ЛАБОРАТОРНАЯ РАБОТА

«Сбор сетевых данных с помощью программы Wireshark»

Цель работы.

Выполнить сбор сетевого трафика с помощью программы Wireshark, чтобы ознакомиться с интерфейсом и средой Wireshark;

Проанализировать трафик для веб-сервера;

Создать фильтр для ограничения сбора сетевых данных пакетами ICMP.

Отправить эхо-запрос удаленному узлу, чтобы понаблюдать за работой фильтра пакетов ICMP в ходе сбора сетевых данных.

Необходимая подготовка

Знание понятий «пакет», «веб-сервер», «протокол ICMP», «внутриполосное управление», «внеполосное управление»

Дистрибутив программы Wireshark версии 0.99.5 (или самая последняя версия) для используемой ОС, подключение к сети Интернет (не обязательно, но желательно), доступ к командной строке ПК, доступ к сетевой конфигурации TCP/IP ПК.

Предварительные знания

В этой лабораторной работе вы установите программу Wireshark, широко известный анализатор сетевых протоколов и средство мониторинга. Программа Wireshark собирает все пакеты, отправленные или полученные сетевой интерфейсной платой (NIC) компьютера. Ее можно установить либо в лаборатории, либо дома на ПК. Вам он понадобиться для отслеживания и просмотра разных типов сетевых протоколов и трафика. Ранее программа Wireshark была известна под именем Ethereal.

Программа Wireshark поставляется бесплатно и доступна по адресу www.wireshark.org.

Ход работы

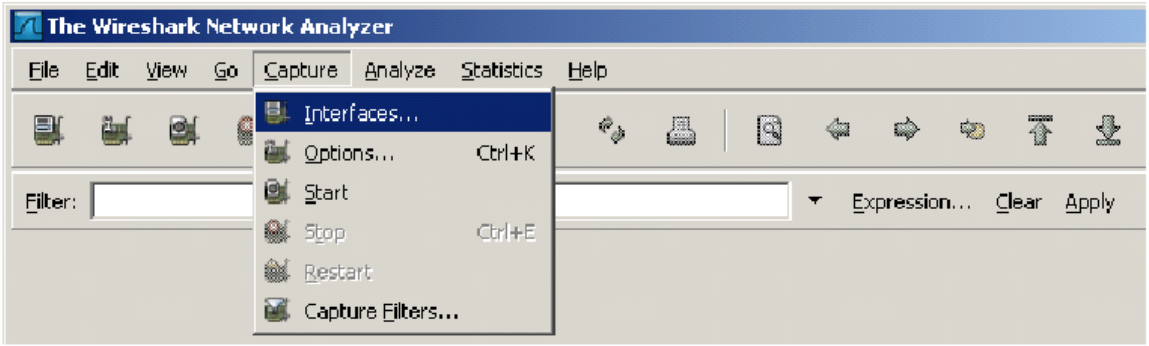
Мониторинг сети при помощи программы Wireshark

Шаг 1. Установка и запуск программы Wireshark

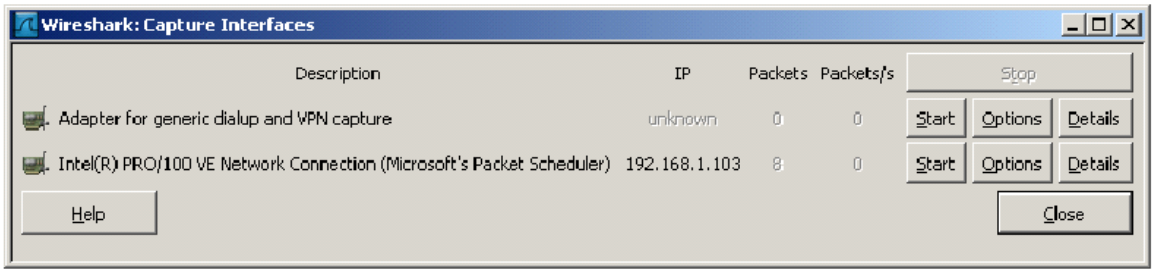
Шаг 2. Выбор интерфейса для сбора пакетов

а. Запустите приложение Wireshark.

