

ЛАБОРАТОРНАЯ РАБОТА. МОНИТОРИНГ СЕТИ

Цель работы

Освоить базовые навыки мониторинга сети с использованием программ для анализа протоколов.

Основные понятия: мониторинг сети, захват пакетов, реассемблирование пакетов, количественные характеристики работоспособности сети, анализ трафика, качественные характеристики сети, tcpdump, Ethereal Network Analyzer, Wireshark, NetMon.

Под мониторингом сети понимают процесс сбора и анализа сетевого трафика, по результатам которого можно судить об эффективности работы всей сети или ее отдельных компонентов.

Для мониторинга используют специальные программы - анализаторы сети. Таких программ много, например Windows Network Monitor, tcpdump, Ethereal Network Analyzer (ENA), Wireshark и т.п. Они схожи по функциям, а отличаются в основном пользовательским интерфейсом и возможностями генерации статистических отчетов. На рис. 2.1 приведены примеры таких программ.

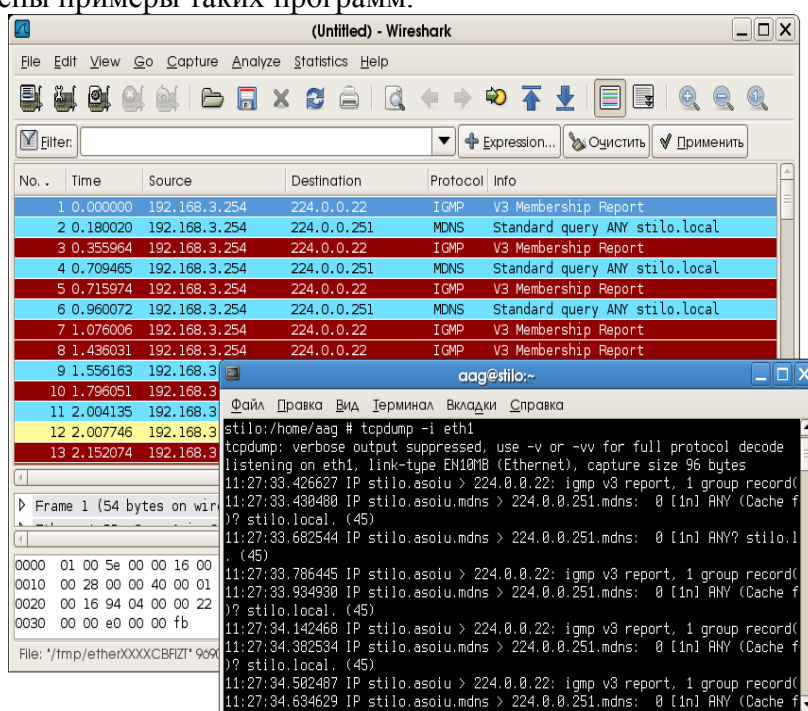


Рис.2.1. Программы анализа трафика. Главное окно программы Wireshark с результатами захвата и программа tcpdump (в консоли).

Для выполнения этой работы рекомендуется использовать программы Ethereal Network Analyzer или Wireshark (версии для UNIX/Linux, Windows-версия работает не стабильно). Эти программы практически идентичны как по возможностям, так и по использованию.

Указания к работе

- Установить (если не установлена ранее) программу анализа трафика.
 - [Ethereal Network Analyzer for Windows \(WinENA\)](#)+библиотека [WinPcap](#) для [WinENA](#)
 - [Ethereal Network Analyzer\(.rpm\)](#)
- Запустить программу (требуется права суперпользователя) и ознакомиться с пользовательским интерфейсом и основными пунктами меню.

Задания к работе

1. Запустить ENA в режиме захвата трафика, проходящего через интерфейс, подключенный к локальной сети (обычно это eth0). Перейти к следующему заданию.

2. Эмулировать сетевую активность в течении 10-15 минут. Для этого можно выполнить, например, некоторые из указанных действий (на выбор).
 - Открыть сайт <http://rtos.asoiu>;
 - Подключиться к серверу <ftp://telecom.asoiu>;
 - Выполнить пинг любых узлов;
 - Подключиться к одному из доступных сетевых дисков Windows (если такие ресурсы представлены в сети)
 - Открыть сайт <http://telecom.asoiu>;
 - Выполнить прочие действия, требующие сетевого подключения.
3. Остановить захват.
4. Заполнить таблицу 2.1. Исходные данные для таблицы представлены в отчете [Statistics/Summary](#). При заполнении таблицы обратите внимание на соблюдение размерности величин (кб, Мб, Мбит).

