

## Краткие теоретические сведения

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 данных (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 X изображено окно, которое появляется при запуске программы.

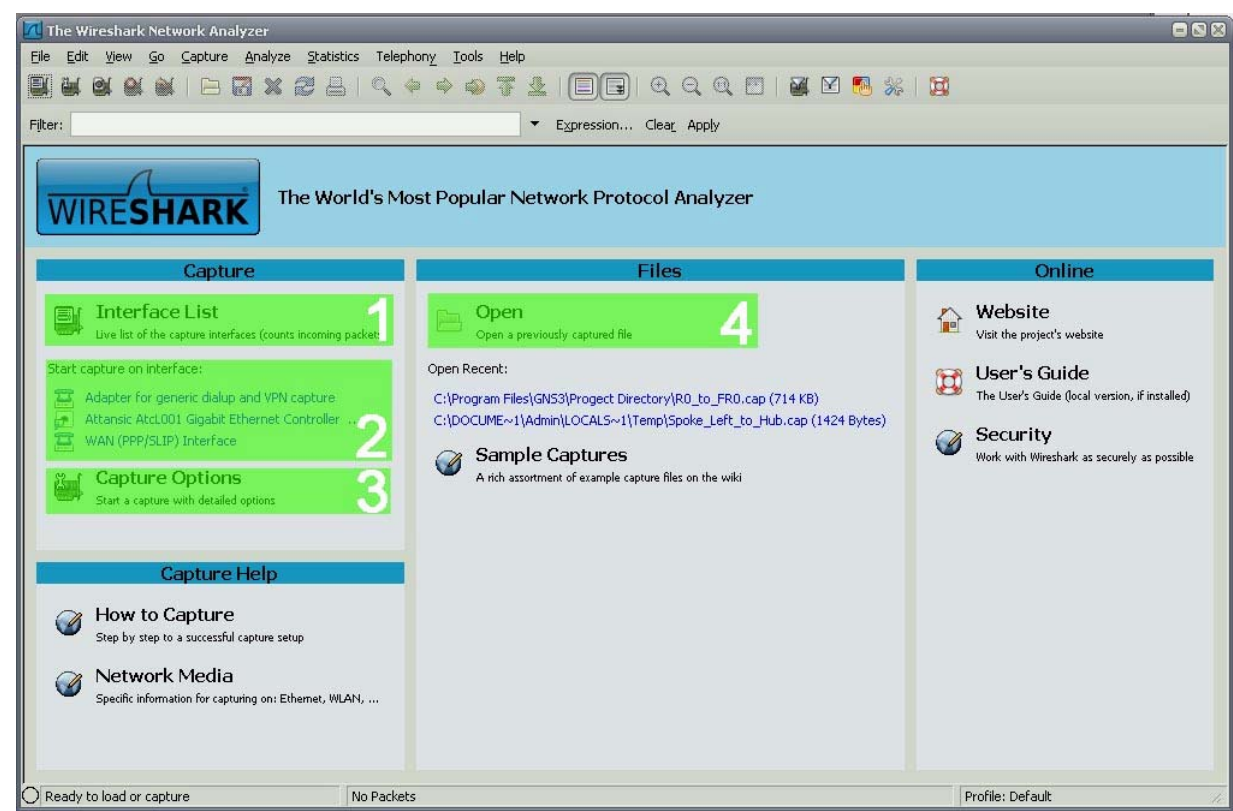


Рисунок 1. Стартовый интерфейс программы.

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.

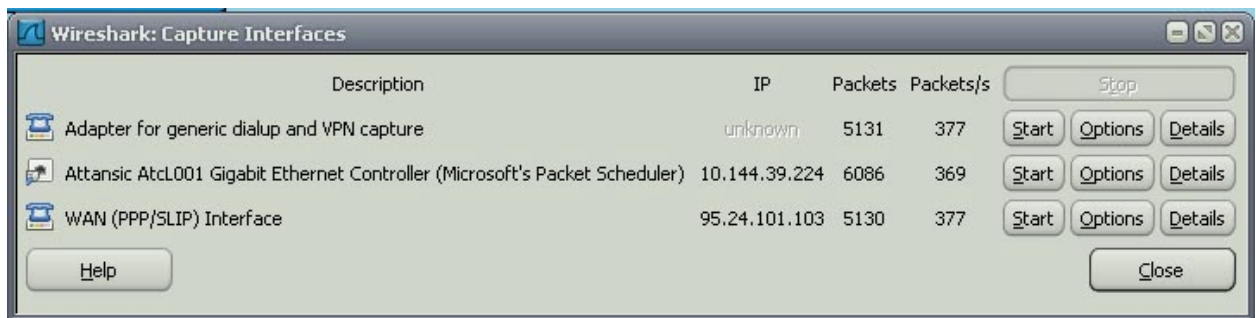


Рисунок 2. Список активных сетевых адаптеров.

