Лабораторная работа #2

Анализ сетевого трафика с помощью программы «Wireshark». Содержание

Этапы выполнения работы	2
Теория	7
Начальная настройка программы и запуск захвата трафика.	7
Главное рабочее окно программы.	
Панель инструментов	11
Фильтр	12
Построение фильтров	
Поле списка захваченных PDU	
Информационное поле.	
Интерпретация вложенных списков.	

Этапы выполнения работы

1. Запустить программу Wireshark.

Для запуска программы необходимо нажать: Пуск > Программы > Wireshark, либо два раза щёлкнуть левой кнопкой мыши по ярлыку программы на рабочем столе.

2. Настроить параметры захвата сетевого трафика.

Для настройки параметров захвата сетевого трафика необходимо:

2.1 Щелчком левой кнопки мыши по кнопке Capture Options вызвать меню настроек.



2.2 Установить параметры в соответствии с рисунком 2.

😃 Wireshark: Ca	pture Opti	ons	
Capture			
Interface: Local		 Attansic AtcL001 Giga 	abit Ethernet Controller (Microsoft's Pacl 💌
IP address: 10.14	4.39.224		
Link-layer header type: Ethernet		emet	(Wireless Settings
Capture packe	Capture packets in promiscuous mode		Remote Settings
Capture packe	ts in pcap-n ket to 1	g format (experimental) bytes	Buffer size: 1 Regabyte(s)
Capture Filter:			
Capture File(s)			Display Options
File:		Browse	
Use <u>m</u> ultiple fil	es		
💌 Next file every	/ 1	🗘 megabyte(s) .	Automatic scrolling in live capture
Next file every	/ 1	🗘 minute(s)	Hide capture info dialog
Ring buffer wi	th 2	C files	Name Despiration
Stop capture a	ifter 1	🗘 file(s)	
Chan Canhuna			Enable MAC name resolution
scop Capcure			
after		c packet(s)	Enable network name resolution
after 1		<pre>packet(s) megabyte(s)</pre>	Enable network name resolution

Следующие опции должны быть активированы:

- Capture packets in promiscuous mode.
- Update list of packets in real time
- Automatic scrolling in live capture
- Enable MAC name resolution
- Enable network name resolution

В качестве интерфейса, используемого для захвата трафика выбрать физический (не виртуальный) адаптер и установить тип адаптера **Local**.

3. Запустить процесс захвата трафика.

Для запуска процесса необходимо нажать кнопку Start в меню настроек.

4. Настроить фильтрацию вывода по протоколам DNS и HTTP.

Для настройки фильтрации необходимо:

4.1 Ввести в поле фильтра выражение: "dns || http".

Filter:	dns http	-	Expression	Clear	Apply
---------	-------------	---	------------	-------	-------

4.2 Нажать кнопку **Apply**.

5. Запустить обновление для антивируса Avira.

Для запуска обновления антивируса необходимо:

5.1 Навести мышь на значок антивируса, который расположен в правом нижнем углу экрана.



5.2 Щёлкнуть по значку правой кнопкой мыши и в появившемся меню выбрать опцию обновить сейчас.

 AntiVir Guard включен 	-
Запустить AntiVir Настройка AntiVir	
Обновить сейчас	100
Справка Avira в Internet	30 JANUARY

6. Остановить захват трафика.

Для того чтобы остановить захват трафика, необходимо нажать кнопку Stop ^н на панели инструментов, либо нажать Capture > Stop.

7. Проанализировать трафик, захваченный программой.

При анализе трафика необходимо произвести следующие действия:

7.1 Среди PDU, захваченных программой, найти **DNS-запрос** (query) и **DNS-ответ** (query response).



7.3 Среди PDU, захваченных программой, найти HTTP-запрос (HTTP GET).

HTTP GET http://80.190.143.233/update/idx/wks_avira-win32-en-pecl.info.

- **7.4** Посмотрев содержимое PDU выяснить и записать в отчёт следующую информацию:
 - Сетевой адрес сервера обновлений.
 - •Данные о вашем компьютере, которые программа обновления передала на сервер: версию Windows, месторасположение компьютера (Страна).

```
B Frame 45 (400 bytes on wire, 400 bytes captured)
B Ethernet II, Src: Foxconn_be:59:fc (00:01:6c:be:59:fc), Dst: Intel_bf:bc:19 (00:04:23:bf:bc:19)
B Internet Protocol, Src: 172.16.1.10 (172.16.1.10), Dst: tessie.mitht.rssi.ru (193.232.216.7)
B Transmission Control Protocol, Src Port: 2973 (2973), Dst Port: 3128 (3128), Seq: 1074, Ack: 14132, Len: 346
B Hypertext Transfer Protocol
B GET http://80.190.143.233/update/idx/vdf.info.gz HTTP/1.0\r\n
Pragma: no-cache\r\n
Cache-Control: no-store, no-cache, must-revalidate\r\n
Host: personal.avira-update.com\r\n
User-Agent: Antivir-NGUpd/9.0.0.52 (PERS; WKS; EN; AVE 8.2.1.150; VDF 7.10.3.62; Windows 2000; Service Pack 4; Russia; Proxy-Connection: Keep-Alive\r\n
\r\n
```

7.5 Изучив содержимое **DNS-запроса**, **HTTP-запрос** и **DNS-ответа** выяснить и записать в отчёт следующую информацию:

- Сетевой адрес компьютера.
- МАС-адрес компьютера.
- •Сетевой адрес шлюза.
- МАС-адрес шлюза.
- ІР-адрес прокси-сервера

- DNS имя прокси-сервера.
- Сетевой адрес DNS-сервера.
- Протокол транспортного уровня, который использует сервис DNS.
- Порт, на который осуществляется DNS-запрос.
- •Протокол транспортного уровня, который использует протокол HTTP.
- •Порт, на который осуществляется запрос обновления антивируса по протоколу HTTP.

8. Сохранить захваченный трафик.