Таблица 2.1.

Параметр	Значение
Время захвата, мин	
К-во захваченных пакетов	
Объем, Мб	
Средн.размер пакета, Кб	
Средняя скорость, пакетов/сек	
Средняя скорость, Мбит/сек	

5. Составить таблицу распределения трафика по протоколам (табл. 2.2). Исходные данные для таблицы можно получить из отчета [Statistics/Protocol Hierarchy](#).

Таблица 2.2.

Протокол	Трафик, Мб	Трафик, %
HTTP		
FTP		
...		
ИТОГО		100

6. Составить таблицу распределения Ethernet-трафика по узлам сети (табл. 2.3). Исходные данные для заполнения таблицы получить из отчета [Statistics/Endpoint list/Ethernet](#).

Таблица 2.3.

MAC-адрес	IP-адрес	Трафик					
		входящий		исходящий		общий	
		Мб	%	Мб	%	Мб	%
ИТОГО			100		100		100

7. По данным табл. 2.1 определить *относительную загрузку* сети (в %) за контрольный период времени по формуле:

$$\text{Загрузка} = \frac{(\text{Трафик, Мбит} / \text{Время, сек}) \cdot 100}{(\text{Пропускная способность, Мбит/сек})}$$

8. По данным табл. 2.2 сделать выводы о качественном составе трафика, т.е. о соотношении *прикладных служебных* протоколов.
9. По данным табл. 2.3 определить, какие из узлов являются наиболее загруженными с учетом направления трафика (исходящий, входящий, общий).

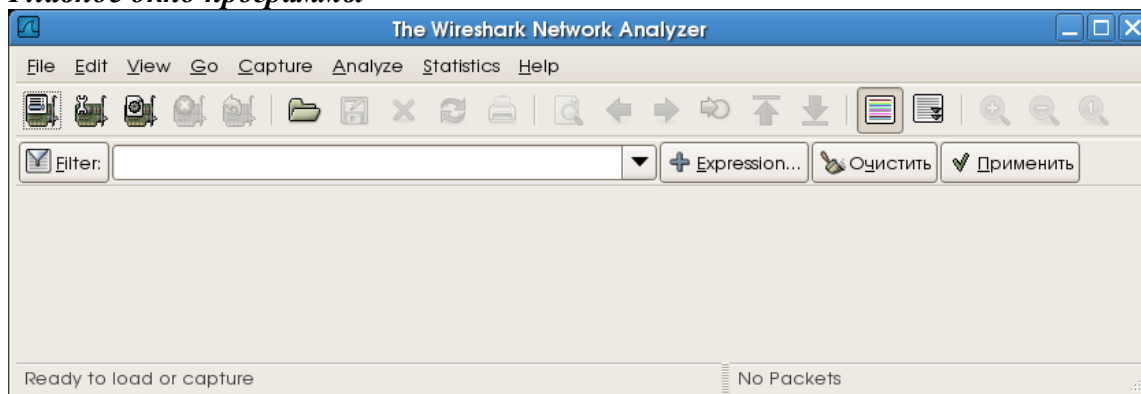
WIRESHARK NETWORK ANALYZER

Wireshark (практически полный аналог **Ethereal Network Analyzer**)- это сетевой анализатор с графическим интерфейсом. Она позволяет в интерактивном режиме просматривать пакеты, передаваемые по сети или анализировать ранее захваченные пакеты, загрузив их из сохраненного файла. Основной формат файла Wireshark такой же, как у libpcap, но поддерживаются и другие форматы.

