МИНИСТЕРСТВО ТРАНСПОРТА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

Институт транспортной техники и систем управления

Кафедра «Автоматика, телемеханика и связь на железнодорожном транспорте»

АНАЛИЗАТОР ПРОТОКОЛОВ WIRESHARK

Учебно-методическое пособие
для выполнения лабораторных работ
по дисциплинам «Передача дискретной информации на железнодорожном транспорте», «Передача данных по цифровым сетям»

Москва – 2017

МИНИСТЕРСТВО ТРАНСПОРТА
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ
«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА (МИИТ)»

Институт транспортной техники и систем управления

Кафедра «Автоматика, телемеханика и связь на железнодорожном транспорте»

АНАЛИЗАТОР ПРОТОКОЛОВ WIRESHARK

Учебно-методическое пособие для студентов специальности 23.05.05 «Системы обеспечения движения поездов» специализаций «Телекоммуникационные системы и сети железнодорожного транспорта», «Автоматика и телемеханика на железнодорожном транспорте» (специалитет)

Москва – 2017

УДК 004
А 64

Анализатор протоколов Wireshark/ П.Н. Толмачев, Н.А. Ермакова, П.В. Подворный, С.А. Сапсай: Учебно-методическое пособие для выполнения лабораторных работ. – М.: РУТ (МИИТ), 2016. – 38 с.

Учебно-методическое пособие для выполнения лабораторных работ содержит методические рекомендации: по установки и запуску на компьютере программы Wireshark, захвату пакетов (TCP, UDP, HTTP и др.), исследованию трафика с помощью сетевого анализатора Wireshark.

Рекомендовано для специальности 23.05.05 «Системы обеспечения движения поездов» специализаций «Телекоммуникационные системы и сети железнодорожного транспорта», «Автоматика и телемеханика на железнодорожном транспорте» (специалитет).

Рецензент: д.т.н., профессор каф. "Электроэнергетика транспорта" РУТ (МИИТ) Гречишников В.А.

ВВЕДЕНИЕ

Wireshark – это программный инструмент для перехвата и анализа сетевого трафика. Сама программа, в первую очередь, предназначена для сбора информации о сетевых взаимодействиях и для обнаружения и устранения неполадок в сети. Анализаторы трафика применяются при разработке новых протоколов и программного обеспечения.

Установленная и запущенная на компьютере программа Wireshark позволяет обнаружить и изучить любой протокольный блок данных (Protocol Data Unit, PDU), который был отправлен и получен с помощью установленных на компьютере сетевых адаптеров (Network Interface Card, NIC). По мере движения потоков данных по сети анализатор перехватывает каждый протокольный блок данных (PDU), после чего расшифровывает или анализирует его содержание согласно соответствующему документу RFC или другим спецификациям.

Анализатор трафика (сниффер) может анализировать только то, что проходит через его сетевую карту. Внутри одного сегмента сети Ethernet все пакеты рассылаются на все компьютеры сегмента. Использование коммутаторов (switch, switch-hub) и их грамотная конфигурация уже является защитой от прослушивания. Между сегментами информация передаётся через коммутаторы. Коммутация пакетов – форма передачи, при которой данные, разбитые на отдельные пакеты, могут

пересылаться из исходного пункта в пункт назначения разными маршрутами. Если в другом сегменте внутри него передаются какие-либо пакеты, то в другой сегмент коммутатор эти данные не отправит.

Перехват трафика может осуществляться:

– обычным «прослушиванием» сетевого интерфейса (метод эффективен при использовании в сегменте концентраторов (хабов) вместо коммутаторов (свитчей), в противном случае метод малоэффективен, поскольку на сниффер попадают лишь отдельные фреймы);

– подключением сниффера в разрыв канала;

– ответвлением (программным или аппаратным) трафика и направлением его копии на сниффер;

– через анализ побочных электромагнитных излучений и восстановление таким образом прослушиваемого трафика;

– через атаку на канальном или сетевом уровне, приводящую к перенаправлению трафика жертвы или всего трафика сегмента на сниффер с последующим возвращением трафика в надлежащий адрес.

ЛАБОРАТОРНАЯ РАБОТА № 1

Изучение программы протокол-анализатора Wireshark

Цель работы: Загрузка и установка программы Wireshark. Настройка программы Wireshark и запуск захвата трафика.

Ход работы: Загрузка программы осуществляется с официального сайта по адресу: www.wireshark.org. Внешний вид программы Wireshark на экране представлен на рис.1.1.

Рис. 1.1. Вид окна «загрузка программы» Wireshark

В верхнем левом углу нажмите поле «Download». В открывшемся окне выберите версию программы в соответствии с архитектурой и операционной системой вашего ПК. Например,

если ваш ПК работает под управлением 64 - разрядной ОС Windows, выберите Windows Installer (64 - bit) (рис. 1.2).

Сразу после этого начнется загрузка. Местонахождение загруженного файла зависит от браузера и операционной системы, которыми вы пользуетесь. В ОС Windows загрузочные файлы по умолчанию находятся в папке «Загрузки». Программа Wireshark готова для установки на ваш компьютер. Загруженный файл называется Wireshark – win – x.x.x.exe, где «x» соответствует номеру версии программы.

Дважды нажмите на файл, чтобы начать установку. Ответьте на все сообщения безопасности, которые появятся на экране.

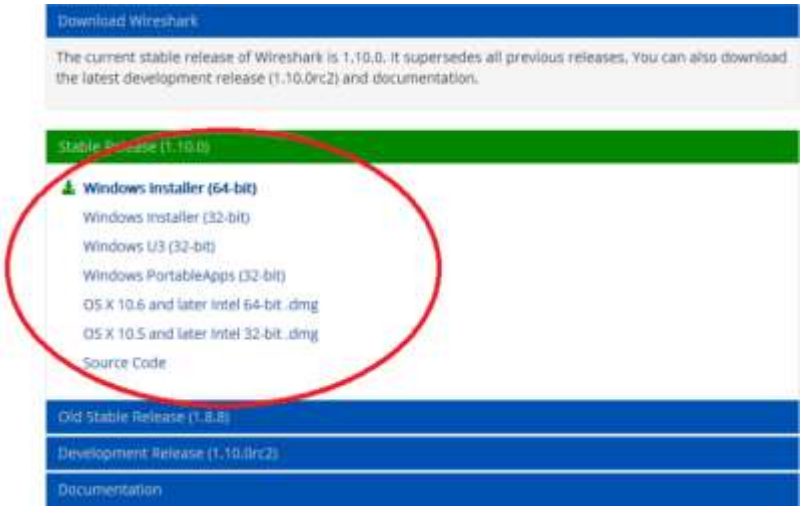


Рис. 1.2. Вид окна «выбор версии программы» Wireshark

При первой установке программы Wireshark на компьютер или в том случае, когда предыдущая версия была удалена, откроется мастер установки программы Wireshark. Нажмите кнопку «Next» (Далее) (рис. 1.3).

Выполните все инструкции по установке. Когда откроется окно «License Agreement» (Лицензионное соглашение), нажмите кнопку «I accept» (Принять). Вид окна «Лицензионного соглашения» представлен на рис. 1.4.

При выборе компонентов оставьте настройки по умолчанию и нажмите кнопку «Next» (Далее) (рис. 1.5).