Список активных адаптеров имеет вид интерактивной таблицы со следующими полями:

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

Также напротив каждого интерфейса расположены 3 кнопки:

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

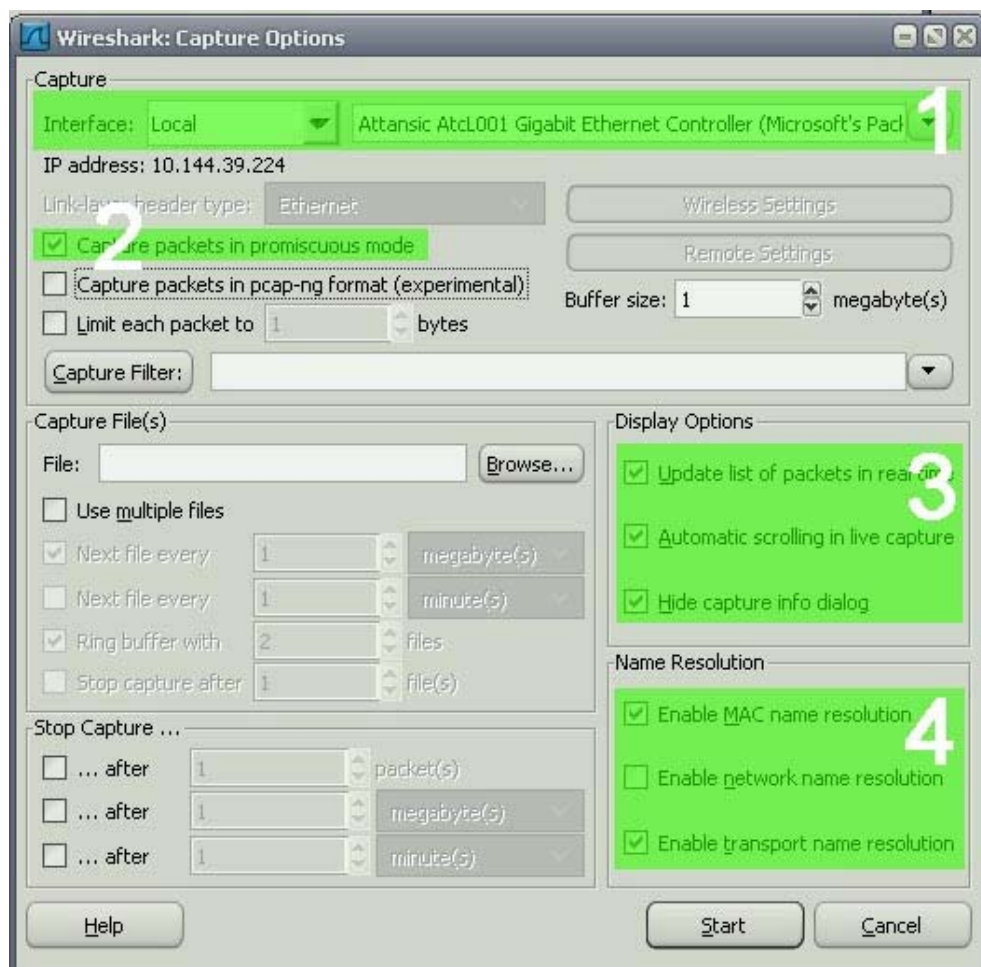
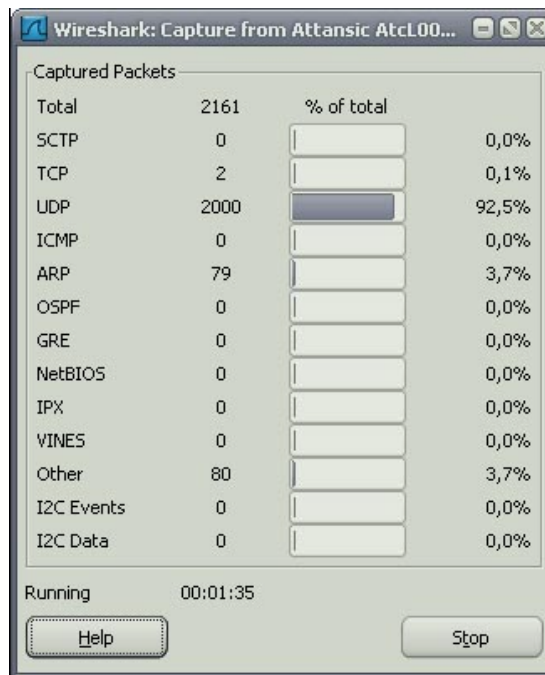


