

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 понадобится 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

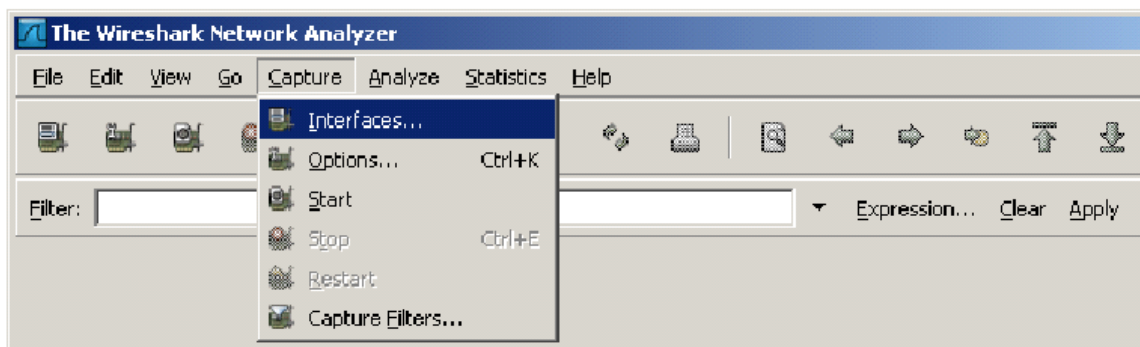
Мониторинг сети при помощи программы Wireshark

Шаг 1. Установка и запуск программы Wireshark

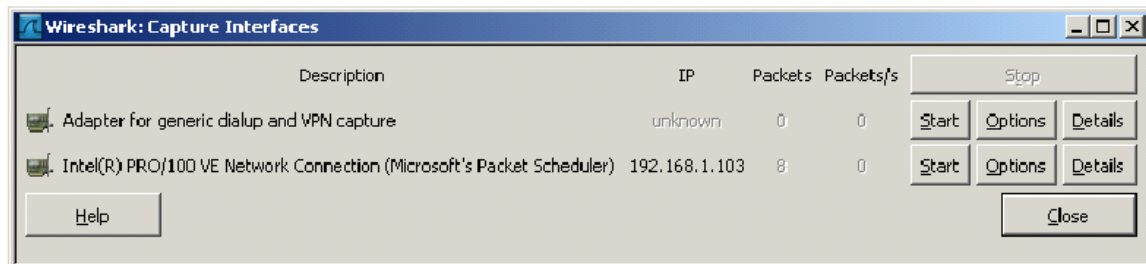
Шаг 2. Выбор интерфейса для сбора пакетов

а. Запустите приложение Wireshark.

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



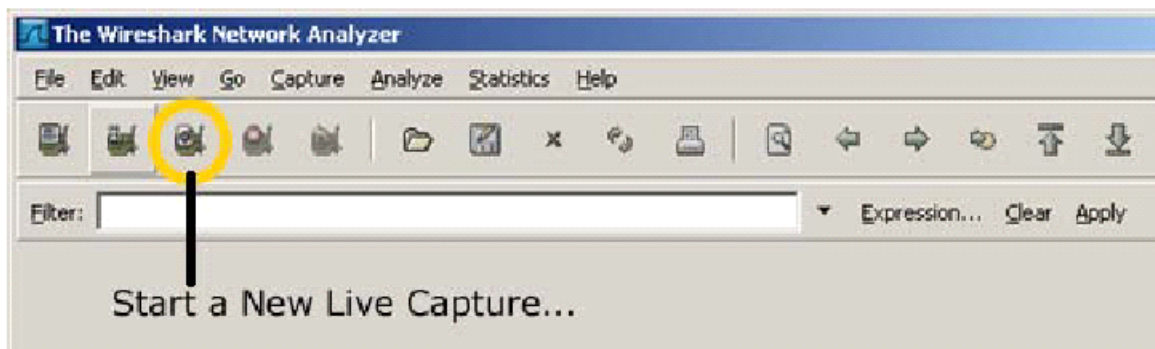
в. Нажмите кнопку Start (пуск) для интерфейса Ethernet (NIC), который требуется использовать для сбора сетевого трафика.



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.

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.103	65.24.7.3	DNS	Standard query A www.weather.com
2	0.014364	65.24.7.3	192.168.1.103	DNS	Standard query response A 65.207.183.11
3	5.013860	Cisco-L1_6e:fe:0b	Intel_63:ce:53	ARP	who has 192.168.1.103? Tell 192.168.1.1
4	5.013878	Intel_63:ce:53	Cisco-L1_6e:fe:0b	ARP	192.168.1.103 is at 00:07:e9:63:ce:53
5	11.955472	192.168.1.103	65.24.7.3	DNS	Standard query A www.google.com
6	11.971037	65.24.7.3	192.168.1.103	DNS	Standard query response CNAME www.l.google.com A
7	11.972176	192.168.1.103	64.233.167.99	TCP	1351 > http [SYN] Seq=0 Len=0 MSS=1260 WS=3
8	12.014043	64.233.167.99	192.168.1.103	TCP	http > 1351 [SYN, ACK] Seq=0 Ack=1 win=6190 Len=
9	12.014085	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=1 Ack=1 win=65535 Len=0
10	12.014893	192.168.1.103	64.233.167.99	HTTP	GET / HTTP/1.1
11	12.062089	64.233.167.99	192.168.1.103	TCP	http > 1351 [ACK] Seq=1 Ack=391 win=6432 Len=0
12	12.074398	64.233.167.99	192.168.1.103	TCP	[TCP segment of a reassembled PDU]
13	12.074538	64.233.167.99	192.168.1.103	TCP	[TCP segment of a reassembled PDU]
14	12.074566	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=391 Ack=2521 win=65535 Len=
15	12.077349	64.233.167.99	192.168.1.103	HTTP	HTTP/1.1 200 OK (text/html)
16	12.201262	192.168.1.103	64.233.167.99	TCP	1351 > http [ACK] Seq=391 Ack=3598 win=64458 Len=
17	14.502969	192.168.1.103	192.168.1.255	BROWSE	Host Announcement HOST-1, workstation, Server, P

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