Рис. 1.3. Мастер установки программы

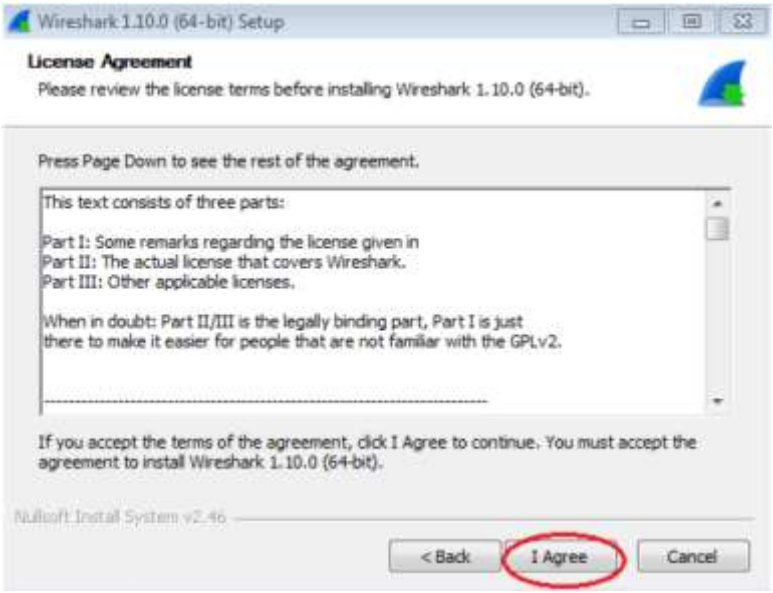


Рис. 1.4. Вид окна «Лицензионного соглашения»

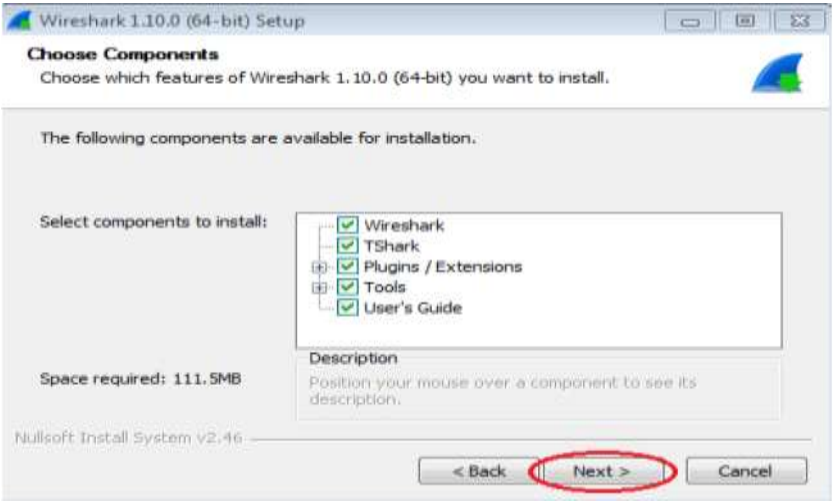


Рис. 1.5. Вид окна программы Wireshark «выбор компонентов»

Выберите где разместить желаемые ярлыки и нажмите кнопку «Next» (Далее) (рис. 1.6).

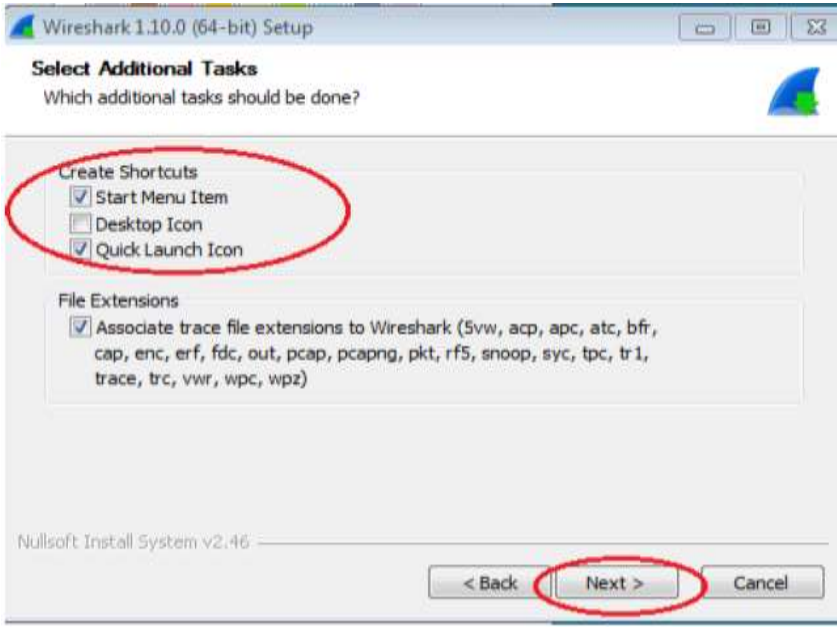


Рис. 1.6. Вид окна программы

Если дисковое пространство ограничено, директорию установки можно изменить, в противном случае оставьте адрес, указанный по умолчанию (рис. 1.7).

После этого начнется установка программы Wireshark. Статус установки будет отображаться в отдельном окне. по завершении установки нажмите кнопку «Next» (Далее) (рис. 1.8).

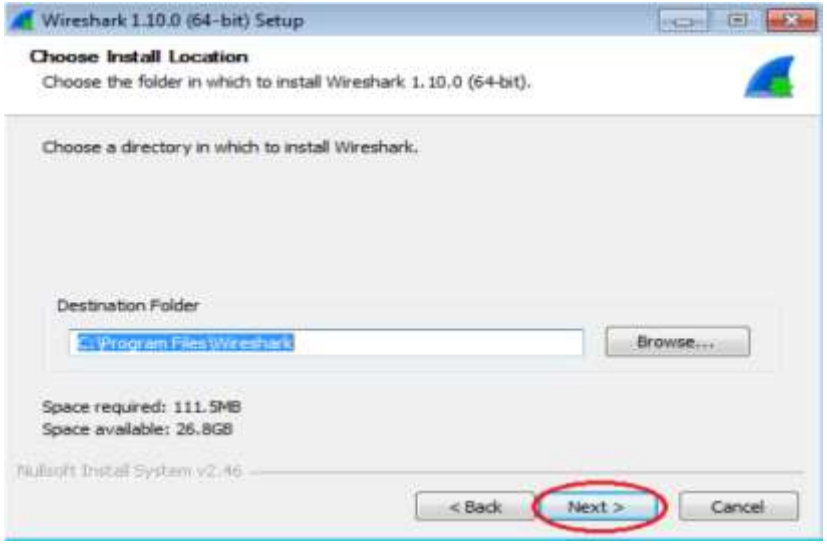


Рис. 1.7. Адрес установки программы

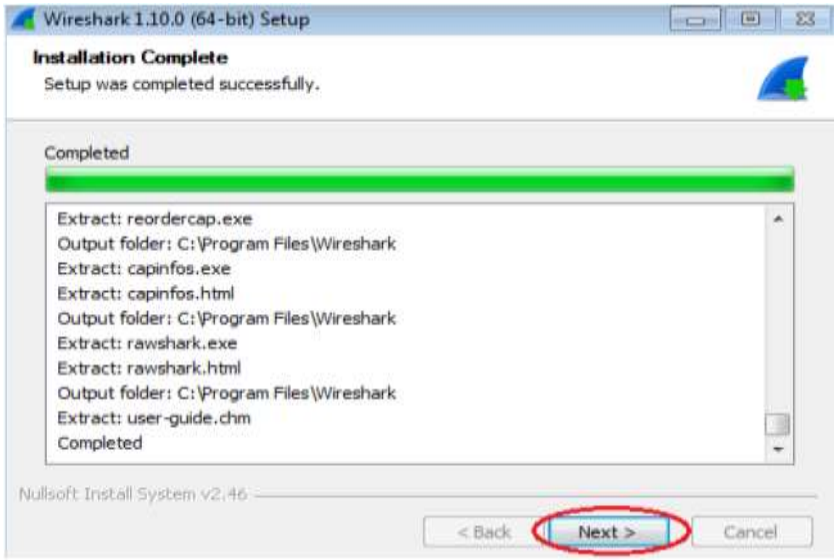


Рис. 1.8. Окно установки программы Wireshark

Для завершения процесса установки программы Wireshark (рис. 1.9) нажмите кнопку «Finish» (Готово).

