Лабораторная работа №4

**Захват и анализ сетевого трафика**

Целью данной работы является ознакомление с программой «The Wireshark Network analyzer», которая представляет собой программный анализатор протоколов. Программа содержит следую­щие основные компоненты: фильтр захвата, буфер кадров, декодер протоко­лов, фильтр отображения захваченных кадров и модуль статистики с элемен­тами экспертной системы и обладает следующими возможностями:

* возможность захвата трафика в сетевых сегментах различных базовых технологий;
* возможность анализа большого числа протоколов;
* возможность экспорта и импорта файлов данных в формат распространен­ных анализаторов;
* мощная и удобная система поиска и фильтрации информации в буфере пакетов;
* наличие элементов экспертной системы;
* возможность сохранения на диск выделенного фрагмента пакета;
* наличие полезных утилит командной строки для осуществления захвата трафика и обработки сохраненных файлов.

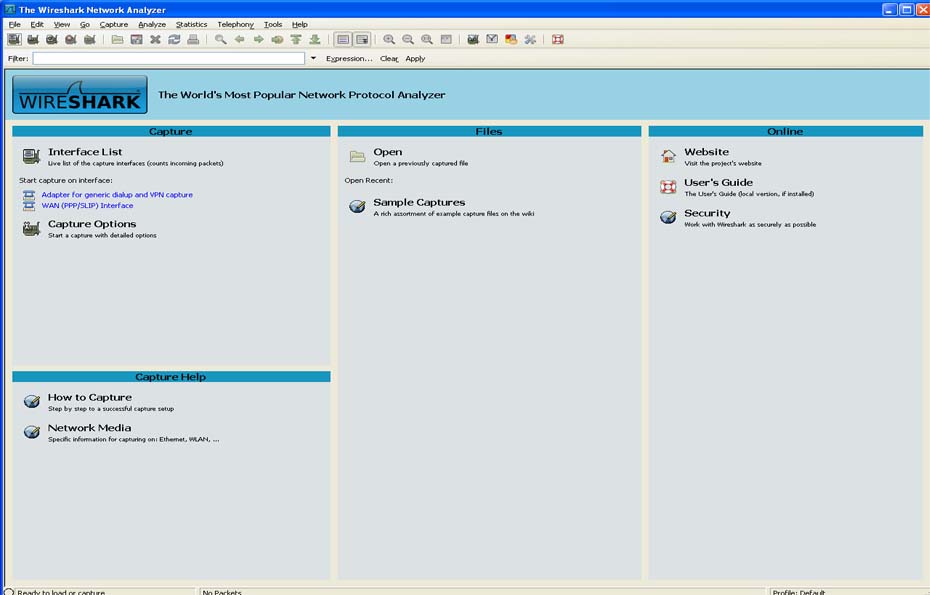


Рис.1 Основной экран программы.

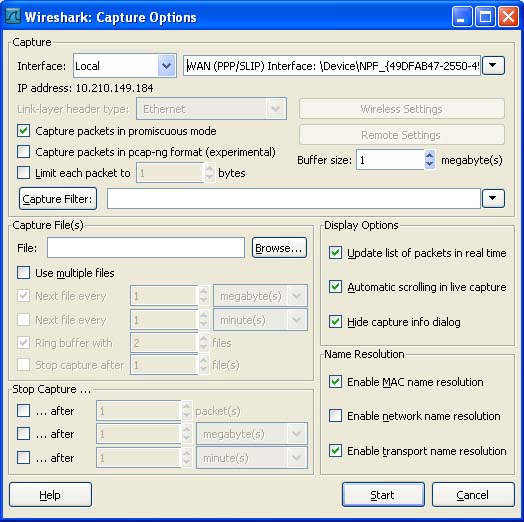


Рис. 2. Окно настроек параметров захвата.