Рисунок 3. Окно настроек захвата сетевого трафика.

Выделенная область	Описание и функции
1	<p>Выбор интерфейса для захвата трафика.</p> <p>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.</p>
2	<p><b>Capture packets in promiscuous mode</b> – Захват пакетов в режиме приёма всех сетевых пакетов.</p> <p>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.</p>
3	<p>Опции отображения захвата пакетов:</p> <p><b>Update list in real time</b> – обновление списка в реальном времени.</p> <p>Если эта опция включена, то программа отображает захваченный трафик в реальном времени.</p> <p><b>Automatic scrolling in live capture</b> – Автоматическая прокрутка при захвате.</p> <p>Если эта опция включена, программа будет автоматически удерживать в окне вывода захваченной информации последние захваченные PDU.</p> <p><b>Hide capture info dialog</b> – Скрыть информационно-диалоговое окно захвата.</p> <p>Если эта опция включена, то информационно-диалоговое окно захвата (Рисунок X) не выводится.</p>
4	<p>Опции преобразования имен.</p> <p><b>Enable MAC name resolution</b> – Включить преобразование MAC-адресов.</p> <p>Эта опция включает автоматическое преобразование физических адресов устройств в более понятный для человека формат.</p> <p>Пример: <b>00:09:5b:01:02:03</b> -&gt; <b>Netgear_01:02:03</b>. Выделенная часть сетевого адреса закреплена за производителем <b>Netgear</b>, поэтому программа преобразовала эту часть в название производителя.</p> <p>Примечание: если включена опция преобразования сетевых имён, то в некоторых случаях программа выводит DNS имя вместо MAC-адреса.</p> <p><b>Enable network name resolution</b> – Включить преобразование сетевых имён.</p> <p>Эта опция включает автоматическое преобразование сетевых адресов устройств в DNS имена устройств.</p> <p>Пример: <b>216.239.37.99</b> -&gt; <b>www.google.com</b>.</p> <p><b>Enable transport name resolution</b> – Включить преобразование TCP/UDP портов.</p> <p>Эта опция включает автоматическое преобразование TCP/UDP закреплённых за определёнными протоколами портов в названия этих протоколов.</p> <p>Пример: <b>80</b> -&gt; <b>http</b></p>



**Рисунок 4. Информационно-диалоговое окно захвата.**

Список активных адаптеров имеет вид интерактивной таблицы со следующими столбцами:

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

Также в окне отображаются следующие параметры:

Параметр	Описание
<b>Total</b>	Общее количество захваченных пакетов.
<b>Running</b>	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.