б. В меню Capture (сбор) выберите пункт Interfaces (интерфейсы).



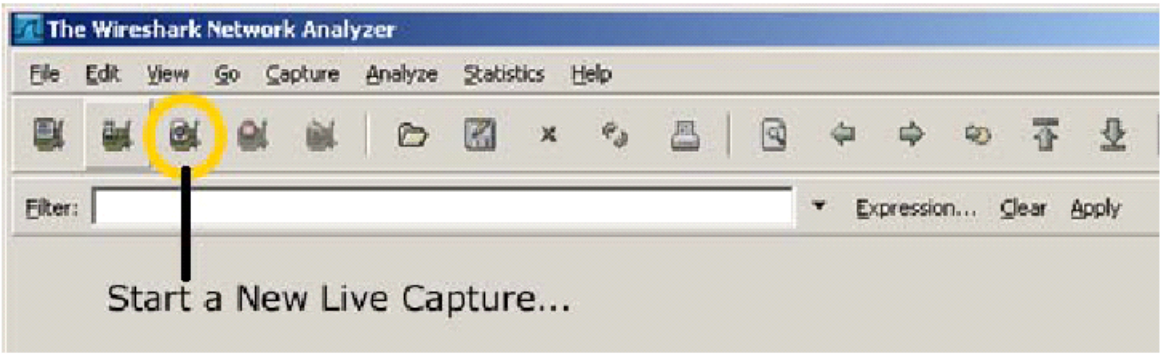
в. Нажмите кнопку Start (пуск) для интерфейса Ethernet (NIC), который требуется использовать для сбора сетевого трафика.



Шаг 3. Запуск сбора сетевых данных

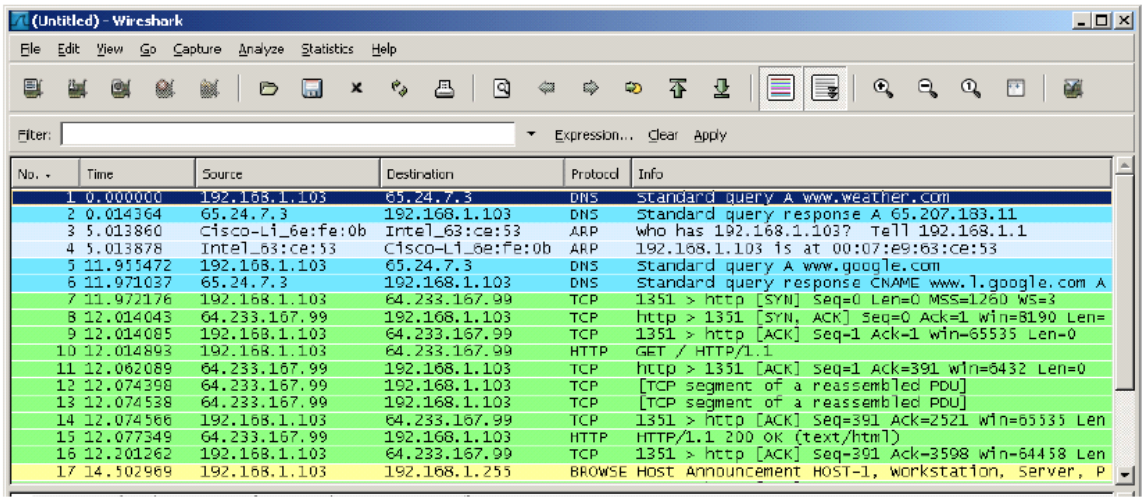
а. Прокрутите меню и просмотрите панель инструментов в интерфейсе запуска Wireshark.

б. Нажмите кнопку New Live Capture (новый сбор динамических данных) и просмотрите сведения, собранные Wireshark. Пусть сбор данных продолжается в течение нескольких минут, чтобы вы могли понаблюдать за различными типами трафика в сети.



