIPEMD160):

1c4d8be1da3db2413fac0d2f5bafc0ca51ce54ac

Хэш (SHA1):

30b283a7450516b6317f4138b70cd7910ae1b92a

Формат:

Wireshark/... - pcapng

Инкапсуляция:

Ethernet

Время

Первый пакет:

2020-09-07 11:25:57

Последний пакет:

2020-09-07 11:26:18

Прошло:

00:00:20

Захват

Оборудование:

AMD Ryzen 5 3500U with Radeon Vega Mobile Gfx (with SSE4.2)

ОС:

64-bit Windows 10 (1903), build 18362

Приложение:

Dumpcap (Wireshark) 3.2.6 (v3.2.6-0-g4f9257fb8ccc)

Интерфейсы

| Интерфейс | Потерянные пакеты | Фильтр захвата | Тип связи | Ограничение размера пакета |
|-------------------|-------------------|----------------|-----------|----------------------------|
| Беспроводная сеть | 0 (0.0%) | никакой | Ethernet | 262144 байты |

Статистика

| Измерение | Захвачено | Показано | Помечено |
|-----------------------------|-----------|----------------|----------|
| Пакеты | 815 | 237 (29.1%) | — |
| Временной промежуток, с | 20.798 | 1.938 | — |
| В среднем, пакетов/с | 39.2 | 122.3 | — |
| Средний размер пакета, Байт | 530 | 496 | — |
| Байты | 432295 | 117574 (27.2%) | 0 |
| В среднем байт/с | 20 k | 60 k | — |
| В среднем бит/с | 166 k | 485 k | — |

Рис. 8. Общая статистика

Ход работы

1. Открыть программу Wireshark, выбрать сетевой адаптер, на котором будет происходить мониторинг (Ethernet, Беспроводная сеть – в зависимости от способа вашего подключения).
2. Захватить около 2000-3000 кадров, при этом пользуясь браузером для более скорого сбора необходимого количества. Заскриньте результаты (это нужно делать и в следующих пунктах)

3. Отобразите все кадры, кроме тех, которые используют в качестве протокола сетевого уровня ICMP.

4. Отобразите кадры, использующие либо протокол DNS, либо протокол HTTP.

5. Отобразите все кадры, где адрес назначения – IP-адрес Вашего компьютера.

6. Отобразите кадры, использующие протокол IP версии 6, с помощью команды `ip.version==6`. Подумайте, с помощью еще какой команды можно сделать это?

7. Пользуясь графиком ввода-вывода, визуально выделить период (периоды) наибольшей нагрузки, задать дисплейный фильтр и определить статистические показатели для этого периода. Определить статистические показатели трафика, отразить график нагрузки сети. На сколько увеличилась скорость захвата пакетов в этот период?