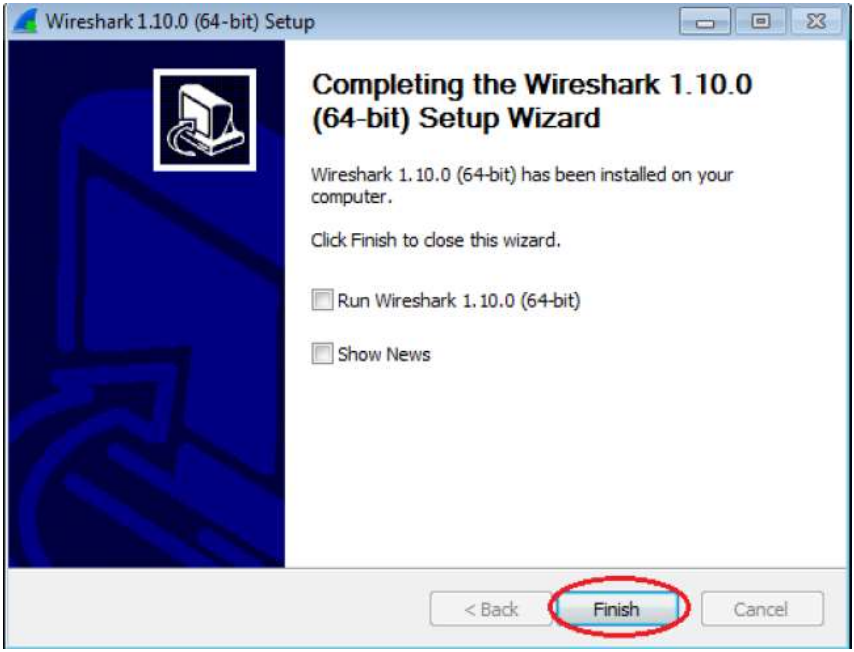


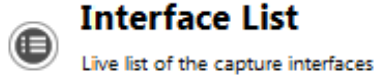
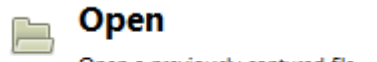
Рис. 1.9. Окно завершения процесса установки

Настройка программы Wireshark и запуск перехвата трафика

Для начала настройки программы Wireshark для запуска перехвата трафика рассмотрим основные функции программы Wireshark (табл. 1.1).

Таблица 1.1

Основные функции программы Wireshark

Название функции	Описание функции
	Кнопка, при нажатии на которую программа выведет список сетевых адаптеров, с которых возможен захват трафика
	Кнопка быстрого старта и выбора активного интерфейса. Нажатие на любой интерфейс из списка запустит процесс захвата трафика
	Кнопка, при нажатии на которую программа выведет окно настроек процесса захвата трафика
	Кнопка, позволяющая загружать в программу захваченный ранее и сохраненный файл с отчётом о захваченном сетевом трафике

При запуске программы Wireshark появится стартовый интерфейс программы, изображенный на (рис 1.10).

Для старта программы и перехвата данных нажмите кнопку «Interface List» (Список интерфейсов), которая помогает вывести весь список сетевых адаптеров для перехвата трафика (рис. 1.11).

В открывшемся окне «Capture Interface» (Перехват интерфейсов) программы Wireshark установите флажок рядом с интерфейсом, подключенным к локальной сети, и нажмите кнопку «Start», чтобы начать перехват данных (рис. 1.12).

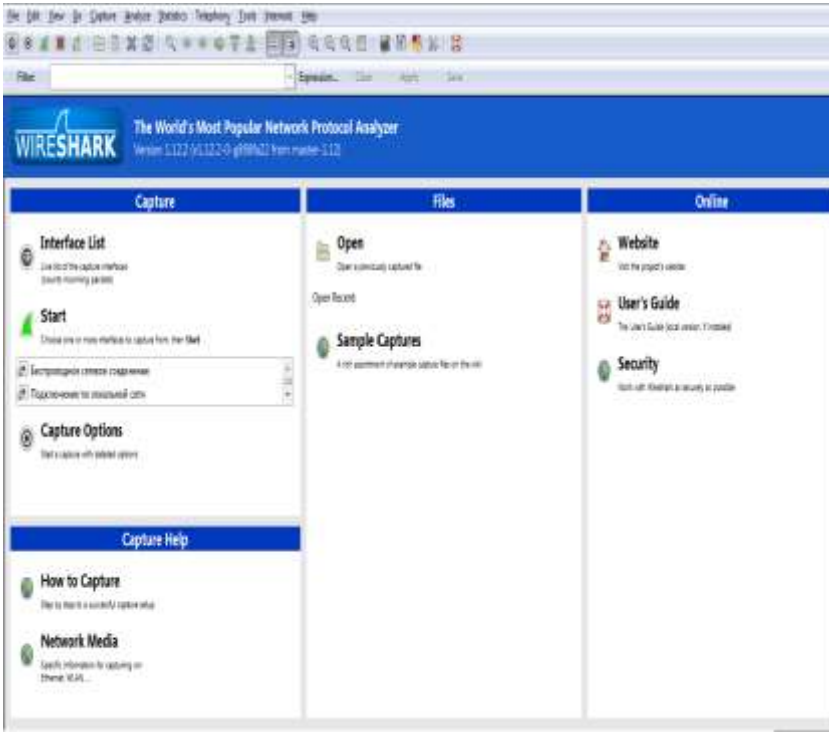


Рис. 1.10. Вид окна стартового интерфейса программы Wireshark

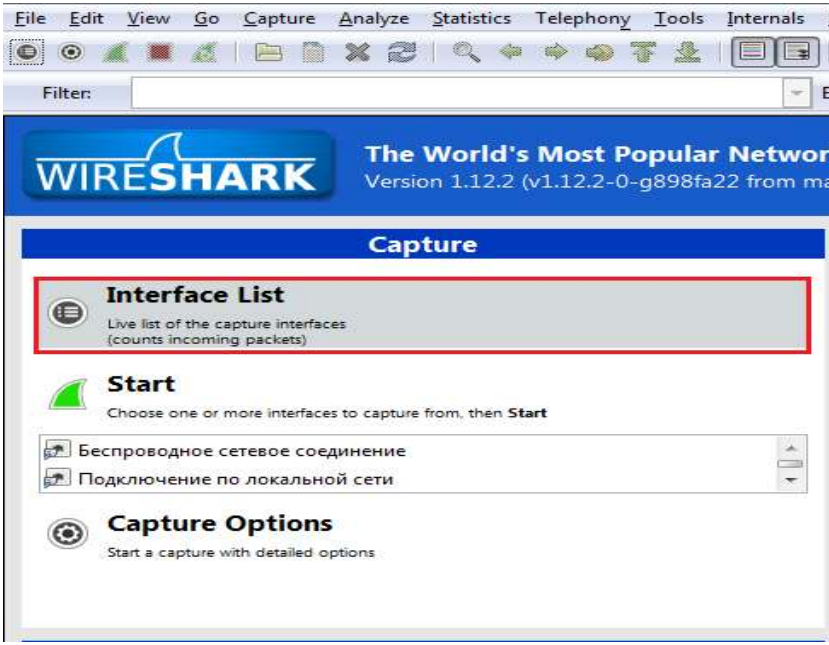


Рис. 1.11. Кнопка «Interface List»

Рис. 1.12. Выбираем интерфейс

В верхней части окна программы Wireshark начнёт отображаться информация. Строки данных выделяются различными цветами в зависимости от протокола (рис. 1.13).