Шаг 4. Анализ сведений о веб-трафике

а. Если существует подключение к сети Интернет, откройте веб-обозреватель и перейдите в узел www.google.com. Сверните окно Google и вернитесь в Wireshark. Должен быть отображен трафик, схожий с тем, что представлен ниже. Найдите столбцы Source, Destination и Protocol (источник, адрес назначения и протокол) на экране Wireshark.



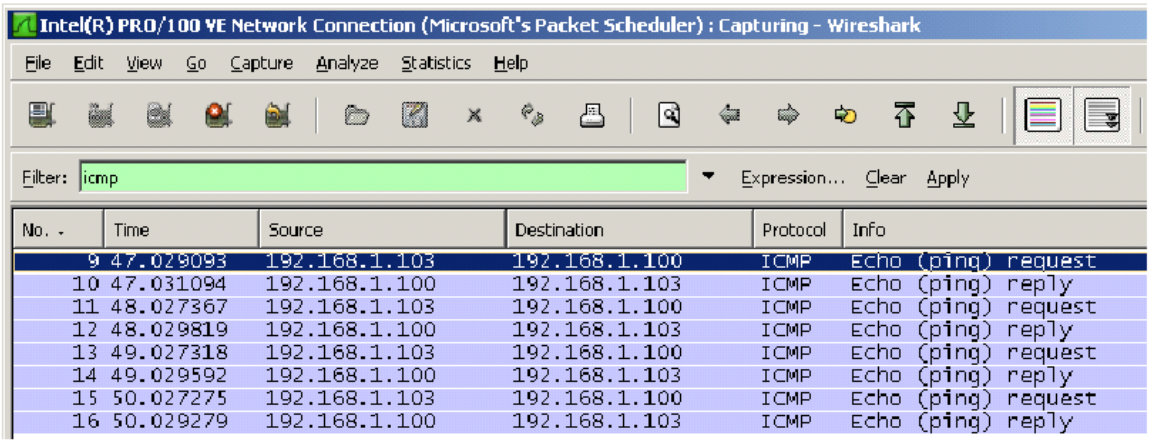
Подключение к серверу Google начнется с отправки запроса на DNS-сервер для поиска IP-адреса сервера. IP-адрес сервера назначения, по всей вероятности, начнется с 64.x.x.x. Каковы источник и адрес назначения первого пакета, отправленного на сервер Google?

Шаг 5. Фильтрация сбора сетевых данных

а. Откройте окно командной строки, выбрав Start > All Programs > Run (пуск > программы > выполнить) и введя cmd. Либо щелкните Start > All Programs > Accessories (пуск > все программы > стандартные > командная строка).

б. Отправьте эхо-запрос по IP-адресу узла в вашей локальной сети и понаблюдайте за процессами в окне сбора Wireshark. Прокрутите вниз и вверх окно, в котором отображается трафик. Какие используются типы протоколов?

в. В текстовом поле Filter (фильтр) введите icmp и щелкните Apply (применить). Протокол управления сообщениями в Интернет (ICMP) — это протокол, используемый эхо-запросом для проверки сетевого подключения к другому узлу.


Intel(R) PRO/100 VE Network Connection (Microsoft's Packet Scheduler) : Capturing - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: icmp
Expression... Clear Apply
No. Time Source Destination Protocol Info
9 47.029093 192.168.1.103 192.168.1.100 ICMP Echo (ping) request
10 47.031094 192.168.1.100 192.168.1.103 ICMP Echo (ping) reply
11 48.027367 192.168.1.103 192.168.1.100 ICMP Echo (ping) request
12 48.029819 192.168.1.100 192.168.1.103 ICMP Echo (ping) reply
13 49.027318 192.168.1.103 192.168.1.100 ICMP Echo (ping) request
14 49.029592 192.168.1.100 192.168.1.103 ICMP Echo (ping) reply
15 50.027275 192.168.1.103 192.168.1.100 ICMP Echo (ping) request
16 50.029279 192.168.1.100 192.168.1.103 ICMP Echo (ping) reply