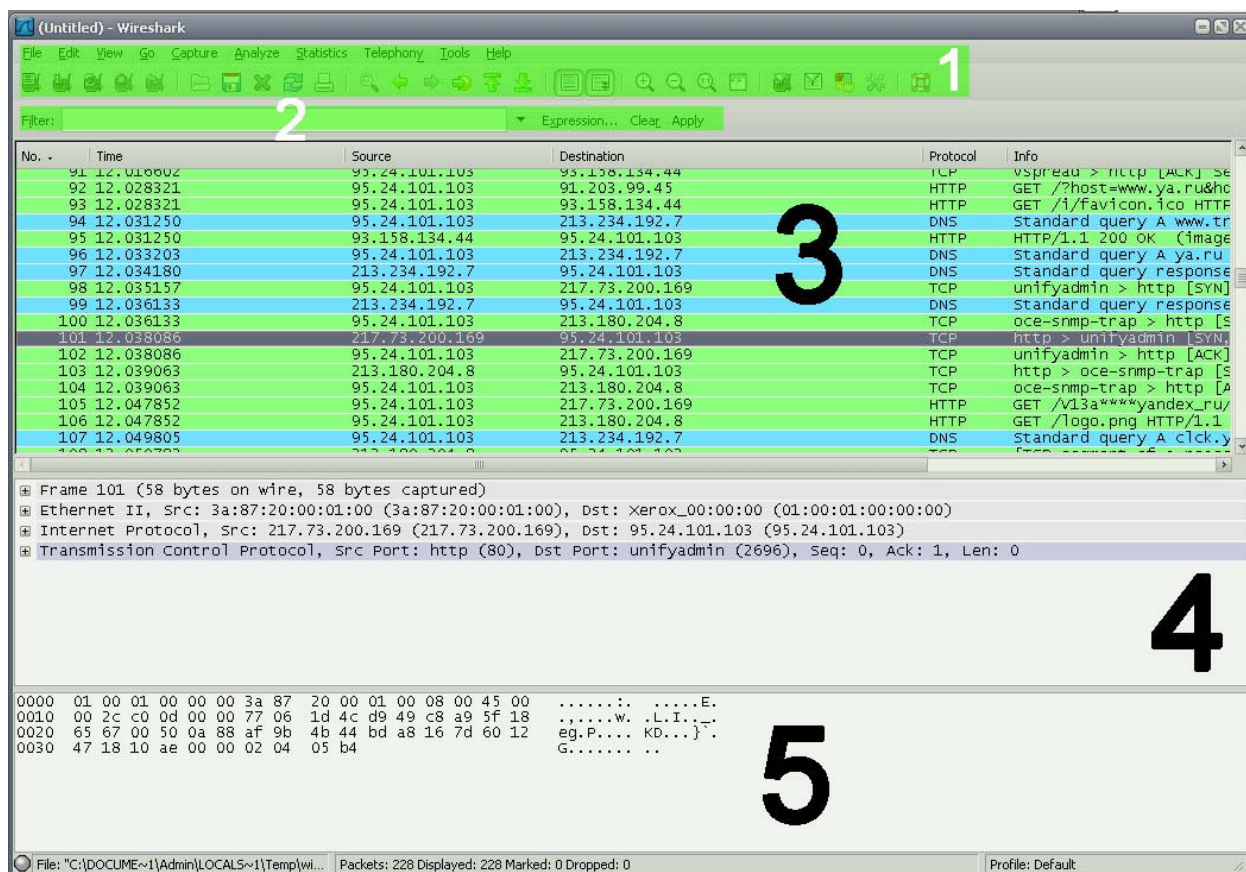


Рисунок 5. Окно отображения захваченного трафика.
















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 X.



Рисунок 6. Панель инструментов.

№	Кнопка	Название кнопки	Соответствующая опция в меню	Функции кнопки
1		Interfaces...	Capture / Interfaces...	Вызов списка активных сетевых адаптеров (Рисунок X).
2		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...	Заккрыть текущий отчёт о захваченном трафике.
9		Reload...	View / Reload...	Заккрыть и открыть заново текущий отчёт о захваченном трафике.
10		Print...	File / Print...	Распечатать текущий отчёт о захваченном трафике.
11		Zoom In...	View / Zoom In...	Увеличить размер шрифта.
12		Zoom Out...	View / Zoom Out...	Уменьшить размер шрифта.
13		Normal Size...	View / Normal Size...	Установить размер шрифта, используемый по умолчанию.
14		Preferences...	Edit / Preferences...	Вызов меню настроек.
15		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 X.



Рисунок 7. Панель фильтра.



№	Кнопка / Поле	Название Кнопки / поля	Функции кнопки / поля
1		Filter:	Вызов диалогового окна для создания и сохранения пользовательских фильтров (Рисунок X).
2		Filter Input	Поле ввода фильтра.
3			Вызов списка применённых ранее фильтров.
4		Expression...	Вызов диалогового окна, позволяющего выбирать фильтры из базы данных программы.
5		Clear	Очистить поле ввода фильтра.
6		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 8. Фильтр введен правильно.