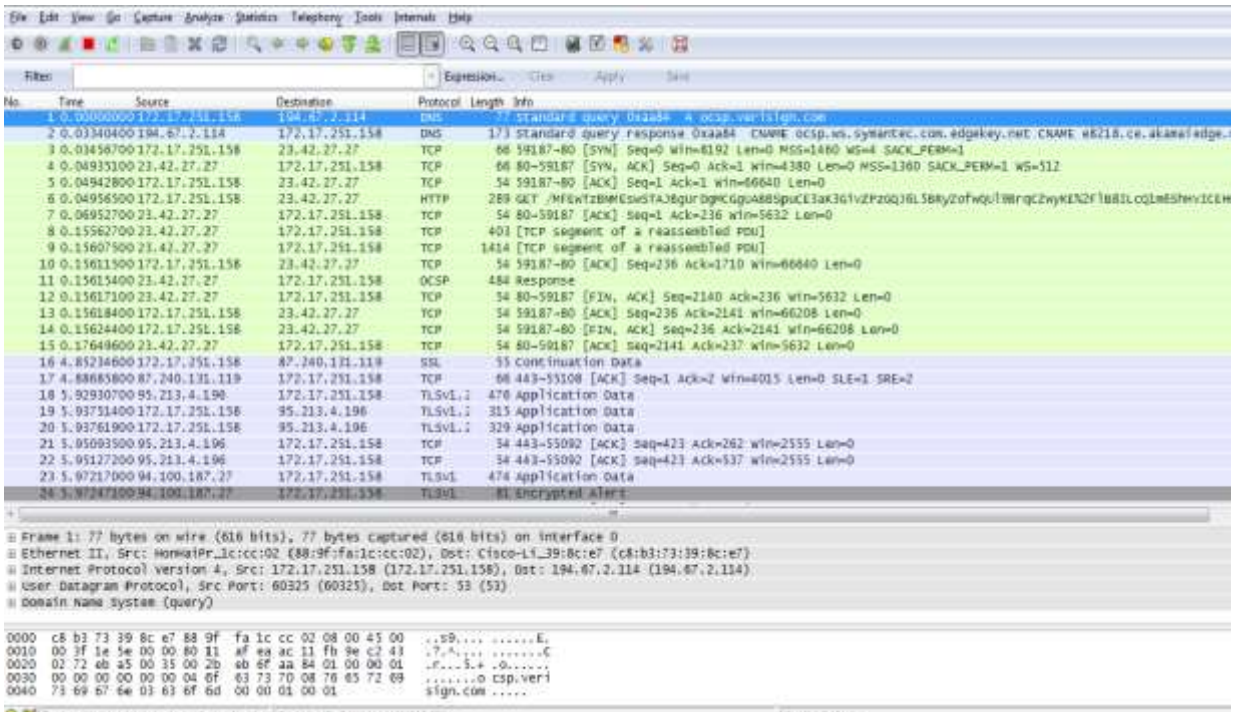


Рис. 1.13. Вид главного рабочего окна программы Wireshark

В верхней части экрана расположена панель инструментов для быстрого использования некоторых функций программы (рис. 1.14). Описание основных функций панели инструментов представлено в табл. 1.2.

Рис. 1.14. Панель инструментов

Таблица 1.2

Основные функции панели инструментов

Кнопка	Название кнопки	Соответствующая опция в меню	Функции кнопки
1	2	3	4
	Interfaces	Capture/Interfaces …	Вызов окна настроек сетевого трафика
	Options	Capture/Options …	Вызов окна настроек захвата сетевого трафика
	Start	Capture/Start…	Старт захвата трафика с текущими параметрами
	Stop	Capture/Stop…	Остановка захвата трафика

Продолжение табл.1.2

1	2	3	4
	Restart	Capture/Restart	Перезапуск захвата трафика с текущими параметрами
	Open	File/Open…	Открыть файл с отчетом о захваченном трафике
	Save As	File/Save As…	Сохранить текущий отчет о захваченном трафике
	Close	File/Close…	Закрыть текущий отчёт о захваченном трафике
	Reload	View/Reload…	Закрыть и открыть заново текущий отчет
	Zoom In	View/Zoom In…	Увеличить размер шрифта
	Zoom Out	View/Zoom Out…	Уменьшить размер шрифта
	Normal Size	View/Normal Size...	Установить размер шрифта, используемый по умолчанию
	Preferences	Edit/Preferences…	Вызов меню настроек
	Help	Help/Contents…	Вызов справки

Под строкой инструментов располагается панель фильтров, которая позволяет настроить программу на отображение только определенного, удовлетворяющего условиям текущего примененного фильтра сетевого трафика. Панель фильтра представлена на рис. 1.15. Описание элементов панели фильтра представлено в табл. 1.3.

Рис. 1.15. Панель фильтра

Таблица 1.3

Описание элементов панели фильтра

Кнопка/поле	Название кнопки/поля	Функция кнопки/поля
Filter:	Filter	Вызов диалогового окна для создания и сохранения пользова тельских фильтров
	Filter Input	Поле ввода фильтра
Expression...	Expression	Вызов диалогового окна, позволяющего выбирать фильтры из базы данных программы
Clear	Clear	Очистить поле ввода фильтра
Apply	Apply	Применить фильтр
Save	Save	Сохранить фильтр

Ниже панели инструментов располагается поле списка PDU, в котором отображается краткая информация по всем захваченным PDU пакетам (рис. 1.16).

В информационном поле (рис. 1.17), отображается подробная информация по выбранному PDU пакетов: версия, длина заголовка, тип обслуживания и т.д.

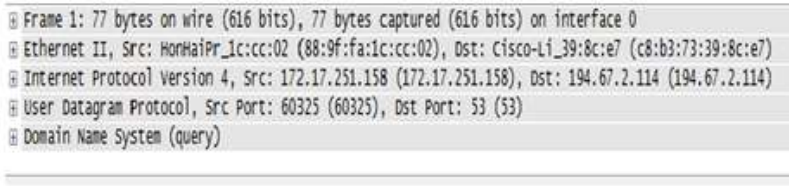


Рис. 1.17. Информационное поле

Внизу экрана располагается поле, в котором отображаются данные, выделенные в информационном поле в шестнадцатеричной системе исчисления и текстовом виде (рис. 1.18).

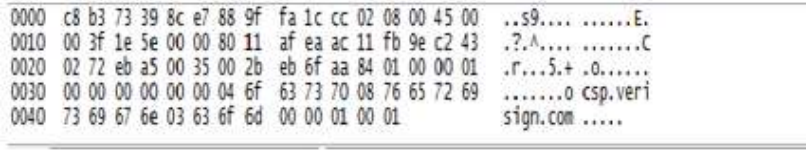
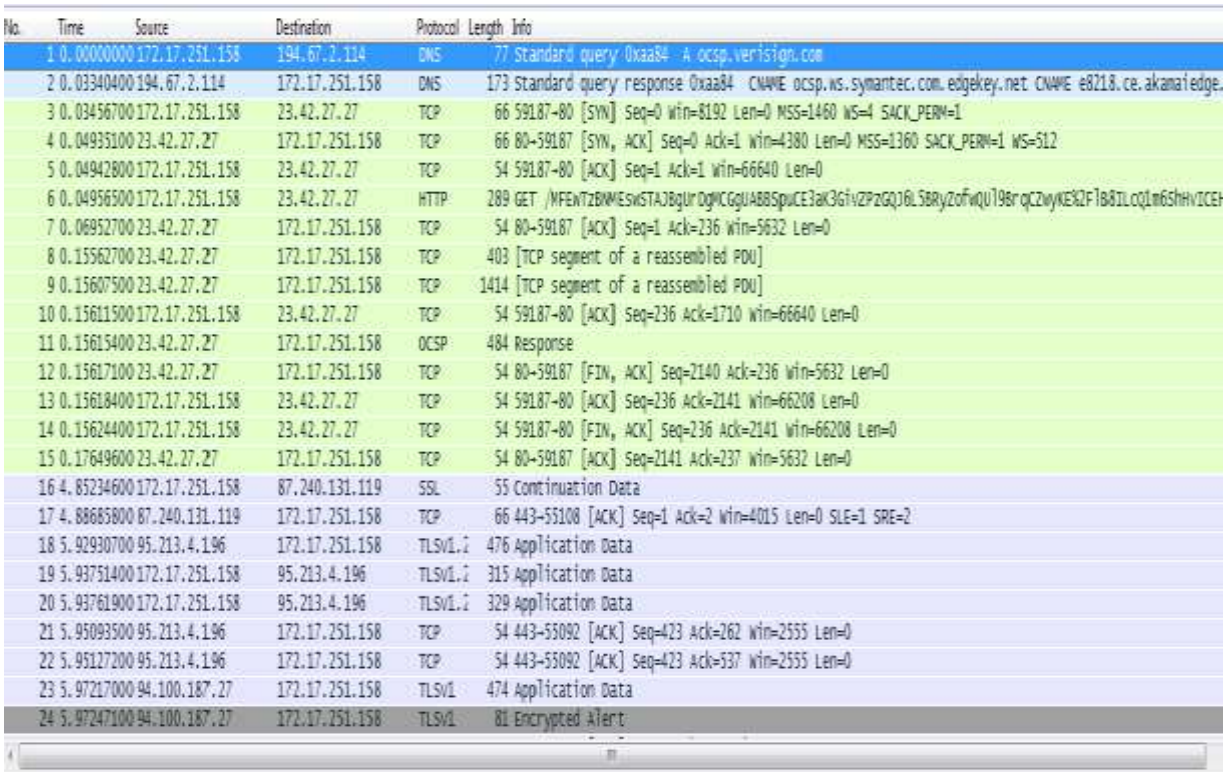


