

Анализ сетевого трафика с помощью программы Wireshark

Цель работы: ознакомление с сетевым анализатором Wireshark.

Ход работы:

При запуске программы Wireshark появится стартовый интерфейс программы.

Для старта программы и перехвата данных нажмите кнопку «Interface List» (Список интерфейсов), которая помогает вывести весь список сетевых адаптеров для перехвата трафика.

В открывшемся окне «Capture Interface» (Перехват интерфейсов) программы Wireshark, установите флажок рядом с интерфейсом, подключенным к вашей локальной сети и нажмите кнопку «Start», чтобы начать перехват данных.

По завершению процесса перехвата пакеты, которые были захвачены, будут отображены в окне программы. Строки данных выделяются различными цветами в зависимости от протокола (рис. 2.1).

Для того чтобы произвести фильтрацию по пакетам и выбрать необходимый фильтр, нажмите на кнопку «Filter» в окне программы. Появится окно с опциями на выбор: Только TCP; только UDP; только HTTP. Пример приведен на рис. 2.2.

File Edit View Go Capture Analyze Statistics Tempory Tools Internet IPv6

Filter: Expressions: Clear Apply

| No. | Time | Source | Destination | Protocol | Length | Info |
|-----|------------|----------------|----------------|----------|--------|--|
| 3 | 0.01300400 | 194.87.2.114 | 172.17.251.158 | TCP | 90 | 3133000000 → 3133010000 [RST] Seq=19487255134 |
| 4 | 0.04846700 | 172.17.251.158 | 23.42.27.27 | TCP | 60 | 3133010000 → 313301158 [RST] Seq=19487255134 |
| 5 | 0.04915100 | 23.42.27.27 | 172.17.251.158 | TCP | 60 | 313301158 → 3133010000 [RST] Seq=19487255134 |
| 6 | 0.04948600 | 172.17.251.158 | 23.42.27.27 | TCP | 60 | 313301158 → 3133010000 [RST] Seq=19487255134 |
| 7 | 0.04985800 | 172.17.251.158 | 23.42.27.27 | TCP | 60 | 313301158 → 3133010000 [RST] Seq=19487255134 |
| 8 | 0.04995200 | 23.42.27.27 | 172.17.251.158 | TCP | 60 | 3133010000 → 313301158 [RST] Seq=19487255134 |
| 9 | 0.15902700 | 23.42.27.27 | 172.17.251.158 | TCP | 60 | 313301158 → 3133010000 [RST] Seq=19487255134 |
| 10 | 0.15903000 | 23.42.27.27 | 172.17.251.158 | TCP | 60 | 313301158 → 3133010000 [RST] Seq=19487255134 |
| 11 | 0.15915000 | 172.17.251.158 | 23.42.27.27 | TCP | 60 | 313301158 → 3133010000 [RST] Seq=19487255134 |
| 12 | 0.15915400 | 23.42.27.27 | 172.17.251.158 | TCP | 60 | 3133010000 → 313301158 [RST] Seq=19487255134 |
| 13 | 0.15941000 | 172.17.251.158 | 23.42.27.27 | TCP | 60 | 313301158 → 3133010000 [RST] Seq=19487255134 |
| 14 | 0.15944400 | 172.17.251.158 | 23.42.27.27 | TCP | 60 | 313301158 → 3133010000 [RST] Seq=19487255134 |
| 15 | 0.17849900 | 23.42.27.27 | 172.17.251.158 | TCP | 60 | 3133010000 → 313301158 [RST] Seq=19487255134 |
| 16 | 4.85246600 | 172.17.251.158 | 87.240.131.119 | SSH | 558 | SSH Connexion data |
| 17 | 4.86858000 | 87.240.131.119 | 172.17.251.158 | TCP | 17 | 66443 → 31008 [ACK] Seq=1. Ach=2 WIn=0 WOut=0 Len=0 |
| 18 | 5.02030700 | 95.213.4.196 | 172.17.251.158 | TLSv1.2 | 476 | Application data |
| 19 | 5.93751000 | 172.17.251.158 | 95.213.4.196 | TLSv1.2 | 305 | Application data |
| 20 | 5.93761000 | 172.17.251.158 | 95.213.4.196 | TLSv1.2 | 309 | Application data |
| 21 | 5.95091000 | 95.213.4.196 | 172.17.251.158 | TCP | 60 | 313301158 → 3133010000 [ACK] Seq=423. Ach=537 WIn=2555 Len=0 |
| 22 | 5.95223000 | 95.213.4.196 | 172.17.251.158 | TCP | 60 | 313301158 → 3133010000 [ACK] Seq=423. Ach=537 WIn=2555 Len=0 |
| 23 | 5.97233000 | 94.100.187.27 | 172.17.251.158 | TLSv1.2 | 474 | Application data |
| 24 | 3.99523300 | 94.100.187.27 | 172.17.251.158 | TLSv1.2 | 474 | Application data |

Packet 17: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0

Ethernet II, Src: Realtek-UTec-8 (88-9f-f6-1c-02), Dst: Cisco-L_28-8c-a2 (8e-b9-73-39-8c-a2)

TCP Reset, Seq=1. Ach=2. Win=0. Len=0

User: Outlook Protocol: SFS PORT: 60323, Src port: 53 (53)

Domain: Mail System (query)

0000 08 0b 73 39 8c a7 88 9f f8 1c 02 02 08 00 45 00 ...E..