Для того, чтобы сохранить захваченный трафик, необходимо:

- 8.1 Нажать кнопку Save 📓 на панели инструментов, либо нажать File > Save As.
- **8.2** В появившемся окне нажать кнопку **Сохранить**, предварительно установив следующие параметры:

<u>И</u> мя файла:	lab2-dump-avira	•
<u>Т</u> ип файла:	Wireshark/topdump/ libpcap (*.pcap;*.cap)	•

	Captured	Displayed
All packets	1761	967
Selected packet	1	1
C Marked packets	0	0
C First to last marked	0	0
C Range:	0	0

9. Заново запустить захват трафика.

Для того, чтобы сохранить захваченный трафик, необходимо нажать кнопку **Restart** на панели инструментов, либо нажать **Capture > Restart**.

10. Настроить фильтрацию вывода по протоколу FTP.

Для настройки фильтрации необходимо:

4.3 Ввести в поле фил	ьтра выражение:	"ftp	ftp-data".
-----------------------	-----------------	------	------------

Filter: ftp ftp-data	Expression	Clear	Apply
-------------------------	------------	-------	-------

4.4 Нажать кнопку **Apply**.

11. Скачать файл с FTP-сервера.

Для того, чтобы скачать файл в адресной строке браузера необходимо набрать <u>ftp://172.16.1.10/file.zip</u> и в появившемся окне нажать кнопку **Сохранить**.

12. Проанализировать трафик, захваченный программой.

При анализе трафика необходимо произвести следующие действия:

12.1 Среди PDU, захваченных программой, найти **FTP Data**, содержащие скачиваемые с FTP-сервера данные.

FTP-DATA FTP Data: 1460 bytes FTP-DATA FTP Data: 1460 bytes

- **12.2** Посмотрев содержимое **FTP Data** выяснить и записать в отчёт следующую информацию:
 - Сколько байт данных содержится в одном PDU
 - Сетевой адрес FTP-сервера.
 - МАС-адрес FTP-сервера
 - Протокол транспортного уровня, который использует протокол FTP.
 - •Порт, который используется при передаче данных по протоколу FTP.
- 13. Сохранить захваченный трафик с именем lab2-dump-ftp.

Теория.

Wireshark - это программный анализатор трафика, который позволяет перехватывать информационные потоки, передаваемые по сети. Программа в первую очередь предназначена для сбора информации о сетевых взаимодействиях и для обнаружения и устранения неполадок в сети. Анализаторы трафика (сниферы) так же часто применяются при разработке новых протоколов и программного обеспечения и в образовательных целях.

Установленная и запущенная на компьютере программа Wireshark позволяет обнаружить и изучить любой протокольный блок данный (Protocol Data Unit, PDU), который был отправлен или получен с помощью любого из установленных на компьютере сетевых адаптеров (Network Interface Card, NIC).

Начальная настройка программы и запуск захвата трафика.



На рисунке Х изображено окно, которое появляется при запуске программы.

Рисунок 1. Стартовый интерфейс программы.

Выделенная область	Описание и функции
1	Кнопка, при нажатии на которую программа выведет список активных сетевых адаптеров (рисунок X), с которых возможен захват трафика. Список имеет вид интерактивной таблицы.
2	Список активных сетевых интерфейсов. Нажатие на любой интерфейс из списка немедленно запустит процесс захвата трафика.
3	Кнопка, при нажатии на которую программа выведет окно настроек процесса захвата трафика (рисунок X).
4	Кнопка, позволяющая загружать в программу захваченный ранее и сохраненный файл и отчётом о захваченном сетевом трафике.

📶 Wireshark: Capture Interfaces	_					
Description	IP	Packets	Packets/s		Stop	
😂 Adapter for generic dialup and VPN capture	unknown	5131	377	Start	Options	Details
😥 Attansic AtcL001 Gigabit Ethernet Controller (Microsoft's Packet Scheduler)	10.144.39.224	6086	369	Start	Options	Details
📇 WAN (PPP/SLIP) Interface	95.24.101.103	5130	377	Start	Options	Details
Help						lose

Рисунок 2. Список активных сетевых адаптеров.

Список активных адаптеров имеет вид интерактивной таблицы со следующими полями:

Поле таблицы	Описание
Description	Описание адаптера
IP	Сетевой адрес (Если есть)
Packets	Количество захваченных блоков данных (PDU) с момента вызова таблицы.
Packets/s	Скорость обработки (приёма и отправки пакетов).

Также напротив каждого интерфейса расположены 3 кнопки:

Кнопка	Функция
Start	Начать захват трафика.
Options	Вызов окна настроек захвата трафика.
Details	Подробная информация о сетевом адаптере.

📶 Wireshark: Captu	ire Optic	ons			= 🛚 🕅	
Capture						
Interface: Local		Attansic AtcL001 Gig	abit Ethernet (Controlle	r (Microsoft's Pack 💌 🔪	
IP address: 10.144.3	9.224					
Link-law theader typ	e: Ethe	ernet	Wireless Settings			
Car' ure packets	in promiso	uous mode		Remote	e Settings	
Capture packets	in pcap-no to 1	g format (experimental) bytes	Buffer size:	1	🖨 megabyte(s)	
Capture Filter:					•	
Capture File(s)			Displa	y Options	5	
File:		Browse	•) 🔽 🛛	Ipdate lisi	t of packets in real and	
Use <u>m</u> ultiple files				1917 - 1917	<u> </u>	
💽 Next file every	1	🗘 megabyte(s)		utomatic	scrolling in live capture	
Next file every	1	🗘 minute(s)		Hide capture info dialog		
🗵 Ring buffer with	2	🗘 files	Name	Docolutio		
Stop capture after	er 1	C file(s)	Indine .	Resolucio		
Stop Capture				nable <u>M</u> A	C name resolution	
🗌 after 🛛 1		<pre>packet(s)</pre>	E	nable <u>n</u> el	twork name resolution	
after 1		🔅 megabyte(s)		1991 		
after 1		🔅 minute(s)		nable <u>t</u> ra	nsport name resolution	
Help			C	<u>S</u> tart		

Рисунок 3. Окно настроек захвата сетевого трафика.