Wireshark может читать/импортировать следующие форматы:

- libpcap, tcpdump и другие, использующие формат tcpdump
- snoop и atmsnoop
- Shomiti/Finisar Surveyor captures
- Novell LANalyzer captures
- Microsoft Network Monitor captures
- AIX's iptrace captures
- Cinco Networks NetXRay captures
- Network Associates Windows-based Sniffer captures
- Network General/Network Associates DOS-based Sniffer (compressed or uncompressed) captures
- AG Group/WildPackets EtherPeek/TokenPeek/AiroPeek/EtherHelp/Packet-Grabber captures
- RADCOM's WAN/LAN analyzer captures
- Network Instruments Observer version 9 captures
- Lucent/Ascend router debug output
- files from HP-UX's nettl
- Toshiba's ISDN routers dump output
- the output from i4btrace from the ISDN4BSD project
- traces from the EyeSDN USB S0.
- the output in IPLog format from the Cisco Secure Intrusion Detection System
- pppd logs (pppdump format)
- the output from VMS's TCPIPtrace/TCPtrace/UCX\$TRACE utilities
- the text output from the DBS Etherwatch VMS utility
- Visual Networks' Visual UpTime traffic capture
- the output from CoSine L2 debug
- the output from Accellent's 5Views LAN agents
- Endace Measurement Systems' ERF format captures
- Linux Bluez Bluetooth stack hcidump -w traces
- Catapult DCT2000 .out files

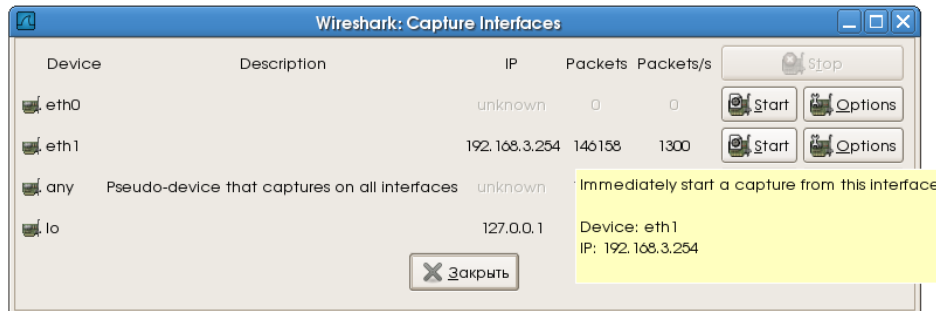
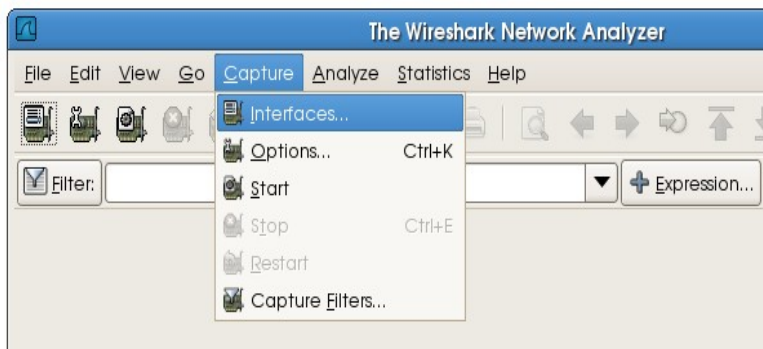
Главное окно программы