0010 00 3f 14 00 00 81 2f 49 2c 11 f8 0c 23 43 ...-..

0020 00 00 00 00 00 00 00 63 73 08 74 65 7f 69 ...:.....

0030 00 00 00 00 00 00 00 63 73 08 74 65 7f 69 ...:.....

0040 73 39 8c a7 03 83 6f 65 00 00 01 00 01 ...:.....

Inspecteur de réseau en ligne (file cap) Paquets 41 - (Durée: 0) 1000%

Profile: Default

Рис. 2.1. Вид главного рабочего окна программы Wireshark

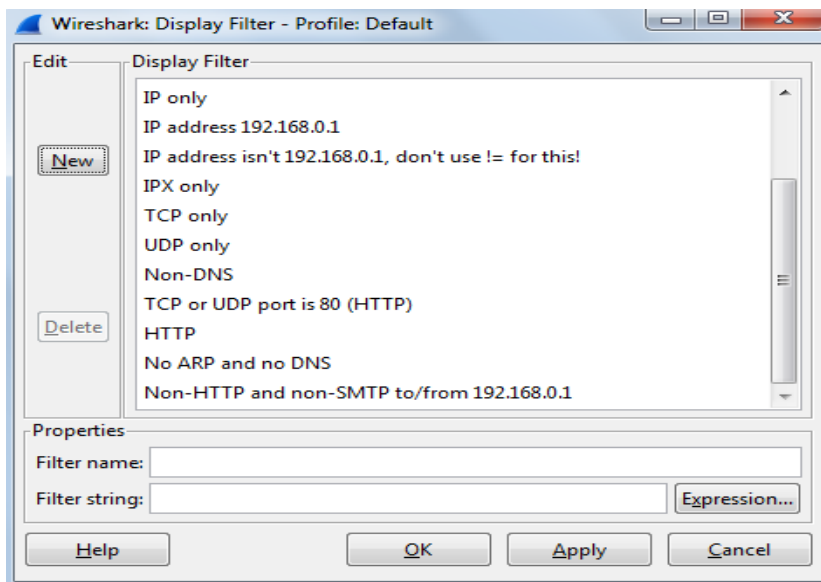


Рис. 2.2. Окно фильтра программы Wireshark

Таким образом, осуществим поиск пакета, используя фильтр и определим только пакеты TCP. Для этого в меню программы Wireshark открываем «Edit» нажмите кнопку «Find Packet», откройте «Filter» и выберите параметр «TCP only». Пример поиска пакета приведен на рис. 2.3.

Протоколы расположены в виде иерархического дерева, от низкоуровневых к более высокоуровневым, согласно стеку протоколов и очередности инкапсуляции. Информация о каждом протоколе может быть развернута до подробного описания всех полей и их значений. Пример представлен на рис. 2.4.