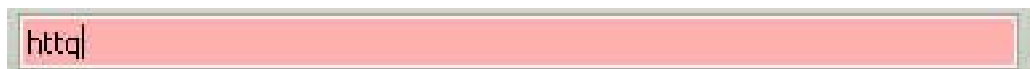


Рисунок 9. Фильтр введен неправильно.

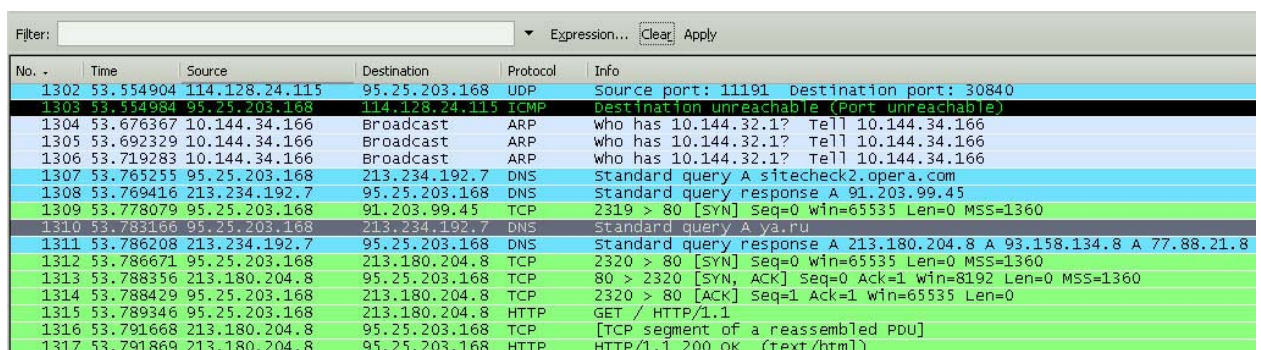
## Построение фильтров.

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 HTTP показан на рисунках X-Y.



No.	Time	Source	Destination	Protocol	Info
1302	53.554904	114.128.24.115	95.25.203.168	UDP	Source port: 11191 Destination port: 30840
1303	53.554984	95.25.203.168	114.128.24.115	ICMP	Destination unreachable (Port unreachable)
1304	53.676367	10.144.34.166	Broadcast	ARP	who has 10.144.32.1? Tell 10.144.34.166
1305	53.692329	10.144.34.166	Broadcast	ARP	who has 10.144.32.1? Tell 10.144.34.166
1306	53.719283	10.144.34.166	Broadcast	ARP	who has 10.144.32.1? Tell 10.144.34.166
1307	53.765255	95.25.203.168	213.234.192.7	DNS	Standard query A sitecheck2.opera.com
1308	53.769416	213.234.192.7	95.25.203.168	DNS	Standard query response A 91.203.99.45
1309	53.778079	95.25.203.168	91.203.99.45	TCP	2319 > 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1360
1310	53.783166	95.25.203.168	213.234.192.7	DNS	Standard query A ya.ru
1311	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
1312	53.786671	95.25.203.168	213.180.204.8	TCP	2320 > 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1360
1313	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
1314	53.788429	95.25.203.168	213.180.204.8	TCP	2320 > 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0
1315	53.789346	95.25.203.168	213.180.204.8	HTTP	GET / HTTP/1.1
1316	53.791668	213.180.204.8	95.25.203.168	TCP	[TCP segment of a reassembled PDU]
1317	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		Expression... Clear Apply			
No. -	Time	Source	Destination	Protocol	Info
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)
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	HTTP/1.1 200 OK (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=xBVRlPGv51toStugxx0HQ== HTTP/1.1
1336	54.077067	95.25.203.168	217.73.200.221	HTTP	GET /Vd3a***yandex.ru/ru/CP1251/tmsec=yandex_ua/0 HTTP/1.1
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	HTTP/1.1 200 OK
1348	54.132425	95.25.203.168	77.88.21.14	HTTP	GET /redir/dtype=stred/pid=17/cid=1729/*http://export.yandex.ru/morc
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 X и Y.

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

Таблица 1. Обозначения полей при построении фильтров.

Оператор		Значение	Примеры
<b>==</b>	<b>eq</b>	Равно	<b>ip.addr==192.168.1.1</b>  Отображать только те пакеты протокола IP, в которых сетевой адрес отправителя или получателя равен 192.168.1.1  <b>eth.dst==ff:ff:ff:ff:ff:ff</b>  Отображать только широковещательные (broadcast) кадры протокола Ethernet.