Выделенная область	Описание и функции
	Выбор интерфейса для захвата трафика.
1	В этой области расположены два выпадающих меню. Первое (левое) определяет тип используемого интерфейса: локальный (Local) или удалённый (Remote). Второе (правое) выпадающее меню определяет сам интерфейс.
2	Сарture packets in promiscuous mode – Захват пакетов в режиме приёма всех сетевых пакетов. Если эта опция включена, программа будет захватывать все PDU, которые принимает сетевой адаптер. Если опция отключена – программа будет захватывать только PDU, предназначенные компьютеру, на котором она установлена.
	Опции отображения захвата пакетов:
	Update list in real time – обновление списка в реальном времени.
	Если эта опция включена, то программа отображает захваченный трафик в реальном времени.
3	Automatic scrolling in live capture – Автоматическая прокрутка при захвате.
	Если эта опция включена, программа будет автоматически удерживать в окне вывода захваченной информации последние захваченные PDU.
	Hide capture info dialog – Скрыть информационно-диалоговое окно захвата.
	Если эта опция включена, то информационно-диалоговое окно захвата (Рисунок X) не выводится.
	Опции преобразования имен.
	Enable MAC name resolution – Включить преобразование MAC-адресов.
	Эта опция включает автоматическое преобразование физических адресов устройств в более понятный для человека формат.
	Пример: 00:09:5b: 01:02:03 -> Netgear_ 01:02:03. Выделенная часть сетевого адреса закреплена за производителем Netgear , поэтому программа преобразовала эту часть в название производителя.
л	Примечание: если включена опция преобразования сетевых имён, то в некоторых случаях программа выводит DNS имя вместо MAC-адреса.
4	Enable network name resolution – Включить преобразование сетевых имён.
	Эта опция включает автоматическое преобразование сетевых адресов устройств в DNS имена устройств.
	Пример: 216.239.37.99 -> www.google.com.
	Enable transport name resolution – Включить преобразование TCP/UDP портов.
	Эта опция включает автоматическое преобразование TCP/UDP закреплённых за определёнными протоколами портов в названия этих протоколов.
	Пример: 80 -> http

-Captureu Packe	.s	10 10 10 10 10 10 10 10 10 10 10 10 10 1	
Total	2161	% of total	
SCTP	0		0,0%
TCP	2		0,1%
UDP	2000		92,5%
ICMP	0		0,0%
ARP	79		3,7%
OSPF	0		0,0%
GRE	0		0,0%
NetBIOS	0		0,0%
IPX	0		0,0%
VINES	0		0,0%
Other	80		3,7%
I2C Events	0		0,0%
I2C Data	0		0,0%
Running	00:01:35		

Рисунок 4. Информационно-диалоговое окно захвата.

Список активных адаптеров имеет вид интерактивной таблицы со следующими столбцами:

№ столбца (слева - направо)	Описание
1	Имя протокола. В таблице представлены наиболее распространенные протоколы.
2	Количество захваченных PDU определённого протокола.
3, 4	Графическое и числовое отображение процентного отношения захваченных PDU конкретного протокола к общему числу захваченных PDU.

Также в окне отображаются следующие параметры:

Параметр	Описание					
Total	Общее количество захваченных пакетов.					
Running	Время, на протяжении которого ведётся захват пакетов.					

Главное рабочее окно программы.

После выбора интерфейса и запуска захвата PDU программа вызовет окно, показанное на рисунке X.

🗖 (Untitled) - Wireshark				BNR
File Edit View Go Canture And	lyze Statistics Telephony Tools Help			
Filter:	2	 Expression Clear Apply 		
			14.2.3	
No Time	Source	Destination	Protocol	Info
92 12 028321	95 24 101 103	91 203 99 45	нттр	GET /2host=www va rushe
93 12,028321	95.24.101.103	93,158,134,44	HTTP	GET /i/favicon.ico HTTE
94 12,031250	95.24.101.103	213,234,192,7	DNS	Standard query A www.tr
95 12.031250	93.158.134.44	95.24.101.103	НТТР	HTTP/1.1 200 OK (image
96 12.033203	95.24.101.103	213.234.192.7	DNS	Standard query A ya.ru
97 12.034180	213.234.192.7	95.24.101.103	DNS	Standard query response
98 12.035157	95.24.101.103	217.73.200.169	ТСР	unifyadmin > http [SYN]
99 12.036133	213.234.192.7	95.24.101.103	DNS	Standard query response
100 12.036133	95.24.101.103	213.180.204.8	TCP	oce-snmp-trap > http [s
101 12.038086	217.73.200.169	95.24.101.103	TCP	http > unifyadmin [SYN,
102 12.038086	95.24.101.103	217.73.200.169	TCP	unifyadmin > http [ACK]
103 12.039063	213.180.204.8	95.24.101.103	TCP	http > oce-snmp-trap [s
104 12.039063	95.24.101.103	213.180.204.8	TCP	oce-snmp-trap > http [A
105 12.047852	95.24.101.103	217.73.200.169	HTTP	GET /VI3a****Yandex_ru/
105 12.047852	95.24.101.103	213.180.204.8	HIIP	GET / Togo.png HTTP/1.1
107 12.049805	95.24.101.103	213.234.192.7	DNS	Standard query A CICK.y
				>
Erame 101 (58 bytes on	wire, 58 bytes captured)			
Ethernet II Src: 32:83	······································	1.00) Det. Yeroy 00.00.00 (01.	.00.01.00.00.00)	
E Etherhet II, Sic. 34.6/	-17 77 200 160 (31.07.20.00.0	160), Dot. AELOX_00.00.00 (01.	101.102.	
Internet Protocol, Src:	217.73.200.169 (217.73.200	.169), DSt: 95.24.101.103 (95.2	(4.101.103)	
Transmission Control Pr	otocol, Src Port: http (80)	, Dst Port: unifyadmin (2696),	Seq: 0, Ack: 1, Len:	0
				_
0000 01 00 01 00 00 00 3	- 97 - 30 - 00 - 01 - 00 - 09 - 00 - 45 - 0	о · г		
	a 87 20 00 01 00 08 00 45 0 7 06 1d 4c d9 49 c8 a9 5f 1	8 W I T		
0020 65 67 00 50 0a 88 a	f 9b 4b 44 bd a8 16 7d 60 1	2 eq.P KD}		
0030 47 18 10 ae 00 00 0	2 04 05 b4	G		
			501	
			il	and the second
File: "C:\DOCUME~1\Admin\LOCALS~	1)Temp)wi Packets: 228 Displayed: 228 M	arked: U Dropped: 0	Pr	ohie: Derault 🛛 🕹

Рисунок 5. Окно отображения захваченного трафика.