Рис. 1.18. Поле отображения данных



No.	Time	Source	Destination	Protocol	Length	Info
1	0.0000000	172.17.251.158	194.67.2.114	DNS	77	Standard query 0xaa84 A ocsp.verisign.com
2	0.0334040	194.67.2.114	172.17.251.158	DNS	173	Standard query response 0xaa84 CNAME ocsp.ws.symantec.com.edgekey.net CNAME e8218.ce.akamaiedge.
3	0.0345670	172.17.251.158	23.42.27.27	TCP	66	59187→80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
4	0.0493510	23.42.27.27	172.17.251.158	TCP	66	80→59187 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=1360 SACK_PERM=1 WS=512
5	0.0494280	172.17.251.158	23.42.27.27	TCP	54	59187→80 [ACK] Seq=1 Ack=1 Win=66640 Len=0
6	0.0495650	172.17.251.158	23.42.27.27	HTTP	289	GET /MFEwTzBNME swSTAJBgUr DgMCGgUABBSpuCE3aK3GivZPzGQJ6L5BRyZofwQU l98rqCZwyKE%2F l8BILcQ1m6ShHvICEH
7	0.0695270	23.42.27.27	172.17.251.158	TCP	54	80→59187 [ACK] Seq=1 Ack=236 Win=5632 Len=0
8	0.1556270	23.42.27.27	172.17.251.158	TCP	403	[TCP segment of a reassembled PDU]
9	0.1560750	23.42.27.27	172.17.251.158	TCP	1414	[TCP segment of a reassembled PDU]
10	0.1561150	172.17.251.158	23.42.27.27	TCP	54	59187→80 [ACK] Seq=236 Ack=1710 Win=66640 Len=0
11	0.1561540	23.42.27.27	172.17.251.158	OCSP	484	Response
12	0.1561710	23.42.27.27	172.17.251.158	TCP	54	80→59187 [FIN, ACK] Seq=2140 Ack=236 Win=5632 Len=0
13	0.1561840	172.17.251.158	23.42.27.27	TCP	54	59187→80 [ACK] Seq=236 Ack=2141 Win=66208 Len=0
14	0.1562440	172.17.251.158	23.42.27.27	TCP	54	59187→80 [FIN, ACK] Seq=236 Ack=2141 Win=66208 Len=0
15	0.1764960	23.42.27.27	172.17.251.158	TCP	54	80→59187 [ACK] Seq=2141 Ack=237 Win=5632 Len=0
16	4.8523460	172.17.251.158	87.240.131.119	SSL	55	Continuation Data
17	4.8868380	87.240.131.119	172.17.251.158	TCP	66	443→55108 [ACK] Seq=1 Ack=2 Win=4015 Len=0 SLE=1 SRE=2
18	5.9293070	95.213.4.196	172.17.251.158	TLSv1.2	476	Application Data
19	5.9375140	172.17.251.158	95.213.4.196	TLSv1.2	315	Application Data
20	5.9376190	172.17.251.158	95.213.4.196	TLSv1.2	329	Application Data
21	5.9509350	95.213.4.196	172.17.251.158	TCP	54	443→55092 [ACK] Seq=423 Ack=262 Win=2555 Len=0
22	5.9512720	95.213.4.196	172.17.251.158	TCP	54	443→55092 [ACK] Seq=423 Ack=537 Win=2555 Len=0
23	5.9721700	94.100.187.27	172.17.251.158	TLSv1	474	Application Data
24	5.9724710	94.100.187.27	172.17.251.158	TLSv1	81	Encrypted Alert

Рис. 1.16. Поле списка PDU

ЛАБОРАТОРНАЯ РАБОТА № 2

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.

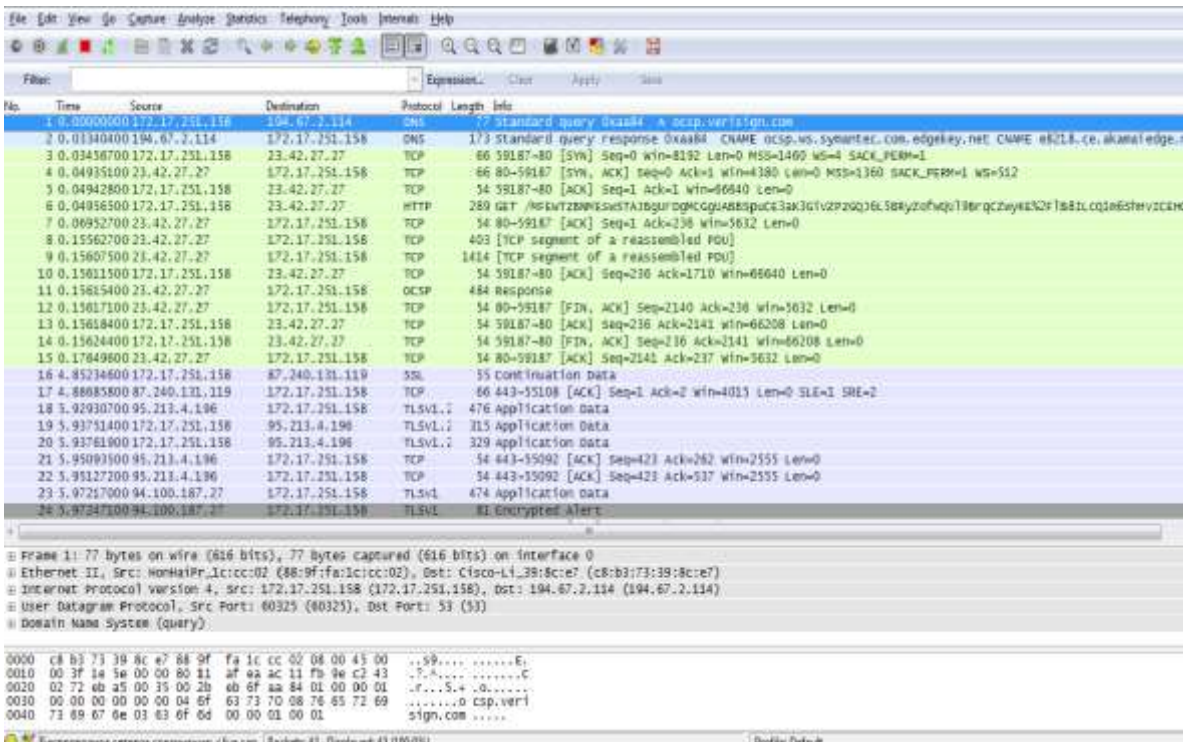


Рис. 2.1. Вид главного рабочего окна программы Wireshark

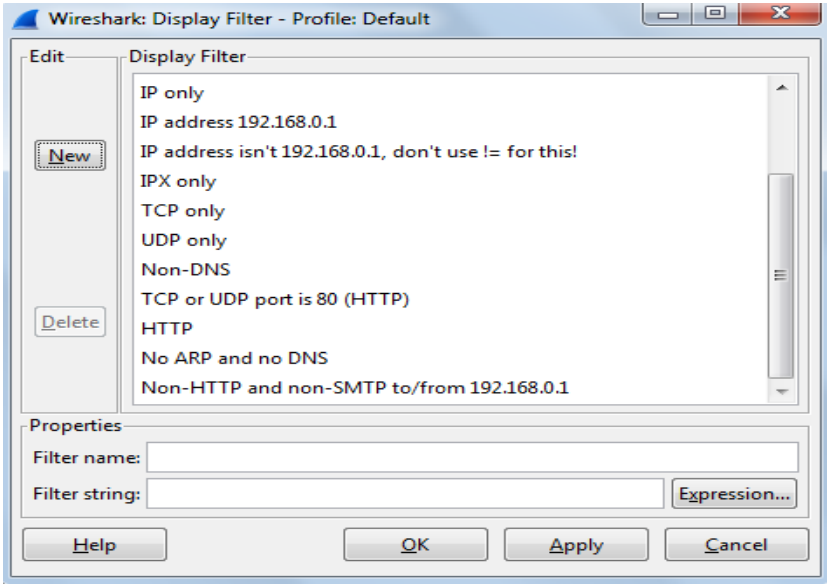


Рис. 2.2. Окно фильтра программы Wireshark

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.