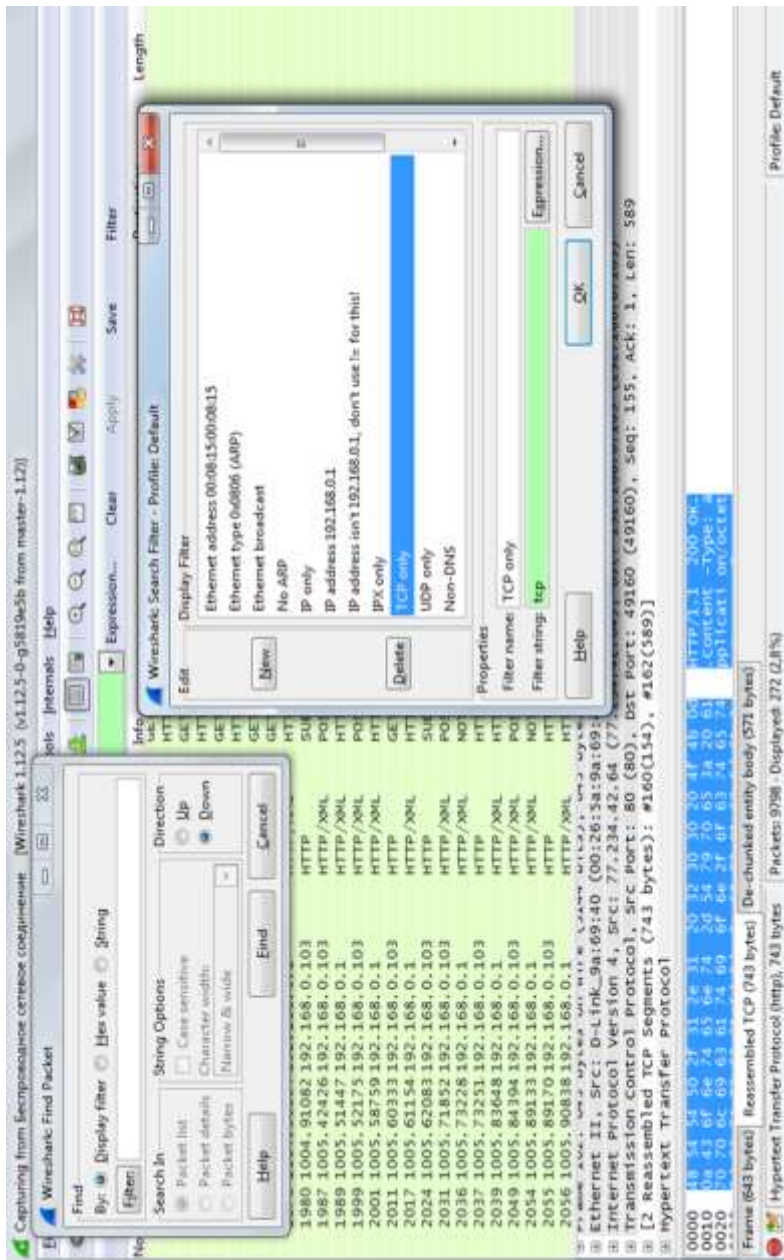


Рис. 2.3. Окно программы поиска пакета через фильтр

Панель «байты пакетов» показывает данные текущего пакета. Слева показывается смещение данных пакета, по центру данные пакета показаны в шестнадцатеричной системе исчисления и справа показывается соответствующий вид код вида ASCII. Пример приведен на рис. 2.5.

Пакет характеризуется следующими параметрами:

- No – номер пакета;
- Time – временная отметка пакета показывает время, в которое захвачен пакет;
- Source – адрес отправителя (откуда пришел пакет);
- Protocol – название протокола в сокращенной версии;
- Info – краткое содержание пакета;
- Destination – адрес получателя (куда пойдет пакет);
- Length – размер пакета.

Далее вся информация протоколов записывается в окне статистики программы Wireshark. Перейдите в меню «Statistics» и выберите «Conversations» (рис. 2.6). Wireshark также может выводить полученную информацию в графическом режиме, что облегчает ее восприятие. Перейдя в «Graphs tool», в меню «Statistics», вы можете выбрать до пяти фильтров для сравнения файлов с помощью выделения различными цветами. Пример графика зависимости разного типа приведен на рис. 2.7.