Выделенная область	Описание и функции							
1	Меню программы, и панель инструментов, предоставляющая доступ к наиболее часто используемым функциям программы.							
2	Фильтр, позволяющий производить выборочный захват PDU.							
3	Поле списка PDU, в котором отображается краткая информация по всем захваченным PDU.							
4	Информационное поле, в котором отображается подробная информация по выбранному PDU.							
5	Поле, в котором отображаются данные выделенные в информационном поле в шестнадцатеричной и текстовой форме.							

Панель инструментов.

Панель инструментов представлена на рисунке Х.



N⁰	Кнопка	Название кнопки	Соответствующая опция в меню	Функции кнопки
1		Interfaces	Capture / Interfaces	Вызов списка активных сетевых адаптеров (Рисунок X).
2	ŭ,	Options	Capture / Options	Вызов окна настроек захвата сетевого трафика (Рисунок X).
3		Start	Capture / Start	Старт захвата трафика с текущими параметрами захвата.
4		Stop	Capture / Stop	Остановить захват трафика.
5		Restart	Capture / Restart	Перезапустить захват трафика с текущими параметрами.
6		Open	File / Open	Открыть файл с отчётом о захваченном трафике.
7		Save As	File / Save As	Сохранить текущий отчёт о захваченном трафике в файл.
8	×	Close	File / Close	Закрыть текущий отчёт о захваченном трафике.
9	Ì	Reload	View / Reload	Закрыть и открыть заново текущий отчёт о захваченном трафике.
10	۳) ا	Print	File / Print	Распечатать текущий отчёт о захваченном трафике.
11	Ð	Zoom In	View / Zoom In	Увеличить размер шрифта.
12	Θ	Zoom Out	View / Zoom Out	Уменьшить размер шрифта.
13	11	Normal Size	View / Normal Size	Установить размер шрифта, используемый по умолчанию.
14	\gg	Preferences	Edit / Preferences	Вызов меню настроек.
15	$\mathbf{\overline{O}}$	Help	Help / Contents	Вызов справки.

Фильтр

Фильтр позволяет настроить программу Wireshark на отображение только определённого, удовлетворяющего условиям текущего примененного фильтра сетевого трафика.

Фильтр может применяться как при захвате трафика в реальном времени, так и при анализе захвата, сохранённого в файле.

Панель фильтра представлена на рисунке Х.

Filter:		•	Expression	Clea <u>r</u>	Apply
1	2	3	4	5	6
	Рисунок 7. Панель фильтра.				

Nº	Кнопка / Поле	Название Кнопки / поля	Функции кнопки / поля
1	Filter:	Filter:	Вызов диалогового окна для создания и сохранения пользовательских фильтров (Рисунок X).
2 Filter Input Поле ввода фильтра.			Поле ввода фильтра.
3	-		Вызов списка применённых ранее фильтров.
4	Expression	Expression	Вызов диалогового окна, позволяющего выбирать фильтры из базы данных программы.
5	Clea <u>r</u>	Clear	Очистить поле ввода фильтра.
6	Apply	Apply	Применить фильтр.

Для применения фильтра необходимо:

- 1. Ввести фильтр в поле ввода.
- 2. Нажать кнопку "Apply".

Если фильтр введён в соответствии с правилами построения фильтров, то цвет поля ввода будет зелёным (Рисунок X), если фильтр введён с ошибкой – красным (Рисунок X).



Рисунок 9. Фильтр введён неправильно.

Построение фильтров.

Фильтрацию, применяемую в программе Wireshark можно условно разделить на две категории:

- Фильтрация по определённым протоколам.
- Фильтрация по определённым значениям полей в заголовках протоколов.

Для применения фильтрации по определённому протоколу необходимо ввести имя протокола в поле ввода фильтра.

Пример выполнения фильтрации по протоколу НТТР показан на рисунках Х-У.

Filter:					▼ Expression Clear Apply			
No	Time	Source	Destination	Protocol	Info			
130	2 53.554904	114.128.24.115	95.25.203.168	UDP	Source port: 11191 Destination port: 30840			
130	3 53.554984	95.25.203.168	114.128.24.11	5 ICMP	Destination unreachable (Port unreachable)			
130	4 53.676367	10.144.34.166	Broadcast	ARP	who has 10.144.32.1? Tell 10.144.34.166			
130	5 53.692329	10.144.34.166	Broadcast	ARP	who has 10.144.32.1? Tell 10.144.34.166			
130	6 53.719283	10.144.34.166	Broadcast	ARP	who has 10.144.32.1? Tell 10.144.34.166			
130	7 53.765255	95.25.203.168	213.234.192.7	DNS	Standard query A sitecheck2.opera.com			
130	8 53.769416	213.234.192.7	95.25.203.168	DNS	Standard query response A 91.203.99.45			
130	9 53.778079	95.25.203.168	91.203.99.45	TCP	2319 > 80 [SYN] Seq=0 win=65535 Len=0 MSS=1360			
131	0 53.783166	95.25.203.168	213.234.192.7	DNS	Standard query A ya.ru			
131	1 53.786208	213.234.192.7	95.25.203.168	DNS	Standard query response A 213.180.204.8 A 93.158.134.8 A 77.88.21.8			
131	2 53.786671	95.25.203.168	213.180.204.8	TCP	2320 > 80 [SYN] Seq=0 win=65535 Len=0 MSS=1360			
131	3 53.788356	213.180.204.8	95.25.203.168	TCP	80 > 2320 [SYN, ACK] seq=0 Ack=1 win=8192 Len=0 MSS=1360			
131	4 53.788429	95.25.203.168	213.180.204.8	TCP	2320 > 80 [ACK] seg=1 Ack=1 win=65535 Len=0			
131	5 53.789346	95.25.203.168	213.180.204.8	HTTP	GET / HTTP/1.1			
131	6 53.791668	213.180.204.8	95.25.203.168	TCP	[TCP segment of a reassembled PDU]			
131	7 53.791869	213.180.204.8	95.25.203.168	HTTP	HTTP/1.1 200 OK (text/html)			

Рисунок 10. Вывод программы до применения фильтра.