После запуска программы Wireshark (Рис.1.) необходимо настроить некоторые параметры. Сначала необходимо открыть панель меню Capture => Options(Рис.2). На этой панели необходимо

установить следующие парамет­ры захвата кадров:

* Interface - сетевой адаптер;
* Buffer size - размер буфера захвата (по умолчанию 1 Мб);
* Capture packets in promiscuous mode - использование режима беспоря­дочного захвата, если флажок снят, то захватываться будут кадры, предназначенные для указанного сетевого интерфейса;
* Limit each packet to - запись только нескольких первых байт (определя­ется установленным значением параметра) каждого кадра;
* Capture Filter - фильтр захвата, предназначен для фильтрации кадров при записи, увеличивает нагрузку на процессор;
* Capture File(s) - файл захвата;
* Stop Capture - условия автоматического завершения захвата;
* Display Options - отображение пакетов в реальном времени и автомати­ческий скроллинг окна информации:
* Name Resolution - разрешение имен на физическом, сетевом и транс­портном уровнях.

Результат выполнения захвата кадра при выполнении команды «ping mail.ru» приведен на рис.3. На экране монитора в программе присутствует несколько панелей с отображением сетевых пакетов, записанных в буфер. 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.

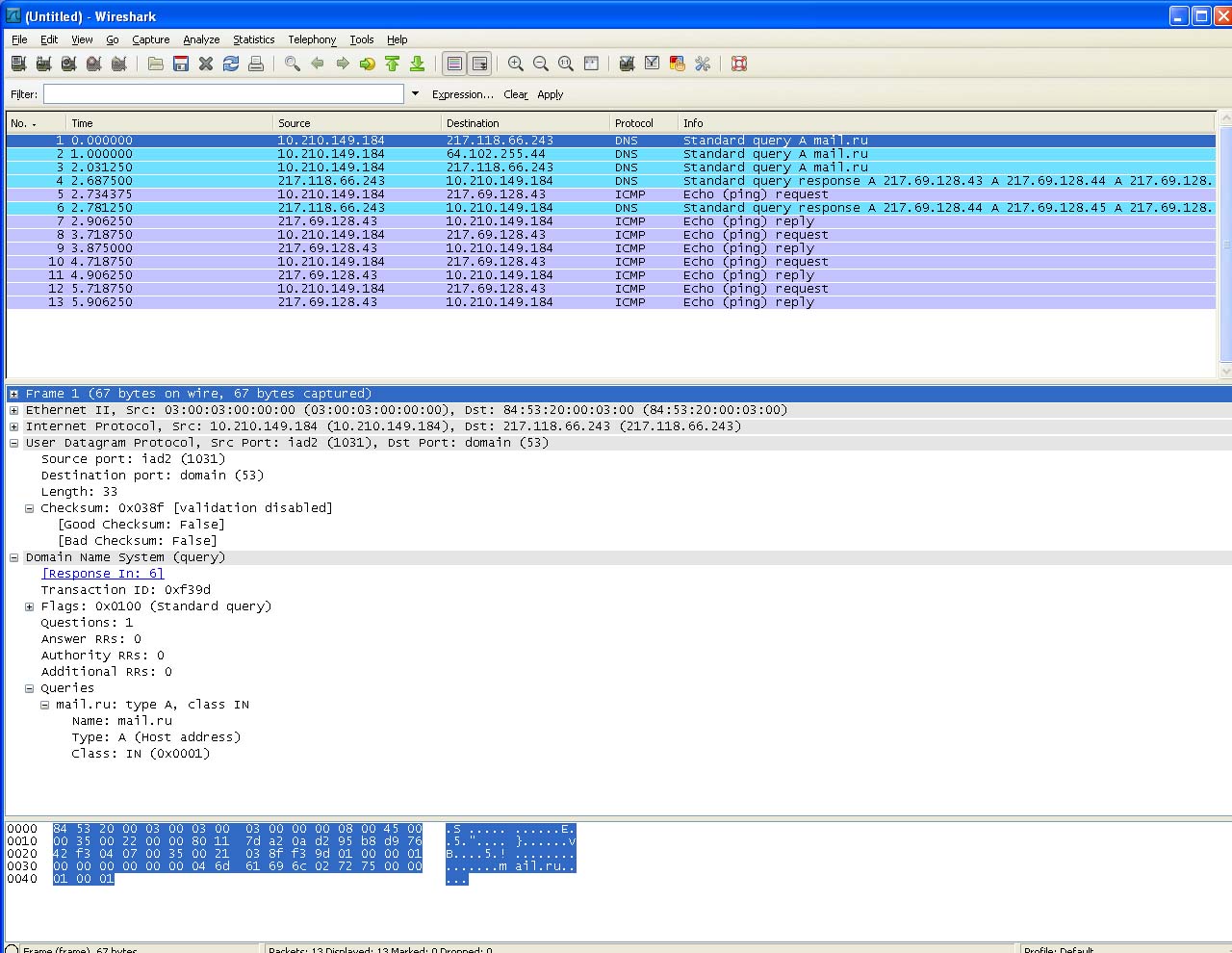


Рис.3. Результат захвата кадра при выполнении команды «ping mail.ru».