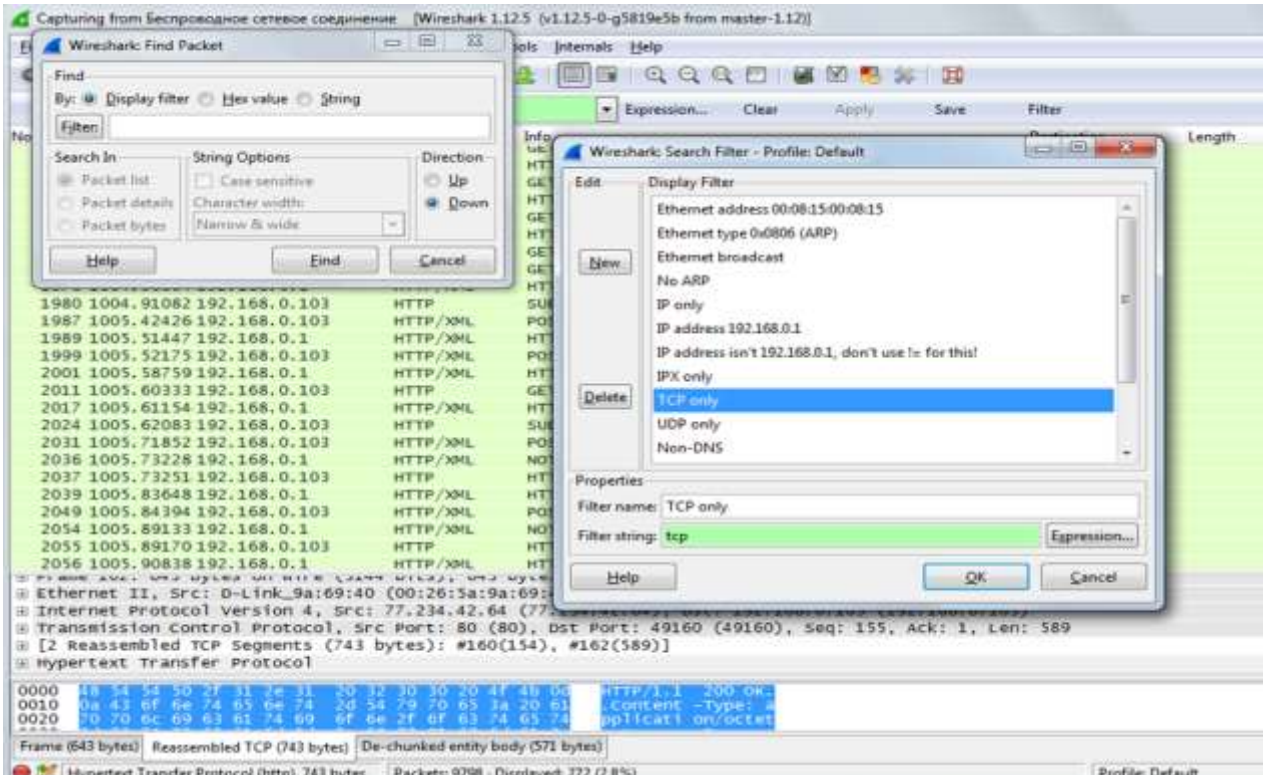


Рис. 2.3. Окно программы поиска пакета через фильтр

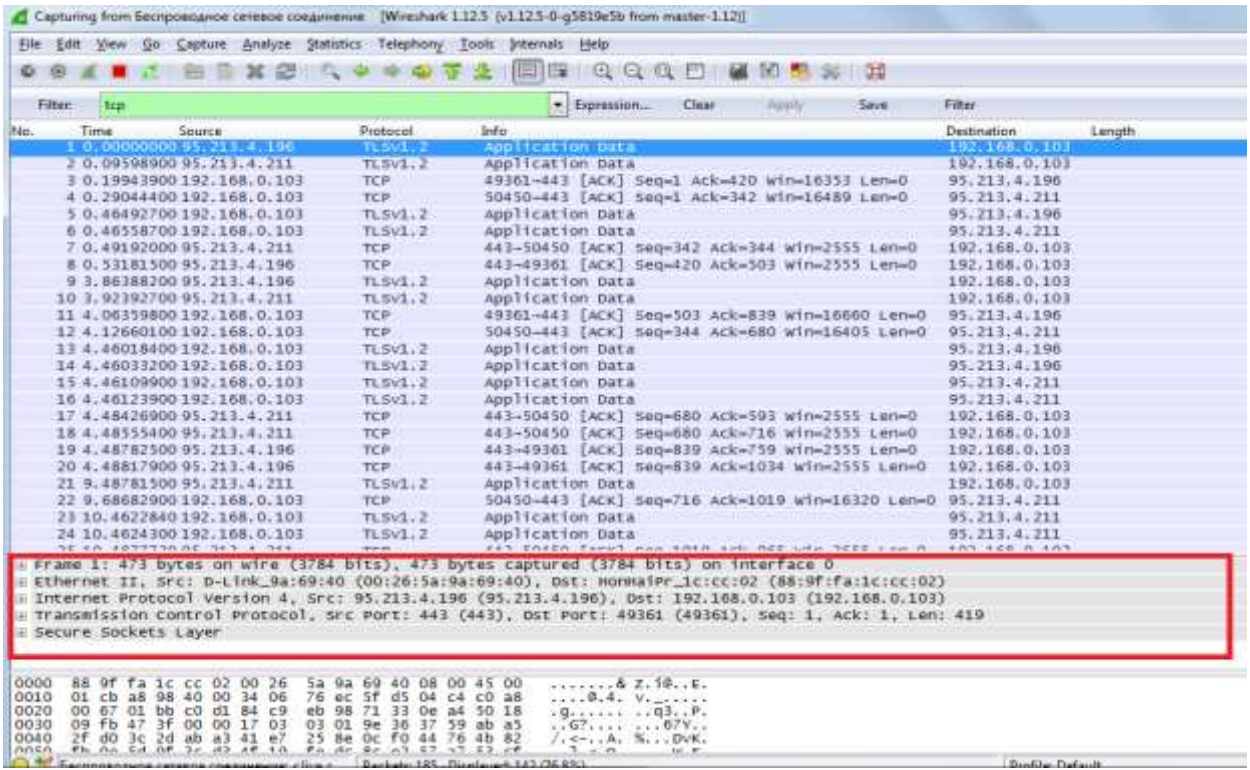


Рис. 2.4. Окно инкапсуляции пакета программы Wireshark

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 «Converstations» (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.