<b>!=</b>	<b>ne</b>	Не равно	<b>ip.dst==255.255.255.255</b>  Не отображать широковещательные (broadcast) пакеты протокола IP.
<b>&gt;</b>	<b>gt</b>	Больше	<b>tcp.dstport&gt;10000</b>  Отображать только те сегменты протокола TCP, в которых порт получателя больше 10000.
<b>&lt;</b>	<b>lt</b>	Меньше	<b>tcp.dstport&lt;1024</b>  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**

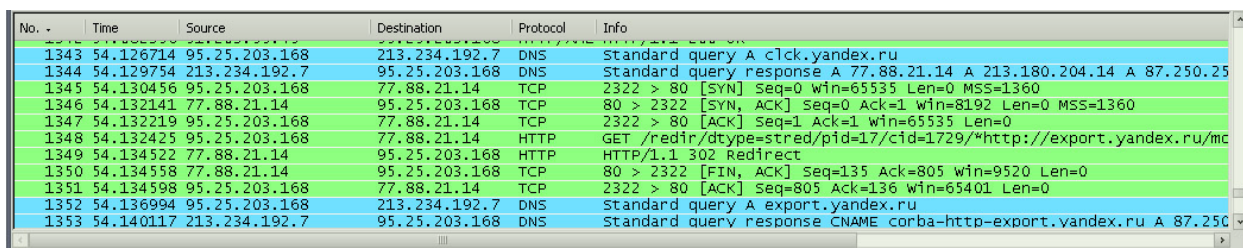
В качестве условия может использоваться как фильтрация по протоколам, так и фильтрация по значениям определённых полей в протоколах.

В таблице X представлены некоторые логические операторы.

Оператор		Значение	Примеры
<b>&amp;&amp;</b>	<b>and</b>	И	<b>ip.src==192.168.1.1 &amp;&amp; ip.dst==192.168.1.10</b>  Отображать только сообщения отправленные устройством с сетевым адресом 192.168.1.1 для устройства с сетевым адресом 192.168.1.10
<b>  </b>	<b>or</b>	ИЛИ	<b>eth.dst==ff:ff:ff:ff:ff:ff    ip.dst==255.255.255.255</b>  Отображать только широковещательные кадры протокола Ethernet или пакеты протокола IP.
<b>!</b>	<b>not</b>	НЕ (Отрицание)	<b>!arp</b>  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 query A c1ck.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

**Рисунок 12. После списка захваченных PDU.**

Сводная информация выводится в виде таблицы со следующими полями:

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

На рисунке X представлен пример сводной информации о захваченной PDU.

No. -	Time	Source	Destination	Protocol	Info
1343	54.126714	95.25.203.168	213.234.192.7	DNS	Standard query A click.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	30.368904	172.16.1.50	it-server.clas	DNS	standard query A personal.avira-update.com
299	34.369097	172.16.1.50	it-server.clas	DNS	standard query A personal.avira-update.com
304	42.369969	172.16.1.50	it-server.clas	DNS	standard query PTR 1.0.0.127.in-addr.arpa
305	42.370315	it-server.clas	172.16.1.50	DNS	standard query response PTR localhost
395	52.563781	it-server.clas	172.16.1.50	DNS	standard query response, server failure
463	85.546583	172.16.1.50	it-server.clas	DNS	standard query PTR 2.1.16.172.in-addr.arpa
464	85.547026	it-server.clas	172.16.1.50	DNS	standard query response, No such name
534	115.38268	172.16.1.50	it-server.clas	DNS	standard query PTR 2.1.16.172.in-addr.arpa
535	115.38314	it-server.clas	172.16.1.50	DNS	standard query response, No such name

<p>Frame 395 (85 bytes on wire, 85 bytes captured)</p> <p>Ethernet II, Src: it-server.class.mitht.ru (00:04:23:bf:bc:19), Dst: Foxconn_be:5a:27 (00:01:6c:be:5a:27)</p> <p>Internet Protocol, Src: it-server.class.mitht.ru (172.16.1.2), Dst: 172.16.1.50 (172.16.1.50)</p> <p>User Datagram Protocol, Src Port: 53 (53), Dst Port: 1343 (1343)</p> <p>Source port: 53 (53)</p> <p>Destination port: 1343 (1343)</p> <p>Length: 51</p> <p>Checksum: 0x49de [validation disabled]</p> <p>Domain Name System (response)</p>	2
--	---

**Рисунок 14. Информационное поле программы.**

Выделенная область	Описание и функции
<b>1</b>	Выделенная запись в листе списка захваченных PDU. Запись выделяется нажатием левой кнопки мыши. Программа помечает текущую выделенную запись серым цветом.
<b>2</b>	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.