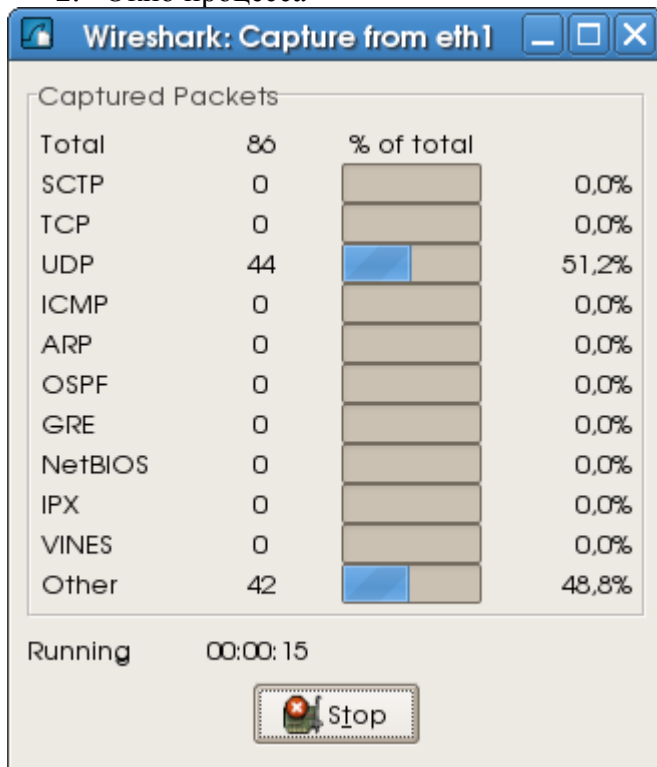
Захват пакетов

Все опции захвата доступны через меню Capture

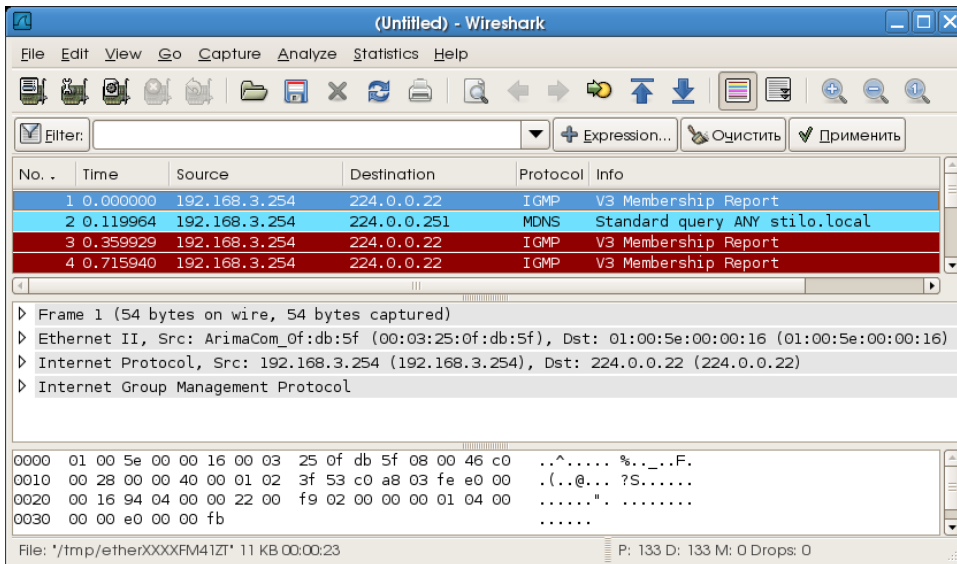
1. Выбор интерфейса (Capture/Interfaces)



2. Окно процесса



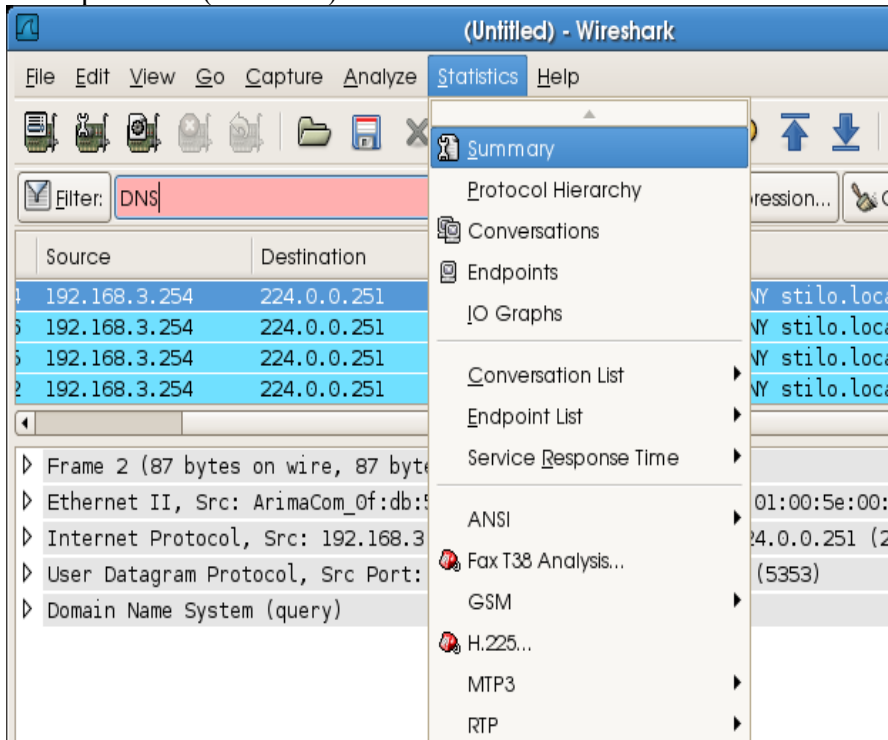
3. Остановка захвата и загрузка результатов



Статистика

Типовые отчеты об использовании сети доступны через меню Statistics. Ниже приведены примеры отображения различных отчетов.