	Filter: http	P			▼ Expres	ssion Clear_ Apply
Γ	No	Time	Source	Destination	Protocol	Info
ľ	391	14.908475	95.25.203.168	80.190.130.226	HTTP	GET /update/idx/master.idx HTTP/1.1
	395	14.966242	80.190.130.226	95.25.203.168	HTTP	HTTP/1.1 200 OK (text/plain)
Γ	1315	53.789346	95.25.203.168	213.180.204.8	HTTP	GET / HTTP/1.1
	1317	53.791869	213.180.204.8	95.25.203.168	HTTP	НТТР/1.1 200 ОК (text/html)
	1329	54.046936	95.25.203.168	213.180.204.8	HTTP	GET /logo.png HTTP/1.1
	1331	54.048771	213.180.204.8	95.25.203.168	HTTP	HTTP/1.1 304 Not Modified
	1332	54.050235	95.25.203.168	91.203.99.45	HTTP	GET /?host=ya.ru&hdn=xBVRlPGv51tOStUgxXX0HQ== HTTP/1.1
	1336	54.077067	95.25.203.168	217.73.200.221	HTTP	GET /v13a*****yandex_ru/ru/CP1251/tmsec=yandex_ya/0 HTTP/1.1
Ľ	1339	54.079406	217.73.200.221	95.25.203.168	HTTP	[TCP out-of-order] HTTP/1.1 200 OK (GIF89a)
	1342	54.082356	91.203.99.45	95.25.203.168	HTTP/XML	НТТР/1.1 200 ОК
	1348	54.132425	95.25.203.168	77.88.21.14	HTTP	GET /redir/dtype=stred/pid=17/cid=1729/*http://export.yandex.ru/mord
	1349	54.134522	77.88.21.14	95.25.203.168	HTTP	HTTP/1.1 302 Redirect
	1357	54.142230	95.25.203.168	87.250.251.69	HTTP	GET /morda/mail.xml?host=yandex.ru HTTP/1.1
	1359	54.145367	87.250.251.69	95.25.203.168	HTTP	HTTP/1.1 200 OK (text/javascript)
	1368	54.249088	95.25.203.168	213.180.204.8	HTTP	GET /b-suggest.css HTTP/1.1
	1369	54.251113	213.180.204.8	95.25.203.168	HTTP	HTTP/1.1 200 OK (text/css)

Рисунок 11. Вывод программы после применения фильтра.

Фильтрация по определённому значению поля в заголовках протоколов строится по следующему синтаксису:

Поле Оператор сравнения Значение

Операторы сравнения и некоторые обозначения полей, которые могут использоваться при построении фильтров, представлены в таблицах Х и У.

Поле	Описание
eth.addr	Физический адрес источника или получателя в кадре протокола Ethernet.
eth.dst	Физический адрес получателя в кадре протокола Ethernet.
eth.src	Физический адрес источника в кадре протокола Ethernet.
eth.len	Длина кадра протокола Ethernet.
ip.addr	Сетевой адрес источника или получателя в пакете протокола IP.
ip.dst	Сетевой адрес получателя в пакете протокола IP.
ip.src	Сетевой адрес источника в пакете протокола IP.
ip.proto	Обозначения протокола, который был инкапсулирован в пакет IP.
tcp.ack	Подтверждения (АСК) протокола ТСР
tcp.port	Порт источника или получателя в сегменте протокола ТСР.
tcp.dstport	Порт получателя в сегменте протокола ТСР.
tcp.srcport	Порт источника в сегменте протокола ТСР.
udp.port	Порт источника или получателя в сегменте протокола UCP.
udp.dstport	Порт получателя в сегменте протокола UCP.
udp.srcport	Порт источника в сегменте протокола UCP.
dns.qry.name	Имя сетевого ресурса в DNS запросе.
dns.resp.name	Имя сетевого ресурса в DNS ответе.

Таблица 1. Обозначения полей при построении фильтров.

Опер	ратор	Значение	Примеры
==	eq	Равно	ip.addr==192.168.1.1
			Отображать только те пакеты протокола IP, в которых сетевой адрес отправителя или получателя равен 192.168.1.1
			Отображать только широковещательные (broadcast) кадры протокола Ethernet.

!=	ne	Не равно	ip.dst==255.255.255.255
			Не отображать широковещательные (broadcast) пакеты протокола IP.
>	gt	Больше	tcp.dstport>10000
			Отображать только те сегменты протокола ТСР, в которых порт получателя больше 10000.
<	lt	Меньше	tcp.dstport<1024
			Отображать только те датаграммы протокола UDP, в которых порт получателя меньше 1024.

Таблица 2. Операторы сравнения.

При построении фильтра можно комбинировать два и более условия, используя логические операторы.

Комбинирование условий при построении операторов производится по следующему принципу:

Условие 1 Логический оператор Условие 2 Логический оператор

В качестве условия может использоваться как фильтрация по протоколам, так и фильтрация по значениям определённых полей в протоколах.

В таблице Х представлены некоторые логические операторы.

Оператор		Значение	Примеры				
&&	and	И	ip.src==192.168.1.1 && ip.dst==192.168.1.10				
			Отображать только сообщения отправленные устройством с сетевым адресом 192.168.1.1 для устройства с сетевым адресом 192.168.1.10				
	or	или	eth.dst==ff:ff:ff:ff:ff:ff ip.dst==255.255.255.255				
			Отображать только широковещательные кадры протокола Ethernet или пакеты протокола IP.				
!	not	НЕ (Отрицание)	!arp				
			Не отображать PDU протокола ARP.				

Поле списка захваченных PDU.

В поле списка захваченных PDU (Рисунок X) выводится сводная информация по всему трафику, захваченному с помощью программы Wireshark.