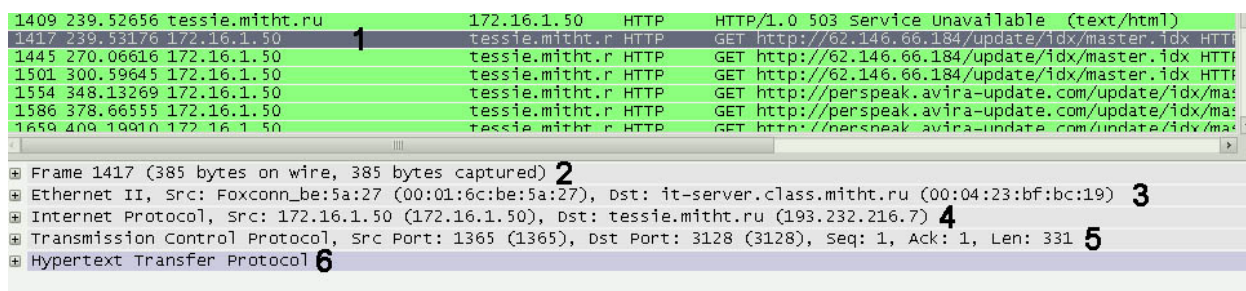


Рисунок 15. Информация о захваченном PDU протокола HTTP.

Выделенная область	Описание и функции
<b>1</b>	Выделенное PDU в поле списка захваченных PDU. В соответствии с установками по умолчанию, программа отмечает выделенное PDU серым цветом.
<b>2</b>	<b>+ Frame 1417</b> В этом вложенном списке содержится справочная информация о захваченном PDU, такая как: время захвата, длина PDU и т.д.
<b>3</b>	<b>+ Ethernet II,</b> В этом вложенном списке расположена информация о заголовке протокола канального (Data Link) уровня. В данном случае это протокол Ethernet.
<b>4</b>	<b>+ Internet Protocol,</b> В этом вложенном списке расположена информация о заголовке протокола сетевого (Network) уровня. В данном случае это протокол IP.
<b>5</b>	<b>+ Transmission Control Protocol,</b> В этом вложенном списке расположена информация о заголовке протокола транспортного (Transport) уровня. В данном случае это протокол TCP.
<b>6</b>	<b>+ Hypertext Transfer Protocol</b> В 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 X.

Зелёным цветом выделены поля, выводимые программой.

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

```
⊞ 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)
  ⊞ Destination: it-server.class.mitht.ru (00:04:23:bf:bc:19)
  ⊞ Source: 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
<b>Destination</b>	<b>Destination: it-server.class.mitht.ru (00:04:23:bf:bc:19)</b> Интерпретация аналогична интерпретации информации из заголовка списка.
<b>Source</b>	<b>Source: Foxconn_be:5a:27 (00:01:6c:be:5a:27)</b> Интерпретация аналогична интерпретации информации из заголовка списка.
<b>Type</b>	<b>Type: IP (0x0800)</b> – 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 Type: <b>0x0806</b> – ARP, <b>0x86DD</b> – IPv6.

## Протокол IP.

Протокол IP — 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	Header length	Differentiated Services Field	Total Length	
Identification			Flag	Fragment Offset
Time to Live		Protocol	Header Checksum	
Source				
Destination				
Options				Padding

```
⊕ 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)
  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)
⊕ 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.

**Dst: tessie.mitht.ru (193.232.216.7)** – Сетевой 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
<b>Time to Live</b>	<b>Time to live: 128</b> – Максимально возможное количество сетевых устройств, которые могут обработать и передать пакет дальше по сети равняется 128.
<b>Protocol</b>	<b>Protocol: TCP (0x06)</b> – 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: <b>0x01</b> – ICMP, <b>0x11</b> - UDP
<b>Source</b>	<b>Source: 172.16.1.50 (172.16.1.50),</b>  Интерпретация аналогична интерпретации информации из заголовка списка.
<b>Destination</b>	<b>Destination: tessie.mitht.ru (193.232.216.7)</b>  Интерпретация аналогична интерпретации информации из заголовка списка.