1. Выбор отчета (Statistics)



2. Общая статистика (меню Statistics/Summary)

Wireshark: Summary

File

Name: /tmp/etherXXXXFM41ZT
Length: 11512 bytes
Format: Wireshark/tcpdump/... - libpcap
Packet size limit: 65535 bytes

Time

First packet: 2007-10-01 12:57:48
Last packet: 2007-10-01 12:58:11
Elapsed: 00:00:23

Capture

Interface: eth1
Dropped packets: 0
Capture filter: none

Display

Display filter: udp
Marked packets: 0

Traffic	Captured	Displayed
Between first and last packet	23,329 sec	22,993 sec
Packets	133	66
Avg. packets/sec	5,701	2,870
Avg. packet size	70,000 bytes	87,000 bytes
Bytes	9360	5742
Avg. bytes/sec	401,211	249,723
Avg. MBit/sec	0,003	0,002

✕ Закрыть

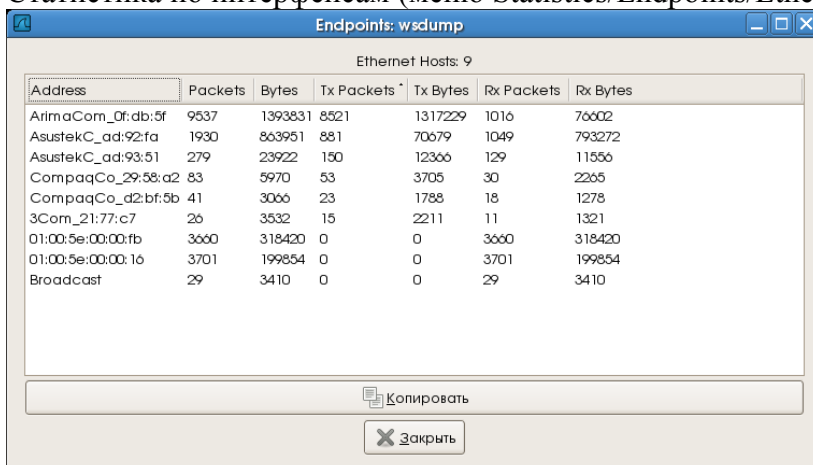
3. Статистика по протоколам (меню Statistics/Protocol Hierarchy)

Wireshark: Protocol Hierarchy Statistics

Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mb
Frame	100,00%	66	5742	0,002	0	0	0
Ethernet	100,00%	66	5742	0,002	0	0	0
Internet Protocol	100,00%	66	5742	0,002	0	0	0
User Datagram Protocol	100,00%	66	5742	0,002	0	0	0
Domain Name Service	100,00%	66	5742	0,002	66	5742	0

OK

4. Статистика по интерфейсам (меню Statistics/Endpoints/Ethernet)



The screenshot shows a window titled "Endpoints: wsdump" with a sub-header "Ethernet Hosts: 9". It contains a table with 7 columns: Address, Packets, Bytes, Tx Packets, Tx Bytes, Rx Packets, and Rx Bytes. The data is as follows:

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
ArimaCom_of:db:5f	9537	1393831	8521	1317229	1016	76602
AsustekC_ad:92:fa	1930	863951	881	70679	1049	793272
AsustekC_ad:93:51	279	23922	150	12366	129	11556
CompaqCo_29:58:a2	83	5970	53	3705	30	2265
CompaqCo_d2:bf:5b	41	3066	23	1788	18	1278
3Com_21:77:c7	26	3532	15	2211	11	1321
01:00:5e:00:00:fb	3660	318420	0	0	3660	318420
01:00:5e:00:00:16	3701	199854	0	0	3701	199854
Broadcast	29	3410	0	0	29	3410

At the bottom of the window, there are two buttons: "Копировать" (Copy) and "Закреть" (Close).