No.	-	Time	Source	Destination	Protocol	Info	^
	1343	54.126714	95.25.203.168	213.234.192.7	DNS	Standard guery A clck.yandex.ru	
	1344	54.129754	213.234.192.7	95.25.203.168	DNS	standard query response A 77.88.21.14 A 213.180.204.14 A 87.250.25	
	1345	54.130456	95.25.203.168	77.88.21.14	TCP	2322 > 80 [SYN] seq=0 win=65535 Len=0 Mss=1360	
	1346	54.132141	77.88.21.14	95.25.203.168	TCP	80 > 2322 [SYN, ACK] seq=0 Ack=1 win=8192 Len=0 MSS=1360	
	1347	54.132219	95.25.203.168	77.88.21.14	TCP	2322 > 80 [ACK] seq=1 Ack=1 win=65535 Len=0	
	1348	54.132425	95.25.203.168	77.88.21.14	HTTP	GET /redir/dtype=stred/pid=17/cid=1729/*http://export.yandex.ru/mc	
	1349	54.134522	77.88.21.14	95.25.203.168	HTTP	HTTP/1.1 302 Redirect	
	1350	54.134558	77.88.21.14	95.25.203.168	TCP	80 > 2322 [FIN, ACK] seq=135 Ack=805 win=9520 Len=0	
	1351	54.134598	95.25.203.168	77.88.21.14	TCP	2322 > 80 [ACK] Seq=805 Ack=136 win=65401 Len=0	
	1352	54.136994	95.25.203.168	213.234.192.7	DNS	Standard query A export.yandex.ru	
	1353	54.140117	213.234.192.7	95.25.203.168	DNS	Standard query response CNAME corba-http-export.yandex.ru A 87.250	¥
4						5	

Рисунок 12. После списка захваченных PDU.

Сводная информация выводится в виде таблицы со следующими полями:

Поле таблицы	Описание					
No.	Порядковый номер захваченного PDU. При использовании фильтра порядковый номер не изменяется.					
Time	Временная отметка, обозначающая время (в секундах) прошедшее с момента начала захвата PDU.					
Source	Сетевой адрес отправителя.					
Destination	Сетевой адрес получателя.					
Protocol	Протокол.					
Info	Дополнительная информация о захваченном PDU.					

На рисунке X представлен пример сводной информации о захваченной PDU.

No. +	Time	Source	Destination	Protocol	Info
and the second se					THE PARTY AND AND A PARTY AND
1343	54.126714	95.25.203.168	213.234.192.7	DNS	Standard query A clck.yandex.ru

Рисунок 13. Пример записи в списке захваченных PDU.

Запись можно интерпретировать следующим образом:

1343 – Этот PDU является 1343-им по счету захваченным PDU.

54.126714 – PDU захвачен через 54 секунды после начала захвата.

95.25.203.168 – Устройство, которое его отправило, имеет сетевой адрес 95.25.203.168.

213.234.192.7 – Устройство, которому оно предназначалось, имеет адрес 213.234.192.7.

DNS – Взаимодействие между устройствами происходит по протоколу DNS.

Standard query A click.yandex.ru – устройство с адресом 95.25.203.168 обращается к устройству с адресом 213.234.192.7 чтобы узнать сетевой адрес информационного ресурса click.yandex.ru

Информационное поле.

В информационном поле (Рисунок X) отображается подробная информация о захваченном PDU, выделенном в поле списка захваченных PDU.

No. +	Time	Source	Destination	Protocol	Info
296 299 304 305 395 463 464 534 535	$\begin{array}{r} 30.368904\\ 34.369097\\ 42.369969\\ 42.370315\\ 52.563781\\ 85.546583\\ 85.547026\\ 115.38268\\ 115.38314 \end{array}$	172.16.1.50 172.16.1.50 172.16.1.50 it-server.clas 172.16.1.50 it-server.clas 172.16.1.50 it-server.clas	it-server.clas it-server.clas it-server.clas 172.16.1.50 it-server.clas 172.16.1.50 it-server.clas 172.16.1.50	DNS DNS DNS DNS DNS DNS DNS DNS DNS	Standard query A personal.avira-update.com Standard query A personal.avira-update.com Standard query PTR 1.0.0.127.in-addr.arpa Standard query response PTR localhost Standard query response, Server failure Standard query PTR 2.1.16.172.in-addr.arpa Standard query PTR 2.1.16.172.in-addr.arpa Standard query PTR 2.1.16.172.in-addr.arpa Standard query PTR 2.1.16.172.in-addr.arpa
 H Fra Eth H Int Use S C L L E O E O 	ume 395 (85 mernet II, cernet Prot ource port cestination length: 51 checksum: C nain Name S	i bytes on wire, Src: it-server. cocol, Src: it-s Protocol, Src 53 (53) port: 1343 (13 0x49de [validati System (response	85 bytes captu class.mitht.ru erver.class.mit Port: 53 (53), 43) ion disabled] e)	ured) (00:04:2 tht.ru (1 Dst Port	3:bf:bc:19), Dst: Foxconn_be:5a:27 (00:01:6c:be:5a:27) 72.16.1.2), Dst: 172.16.1.50 (172.16.1.50) : 1343 (1343)

Рисунок 14. Информационное поле программы.

Выделенная область	Описание и функции							
1	Выделенная запись в листе списка захваченных PDU. Запись выделятся нажатием левой кнопки мыши. Программа помечает текущую выделенную запись серым цветом.							
2	Подробная информация о выделенном PDU.							

Информация о выделенном PDU выводится в виде иерархического списка. Иерархия списка соответствует порядку инкапсуляции данных, применяемой при использовании протоколов стека TCP/IP для передачи информации между устройствами.

На рисунке X показан пример вывода информации о захваченном PDU протокола HTTP.