## Протокол TCP

Протокол TCP – 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 X.

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 TCP.

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
<b>Source port</b>	<b>Source Port: 1365 (1365)</b>  Интерпретация аналогична интерпретации информации из заголовка списка.
<b>Destination port</b>	<b>Destination Port: 3128 (3128)</b>  Интерпретация аналогична интерпретации информации из заголовка списка.
<b>Sequence number и Acknowledgement number</b>	<b>Sequence number: 1 (.relative sequence number)</b> <b>[Next sequence number: 332 (relative sequence number)]</b> <b>Acknowledgement number: 1 (relative ack number)</b>  Поля, использующиеся для организации надёжной доставки информации между приложениями.
<b>Window size</b>	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 X.

Зелёным цветом выделены поля, выводимые программой.

2 Bytes	2 Bytes
<b>Source Port</b>	<b>Destination Port</b>
<b>Length</b>	<b>Checksum CRC</b>

```
⊞ Frame 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
<b>Source port</b>	<b>Source Port: 1364 (1364)</b> Интерпретация аналогична интерпретации информации из заголовка списка.
<b>Destination port</b>	<b>Destination Port: 88 (88)</b> Интерпретация аналогична интерпретации информации из заголовка списка.
<b>Length</b>	Длина датаграммы.

## Этапы старта программы

### 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.

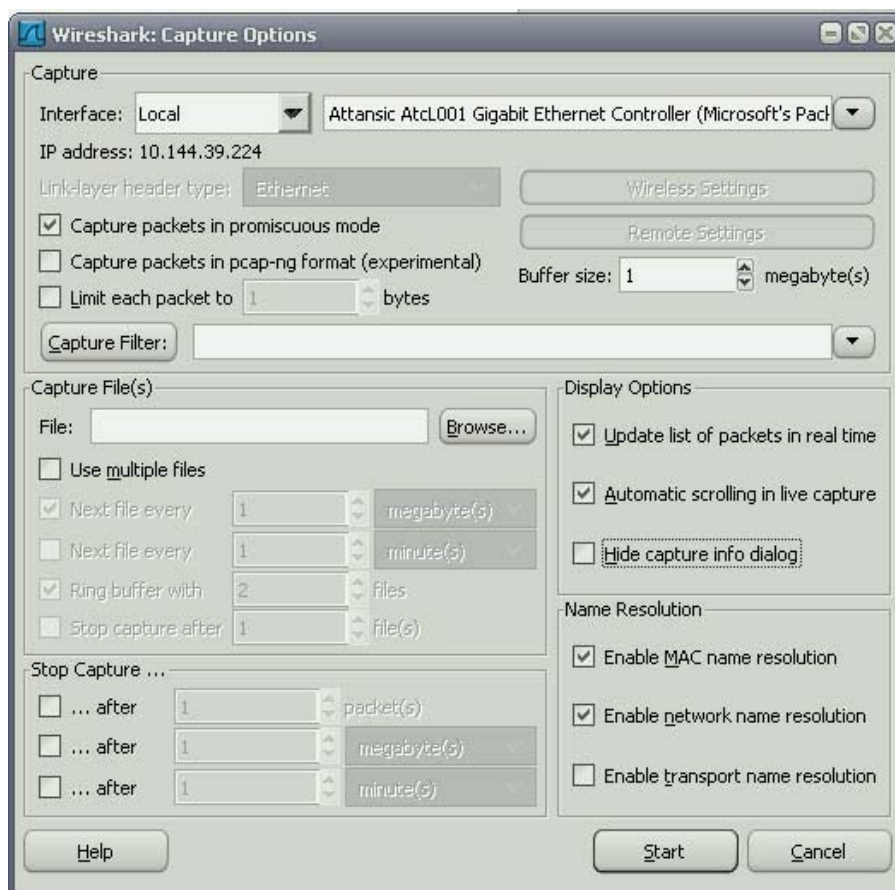
### 2. Настроить параметры захвата сетевого трафика.

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.



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.