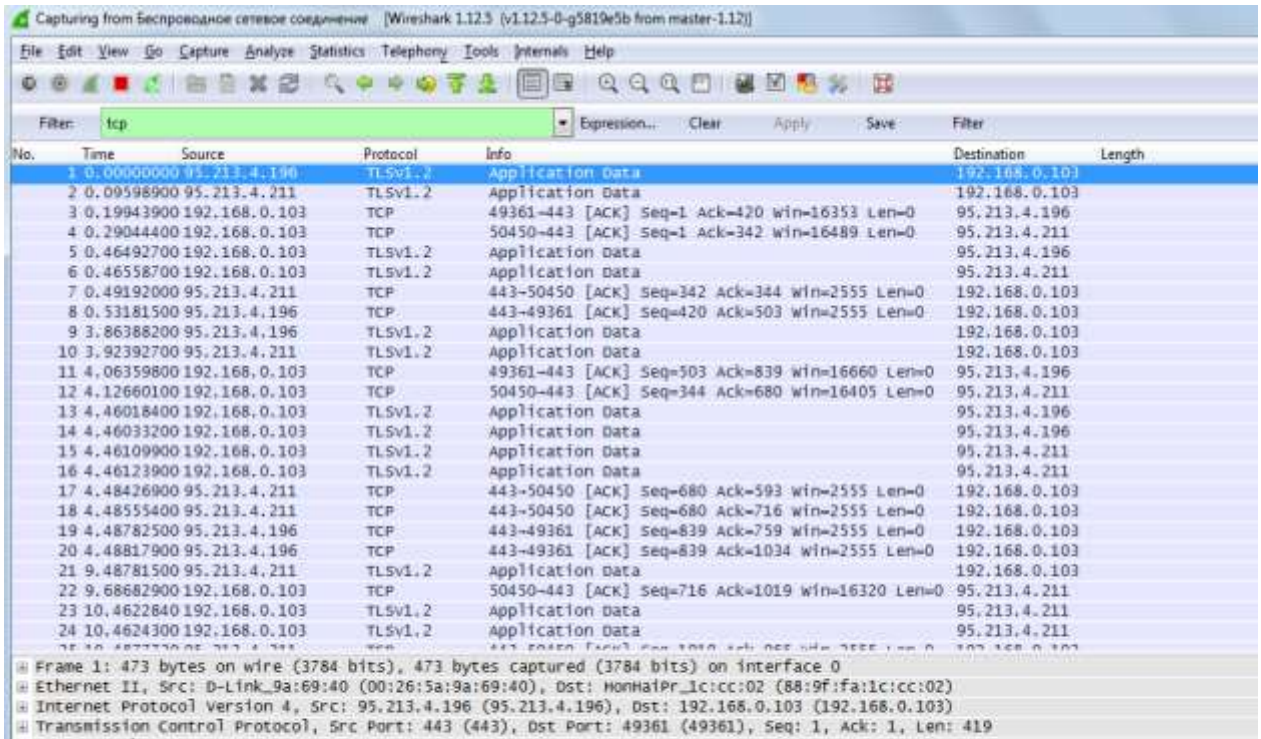


Рис. 2.5. Окно «байты пакетов» программы Wireshark

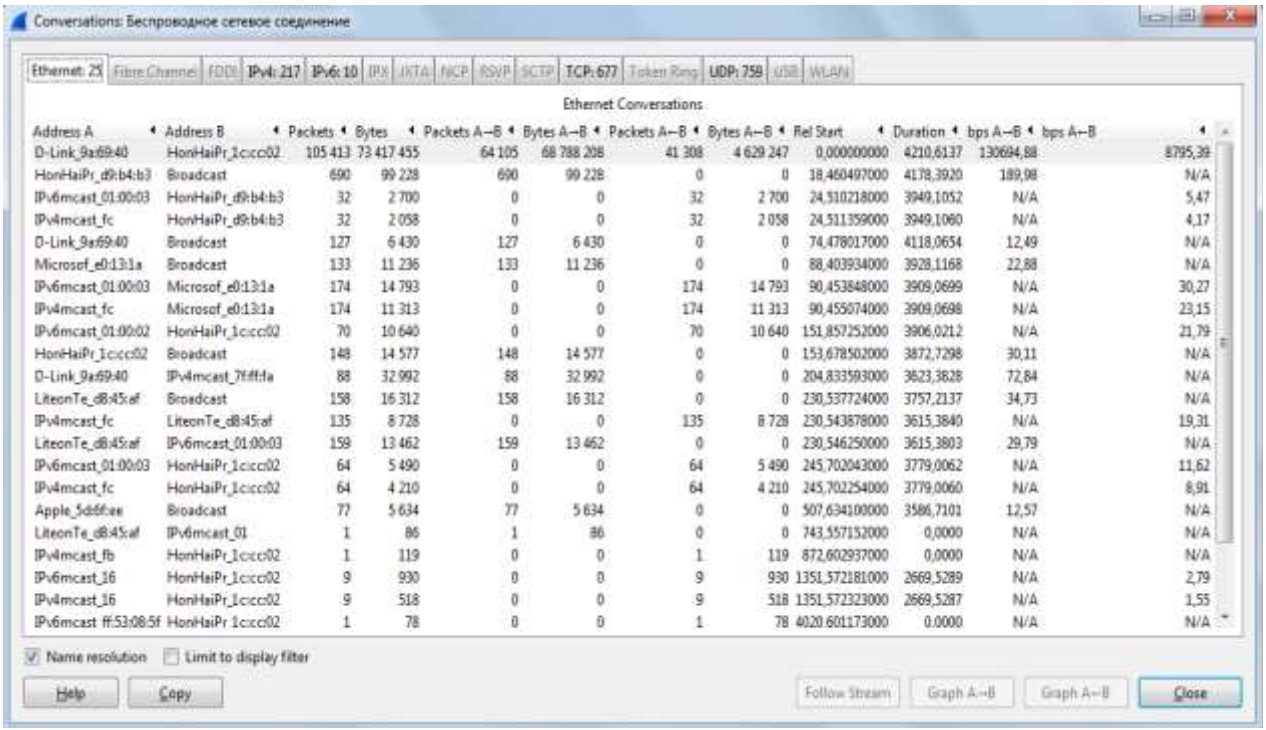


Рис. 2.6. Окно статистики программы Wireshark

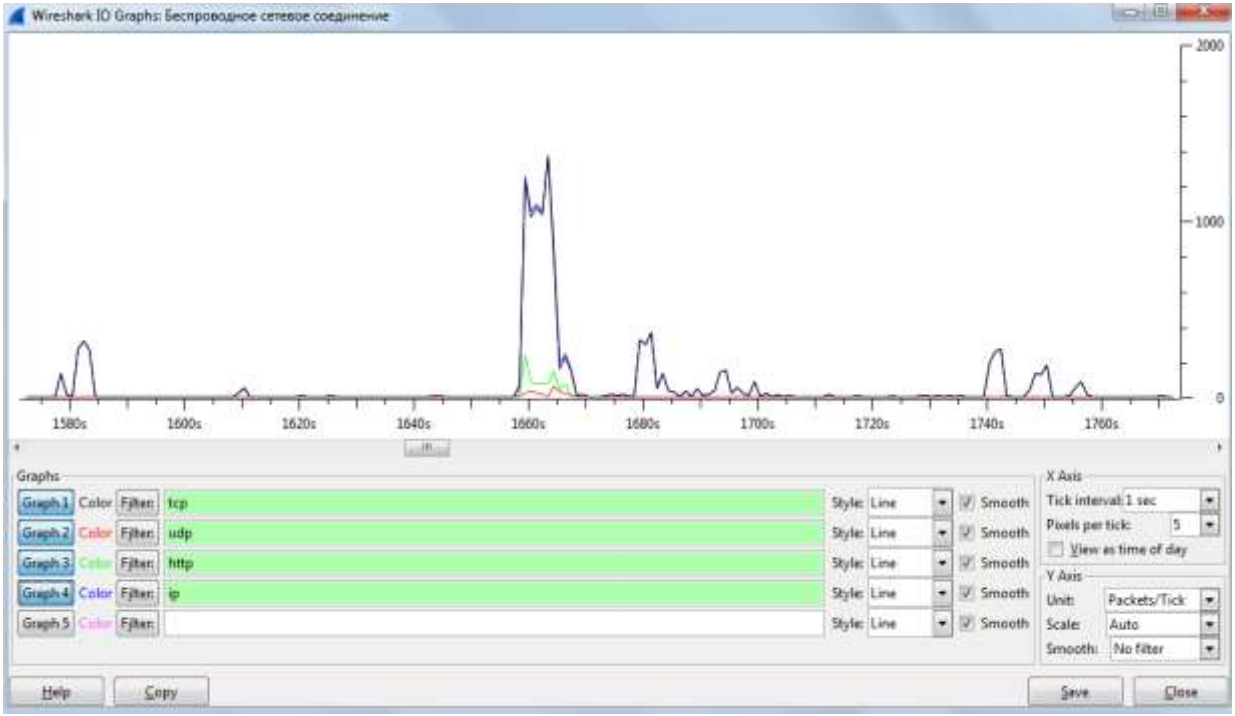


Рис. 2.7. Окно графика зависимости разного типа программы Wireshark

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.