1409 239.52656 tessie.mitht.ru	172.16.1.50 HTTP	HTTP/1.0 503 Service Unav	ailable (text/html) 📃
1417 239.53176 172.16.1.50	tessie.mitht.r HTTP	GET_http://62.146.66.184/	update/idx/master.idx HTTF
1445 270.06616 172.16.1.50	tessie.mitht.r HTTP	GET http://62.146.66.184/	update/idx/master.idx HTTF
1501 300.59645 172.16.1.50	tessie.mitht.r HTTP	GET http://62.146.66.184/	update/idx/master.idx HTTF
1554 348.13269 172.16.1.50	tessie.mitht.r HTTP	GET http://perspeak.avira	-update.com/update/idx/ma:
1586 378.66555 172.16.1.50	tessie.mitht.r HTTP	GET http://perspeak.avira	-update.com/update/idx/ma:
1659 409 19910 172 16 1 50	tessie mitht r HTTP	GET http://nerspeak_avira	-undate_com/undate/idv/ma(🗡
<u> ()</u>			>
⊞ Frame 1417 (385 bytes on wire, 385 bytes	captured) 2		
	:6c:be:5a:27), Dst: it-	server.class.mitht.ru (00:04	4:23:bf:bc:19) 3
⊞ Internet Protocol, Src: 172.16.1.50 (172.	16.1.50), Dst: tessie.m	itht.ru (193.232.216.7) 4	
⊞ Transmission Control Protocol, Src Port:	1365 (1365), Dst Port:	3128 (3128), seq: 1, Ack: 1,	Len: 331 5
🗄 Hypertext Transfer Protocol 🔓			



Выделенная область	Описание и функции
1	Выделенное PDU в поле списка захваченных PDU. В соответствии с установками по умолчанию, программа отмечает выделенное PDU серым цветом.
2	
3	Ethernet II, B этом вложенном списке расположена информация о заголовке протокола канального (Data Link) уровня. В данном случае это протокол Ethernet.
4	 Internet Protocol, В этом вложенном списке расположена информация о заголовке протокола сетевого (Network) уровня. В данном случае это протокол IP.
5	Transmission Control Protocol, B этом вложенном списке расположена информация о заголовке протокола транспортного (Transport) уровня. В данном случае это протокол TCP.
6	Hypertext Transfer Protocol B этом вложенном списке расположена информация о заголовке протокола транспортного (Application) уровня. В данном случае это протокол HTTP.

Интерпретация вложенных списков.

Каждый вложенный список представляет собой последовательность полей (всех, или основных), содержащихся в заголовке протокола, используемого при инкапсуляции данных.

Порядок полей в списке соответствует порядку полей в заголовке протокола.

Протокол Ethernet

Стандарты Ethernet определяют проводные соединения и электрические сигналы на физическом уровне, формат кадров и протоколы управления доступом к среде — на канальном уровне модели OSI.

Схематичное изображение кадра протокола Ethernet и соответствующий вывод программы Wireshark показаны на рисунке Х.

Зелёным цветом выделены поля, выводимые программой.

7	1	6	6	2	46-1500	4
Preamble	Start of Frame	Destination	Source	Туре	Data	FCS

⊞ Frame 1417 (385 bytes on wire, 385 bytes captured)

 Hame 111, (Sor Spice on Wine, Sor Spice capacity)
 Ethernet II, Src: Foxconn_be:5a:27 (00:01:6c:be:5a:27), Dst: it-server.class.mitht.ru (00:04:23:bf:bc:19)
 Bource: Foxconn_be:5a:27 (00:01:6c:be:5a:27) Type: IP (0x0800)
 Internet Protocol, Src: 172.16.1.50 (172.16.1.50), Dst: tessie.mitht.ru (193.232.216.7)
 Transmission Control Protocol, Src Port: 1365 (1365), Dst Port: 3128 (3128), Seq: 1, Ack: 1, Len: 331
 Hypertext Transfer Protocol

Рисунок 16. Поля заголовка кадра протокола Ethernet.

Информацию в заголовке списка можно интерпретировать следующим образом:

Ethernet II, - Это кадр протокола Ethernet.

Src: Foxconn_be:5a:27 (00:01:6c:be:5a:27), - Физический адрес устройства отправителя, 00:01:6c:be:5a:27, производитель сетевой карты – компания Foxconn.

Dst: it-server.class.mitht.ru (00:04:23:bf:bc:19) – Физический адрес устройства получателя 00:04:23:bf:bc:19, DNS имя устройства - it-server.class.mitht.ru.

Поле	Описание					
Destination	Destination: it-server.class.mitht.ru (00:04:23:bf:bc:19)					
	интерпретация аналогична интерпретации информации из заголовка списка.					
Source	Source: Foxconn_be:5a:27 (00:01:6c:be:5a:27)					
	Интерпретация аналогична интерпретации информации из заголовка списка.					
Туре	Туре: IP (0x0800) – На сетевом уровне используется протокол IPv4.					
	Значение, этого поля позволяет устройству определить, какому протоколу сетевого уровня следует дальше передать полученное PDU. В данном случае – это протокол IP.					
	Другие наиболее часто встречающиеся значения поля Туре: 0x0806 – ARP, 0x86DD – IPv6.					

Протокол IP.

Протокол ІР — протокол сетевого уровня, обеспечивающий систему глобальной логической адресации для устройств в сети.

Схематичное изображение заголовка пакета протокола IP и соответствующий вывод программы Wireshark показаны на рисунке X.

Зелёным цветом выделены поля, выводимые программой.

Byte 1		Byte 2	Byte 3		Byte 4	
Version	Version Header Differentiated length Services Field		Total Length			
Identification			Flag	Fragment Offset		
Time to Live Protocol		Header Checksum				
Source						
Destination						
Options				Padding		

■ Ethernet II, Src: Foxconn_be:5a:27 (00:01:6c:be:5a:27), Dst: it-server.class.mitht.ru (00:04:23:bf:bc:19) ■ Internet Protocol, Src: 172.16.1.50 (172.16.1.50), Dst: tessie.mitht.ru (193.232.216.7)

	Version: 4 Header length: 20 bytes
	🖩 Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
	Total Length: 371
	Identification: 0xd63d (54845)
	🗷 Flags: 0x04 (Don't Fragment)
	Fragment offset: 0
	Time to live: 128
	Protocol: TCP (0x06)
	🗄 Header checksum: 0xdc14 [correct]
	Source: 172.16.1.50 (172.16.1.50)
	Destination: tessie.mitht.ru (193.232.216.7)
Ŧ	Transmission Control Protocol, Src Port: 1365 (1365), Dst Port: 3128 (3128), Seq: 1, Ack: 1, Len: 331
+	Hypertext Transfer Protocol

Рисунок 17. Поля заголовка пакета протокола IP.