Панель со списком пакетов построчно отображает характеристики того или иного пакета (номер по порядку в буфере, время захвата, адреса источни­ка и получателя, тип протокола и общая информация о нем).

В поле Filter используется для фильтрации захваченных данных. Используемыми переменными являются поля заголовков протоколов. Можно создавать довольно сложные условия с использованием операторов “!=”, “==”, “<”, “>”, “>=”, “<=”, а также OR, AND, NOT(!). Например, условие TCP.Flags.SYN == 1 означает отбор всех кадров, в которых протокол TCP осуществляет запрос на установление соединения.

Поиск захваченных кадров можно осуществлять через меню Edit->Find Paket. Фильтр может содержать вышеописанные условия фильтрации, шестнадцатиричный код или данные типа «строка». Поиск может происходить в любой из трех областей – области пакетов, в области расшифровки протоколов пакета или непосредственно в пакете.

В настройках программы можно отключать показ выбранных протоколов с помощью пункта Analyze->Enabled Protocols.

**Задание**

1. Перед выполнение лабораторной работы необходимо повторить механизмы работы и структуру стека протоколов TCP/IP(TCP,IP,ARP,ICMP), протоколы SMTP,POP3.
2. Запустите программу «The Wireshark Network analyzer».
3. Выберите необходимый сетевой интерфейс.
4. Снимите флажок опции «Capture packets in promiscuous mode».
5. Чтобы начать процесс захвата нажми­те на кнопку «Start» (Рис.2) либо на соответствующий значок на панели управления.
6. В командной строке выполните команду ping на любой хост.
7. После завершения команды ping остановите захват, нажав кнопку «Stop».
8. Проанализируйте результаты работы команды, содержимое экрана.
9. Загрузите в программу файл POP3.pcap. В этом файле находятся результаты связи по протоколу POP3 с почтовым сервером mail.ru для учетной записи test0073. Проанализируйте содержимое захваченных пакетов, определите пароль учетной записи. Найдите все пакеты, содержащие имя учетной записи. Отфильтруйте с помощью опции меню сеанс связи из общего потока. Отфильтруйте команду ping на сервер pop3.mail.ru.
10. Загрузите в программу файл SMTP.pcap. В этом файле находятся результаты связи по протоколу SMTP с почтовым сервером mail.ru для учетной записи test0073. Отфильтруйте с помощью опции меню сеанс связи из общего потока.
11. Включите захват кадров, среди захваченных кадров с помощью фильтра оставьте только ICMP-сообщения. Для этого можно в поле фильтр набрать ICMP и применить этот фильтр. Если после набора icmp набрать символ «.», то откроется окно с возможными вариантами дальнейшего выбора параметров второго уровня.
12. Дайте команду ping на какой-либо узел. Установите фильтр для выбора протокола ARP, в поле IP-адрес назначения которого присутствовал бы набранный IP-адрес.
13. Отберите кадры, содержащие в поле «Протокол» IP-протокола протокол ICMP, где адресом назначения является выбранный Вами адрес в команде ping.
14. Найдите все пакеты по строке «request» в области расшифровки протоколов.
15. Захватите кадры при копировании файла размером не менее 10кБ с ftp-сервера. Отключите протоколы, находящиеся выше протокола TCP, оставьте только протокол TCP. Проанализируйте, как изменились области, как фрагментировалась дейтаграмма, сколько TCP-сегментов получилось и какого размера.
16. Захватите кадры при копировании файла 111.txt с ftp-сервера из директории с заданием для данной лабораторной работы. Найдите в захваченных кадрах переданную структуру каталога, имя передаваемого файла, его содержимое.
17. Составьте условия отбора, чтобы определить количество TCP-соединений в захваченных кадрах.
18. Изучите пункт меню Analyze.
19. Откройте статистику сеансов TCP, выберите первый сеанс из меню Apply as Filter -> Selected -> A<->B.