ЛАБОРАТОРНАЯ РАБОТА № 3

Расчет параметров сетевого трафика

Цель работы: на основе собранной статистики из лабораторной работы № 2 осуществить расчет параметров трафика.

Ход работы:

Для данного расчета воспользуемся определением Херста методом R/S статистики. По снятому графику определим параметры, что при дальнейших расчетах определить, является ли трафик самоподобным или нет.

На рис.2.7 в качестве примера представлены результаты моделирования суммарной нагрузки трафика. Продолжительность проведенного моделирования 24 минуты. При желании эта величина может быть увеличена для изучения фрактального характера трафика передачи данных.

Определим значения среднеарифметического по формуле:

$$M = \frac{1}{N}\sum_{i=1}^{N} X_i \,,$$

Определим дисперсию по формуле:

$$S^2 = \frac{1}{N}\sum_{i=1}^{N} (X_i - M)^2 \,,$$

Определим значения колебаний относительно среднего M:

$$D_j = \sum_{k}^{j} X_k - jM \,,$$

Определим диапазон между максимальным и минимальным значением D:

$$R = \max\{D_j\} - \min\{D_j\},$$

Определим коэффициент Херста по формуле:

$$H = \ln(\frac{R}{S}) / \ln(N).$$

Используя значение показателя Херста (H), выделяют три типа случайных процессов:

- H ≤ 0,5 – случайный процесс является антиперсистентным или эргодическим рядом, который не обладает самоподобием;
- H = 0,5 – полный случайный ряд со смещением частицы при классическом броуновском движении;
- H ≥ 0,5 – персистентный (само-поддерживающийся) процесс, который обладает длительной памятью и является самоподобным.

Задание:

- рассчитать математическое ожидание, дисперсию, параметр Херста;
- доказать самоподобие исследуемого трафика;
- сделать выводы по выполненной работе.

ЛАБОРАТОРНАЯ РАБОТА № 4

Определение среднего коэффициента загрузки дуплексного канала передачи сети Fast Ethernet с помощью пакетного анализатора

Цель работы: определить коэффициент загрузки локальной сети при передаче данных от выделенного сервера сразу нескольким рабочим станциям.

Описание схемы измерений

В данной работе необходимо организовать одновременную передачу данных с сервера файлов (S) (рис. 4.1) на рабочие станции (WS). Для этого необходимо одновременно на нескольких станциях запустить процесс копирования ресурса (сетевой папки), размещенного на сервере. Ресурс должен быть достаточного размера. Достаточного означает, что его размер будет достаточным, для того чтобы провести замеры трафика до окончания передачи данных.

При копировании канал от сервера к коммутатору загружен на 100%. Эта нагрузка на выходе коммутатора распределяется по рабочим станциям. Если рабочая станция будет осуществлять и копирование ресурса и сбор всех пакетов, так как пропускная способность канала не может быть больше 100%. Для уменьшения потерь пакетов и увеличения точности измерений в данной работе используется зеркалирование трафика (SPAN). Данная функция осуществляет копирование всех данных,

проходящих через определенный порт коммутатора на «зеркальный» порт. К «зеркальному» порту подключается станция, которая осуществляет захват пакетов.

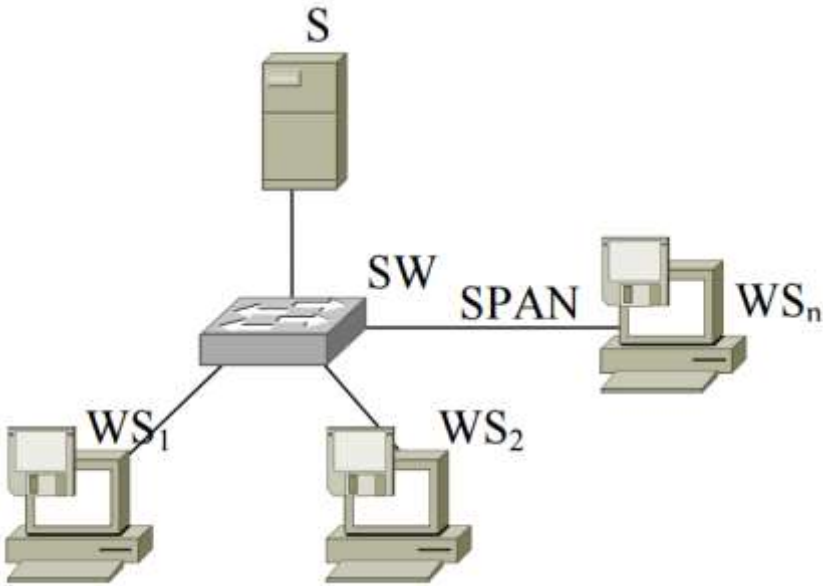


Рис. 4.1. Схема сети передачи данных с сервера

Расчет коэффициента загрузки канала

Коэффициент загрузки канала рассчитывается по формуле:

$$\rho = \frac{\sum \tau_i}{\sum \upsilon_i},$$

где τ_i – время обслуживания i-го кадра;

υ_i – время конца обслуживания i–1 кадра до конца обслуживания i-го кадра.

Известно количество кадров и их размер (в байтах) и время измерения трафика. Тогда, не учитывая задержки среды, суммарное время обслуживания равно:

$$\sum \tau_i = \frac{(L + N \cdot 24) \cdot 8}{B},$$

где L – количество переданных (принятых) байт;

N – количество переданных (принятых) пакетов;

N · 24 – не учтенные Wireshark межкадровый интервал, начальный ограничитель и преамбула;

B – скорость передачи в сети Fast Ethernet (100Мбит/с).

$$\sum \upsilon_i = T,$$

где T – время измерения трафика, тогда

$$\rho = \frac{(L + N \cdot 24) \cdot 8}{BT}.$$

Ход работы

1. На рабочей станции, которая будет осуществлять перехват трафика, запустить программу Wireshark и подготовить ее к сбору трафика;

2. Попросить преподавателя настроить коммутатор на зеркалирование трафика.

3. На двух других рабочих станциях запустить процесс копирования ресурса, указанного преподавателем.

4. После того, как одновременно обе станции начнут получать данные, запустить захват.

5. После окончания захвата копирование отменить.

6. Необходимо выделить одно направление дуплексного канала. Для этого необходимо задать фильтр «ip.src == <IP-адрес отправителя>» – для трафика с IP-адресом источника, «ip.dst == <IP-адрес получателя>» – для трафика с IP-адресом назначения.

7. Получить исходные данные для расчета (Statistics Summary).

8. Произвести расчет и сделать вывод о загрузке канала.

СПИСОК ЛИТЕРАТУРЫ

1. http://www.wireshark.org/ – официальный сайт Wireshark.
2. В. Г. Олифер, Н. А. Олифер. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов. 3-е изд. – СПб.: Питер, 2006.
3. Д. Дэвис, Т. Ли. Microsoft Windows Server 2003. Протоколы и службы TCP/IP. Техническое руководство.

СОДЕРЖАНИЕ

Учебно-методическое издание

Толмачев Петр Николаевич
Ермакова Наталья Анатольевна
Подворный Павел Валерьевич
Сапсай Сергей Александрович

АНАЛИЗАТОР ПРОТОКОЛОВ WIRESHARK

Учебно-методическое пособие
для выполнения лабораторных работ

Формат 60x84 1/16 Тираж 100 экз.
Изд.№ 27-17

Москва, Копировальный центр «PrintSide»