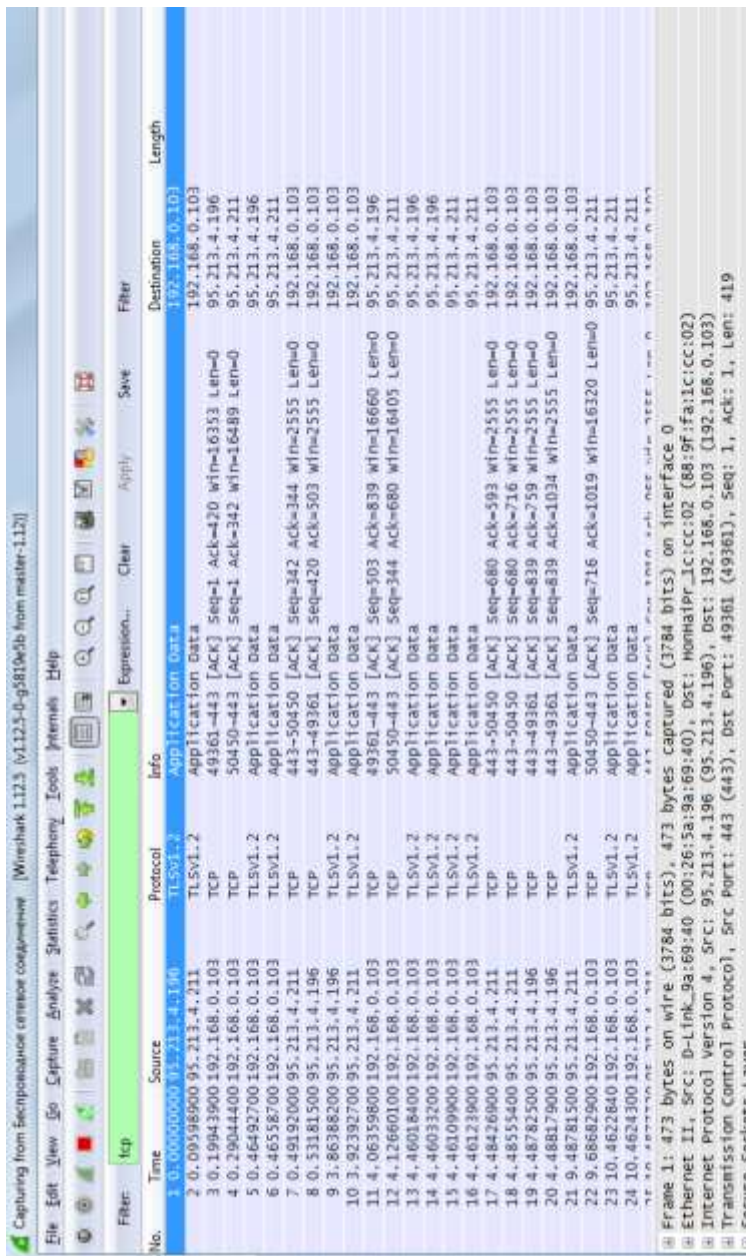


Рис. 2.5. Окно «байты пакетов» программы Wireshark



Рис. 2.6. Окно статистики программы Wireshark

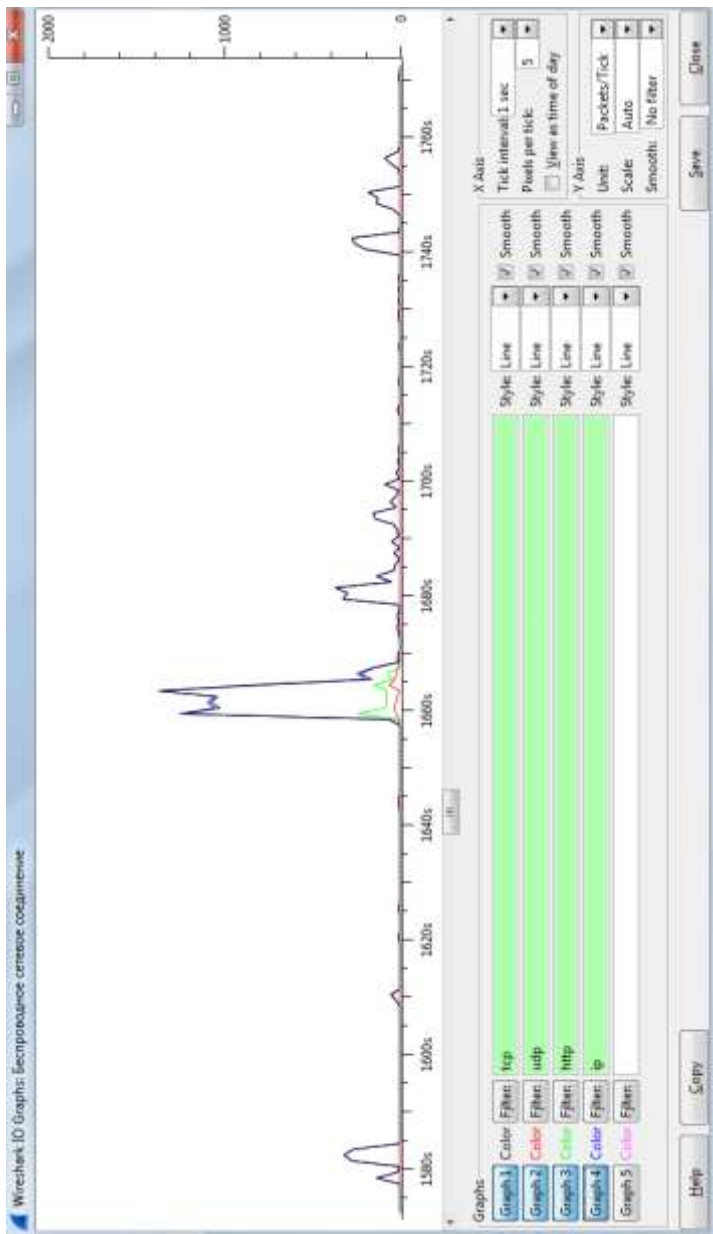


Рис. 2.7. Окно графика зависимости разного типа программы Wireshark

Задание:

- осуществить перехват трафика;
- произвести фильтрацию трафика по пакетам типа: TCP, UDP, HTTP;
- произвести поиск пакета в соответствии с заданием преподавателя и расшифровать его содержимое;
- сделать анализ по выполненной работе.