Информацию в заголовке списка можно интерпретировать следующим образом:

Internet Protocol, - Это пакет протокола IP.

src: 172.16.1.50 (172.16.1.50), - Сетевой адрес устройства отправителя 172.16.1.50.

tessie.mitht.ru (193.232.216.7) – Сетевой Dst: адрес устройства получателя 193.232.216.7, DNS имя устройства получателя tessie.mitht.ru.

Интерпретация значений наиболее важных полей приведена в таблице ниже.

Поле	Описание					
Time to Live	Тіте to live: 128 – Максимально возможное количество сетевых устройств,					
	которые могут обработать и передать накот дальше по сети равняется т20.					
Protocol	Protocol: TCP (0x06) – На транспортном уровне используется протокол TCP.					
	Значение, этого поля позволяет устройству определить, какому протоколу транспортного уровня следует дальше передать полученное PDU. В данном случае – это протокол TCP.					
	Другие наиболее часто встречающиеся значения поля Protocol: 0x01 – ICMP, 0x11 - UDP					
Source	Source: 172.16.1.50 (172.16.1.50),					
	Интерпретация аналогична интерпретации информации из заголовка списка.					
Destination	Destination: tessie.mitht.ru (193.232.216.7)					
	Интерпретация аналогична интерпретации информации из заголовка списка.					

Протокол ТСР

Протокол ТСР – протокол транспортного уровня, обеспечивающий надёжную передачу информации между приложениями взаимодействующих устройств.

Схематичное изображение заголовка пакета протокола IP и соответствующий вывод программы Wireshark показаны на рисунке Х.

Зелёным цветом выделены поля, выводимые программой.

2 Bytes			2 Bytes		
Source port			Destination Port		
Sequence number					
	Acknowledgement number				
Header Length (Reserved) Flags Window Size					
TCP Checksum			Urgent Pointer		
Options (if any)					

Frame 1417 (385 bytes on wire, 385 bytes captured)
Ethernet II, Src: Foxconn_be:5a:27 (00:01:6c:be:5a:27), Dst: it-server.class.mitht.ru (00:04:23:bf:bc:19)
Internet Protocol, Src: 172.16.1.50 (172.16.1.50), Dst: tessie.mitht.ru (193.232.216.7)
Transmission Control Protocol, Src Port: 1365 (1365), Dst Port: 3128 (3128), Seq: 1, Ack: 1, Len: 331
Source port: 1365 (1365)
Destination port: 3128 (3128)
[Stream index: 30]

```
Sequence number: 1 (relative sequence number)
[Next sequence number: 332 (relative sequence number)]
Acknowledgement number: 1 (relative ack number)
Header length: 20 bytes

Flags: 0x18 (PSH, ACK)
window size: 17520
Checksum: 0xd8b0 [validation disabled]
[SEQ/ACK analysis]
Hypertext Transfer Protocol
```

Рисунок 18. Поля заголовка сегмента ТСР.

Информацию в заголовке списка можно интерпретировать следующим образом:

Transmission control Protocol, - Это сегмент протокола TCP.

Src Port: 1365 (1365), - Приложение устройства отправителя использует порт 1365.

Dst Port: 3128 (3128), - Приложение устройства получателя использует порт 3128

Len: 331 – Сегмент содержит 331 байт информации.

Интерпретация значений наиболее важных полей приведена в таблице ниже.

Поле	Описание					
Source port	Source Port: 1365 (1365)					
	Интерпретация аналогична интерпретации информации из заголовка списка.					
Destination port	Destination Port: 3128 (3128)					
	Интерпретация аналогична интерпретации информации из заголовка списка.					
Sequence number и Acknowledgement	Sequence number: 1(.relative sequence number)[Next sequence number: 332(relative sequence number)]Acknowledgement number: 1(relative ack number)					
number	Поля, использующиеся для организации надёжной доставки информации между приложениями.					
Window size	Количество байт, которые могут быть переданы без подтверждения.					

Протокол UDP.

Протокол TCP – протокол транспортного уровня, обеспечивающий передачу информации между приложениями взаимодействующих устройств с минимальным задержками.

Схематичное изображение заголовка пакета протокола IP и соответствующий вывод программы Wireshark показаны на рисунке Х.

Зелёным цветом выделены поля, выводимые программой.

2 Bytes	2 Bytes
Source Port	Destination Port
Length	Checksum CRC

Brame 1334 (1340 bytes on wire, 1340 bytes captured)
 Ethernet II, Src: Foxconn_be:5a:27 (00:01:6c:be:5a:27), Dst: it-server.class.mitht.ru (00:04:23:bf:bc:19)
 Internet Protocol, Src: 172.16.1.50 (172.16.1.50), Dst: it-server.class.mitht.ru (172.16.1.2)
 User Datagram Protocol, Src Port: 1364 (1364), Dst Port: 88 (88)
 Source port: 1364 (1364)
 Destination port: 88 (88)
 Length: 1306
 Checksum: 0x4902 [validation disabled]
 Kerberos TGS-REQ

Рисунок 19. Поля заголовка датаграммы UDP.

Информацию в заголовке списка можно интерпретировать следующим образом:

User Datagram Protocol, - Это датаграмма протокола TCP

Src Port: 1364 (1364), - Приложение устройства отправителя использует порт 1364.

Dst Port: 88 (88) - Приложение устройства получателя использует порт 88

Поле	Описание					
Source port	Source Port: 1364 (1364)					
	Интерпретация списка.	аналогична	интерпретации	информации	ИЗ	заголовка
Destination port	Destination Port: 88 (88)					
	Интерпретация списка.	аналогична	интерпретации	информации	ИЗ	заголовка
Length	Длина датаграмм	<i>и</i> ы.				