Лабораторная работа #2

Анализ сетевого трафика с помощью программы «Wireshark».

Содержание

Этапы выполнения работы

1. **Запустить программу Wireshark.**

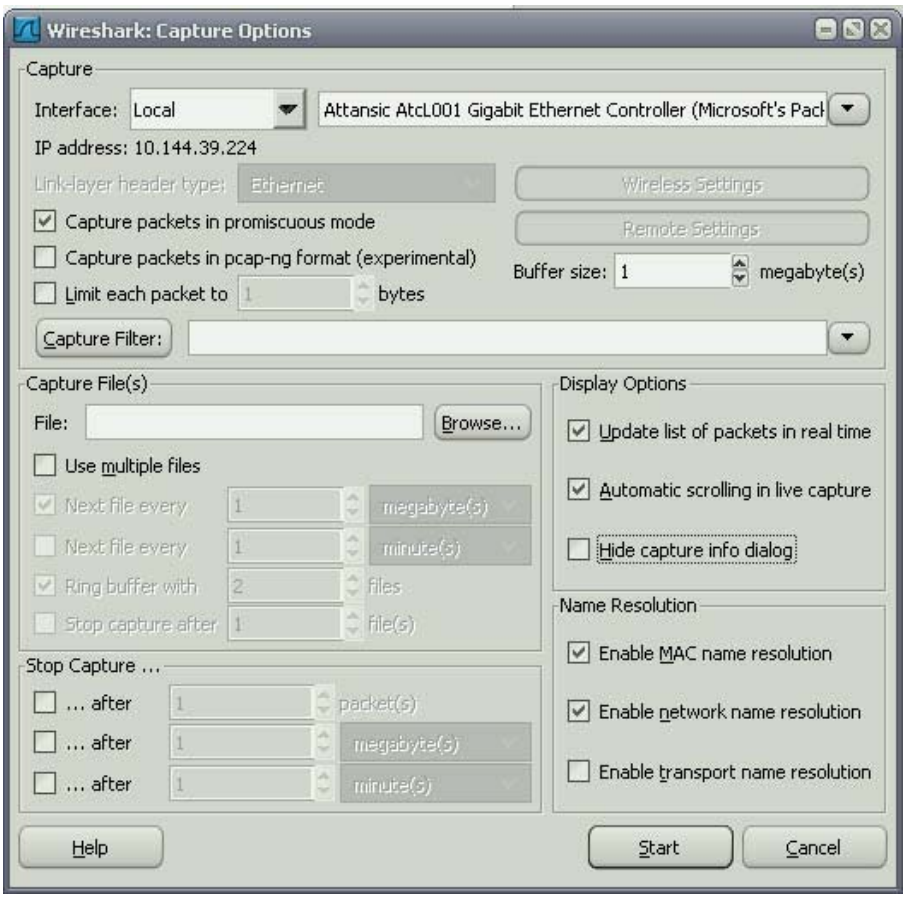
Для запуска программы необходимо нажать: **Пуск** > **Программы** > **Wireshark**, либо два раза щёлкнуть левой кнопкой мыши по ярлыку программы на рабочем столе.

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.



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**.

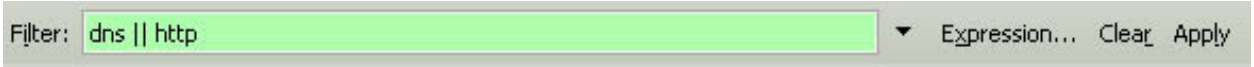
3. **Запустить процесс захвата трафика.**

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**”.



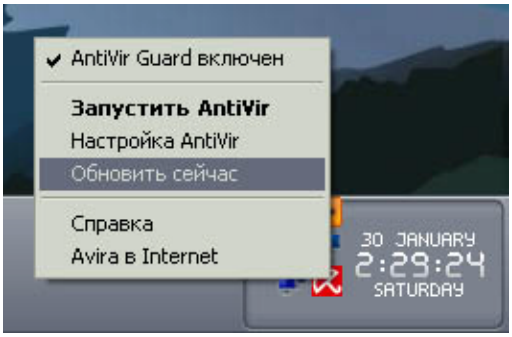
4.2 Нажать кнопку **Apply.**

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**.



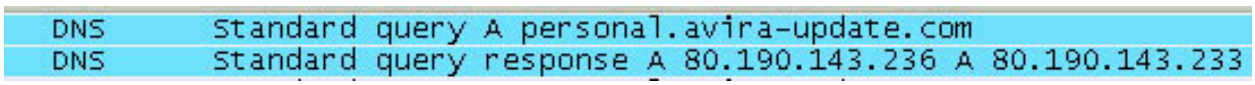
6. **Остановить захват трафика.**

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

7. **Проанализировать трафик, захваченный программой.**

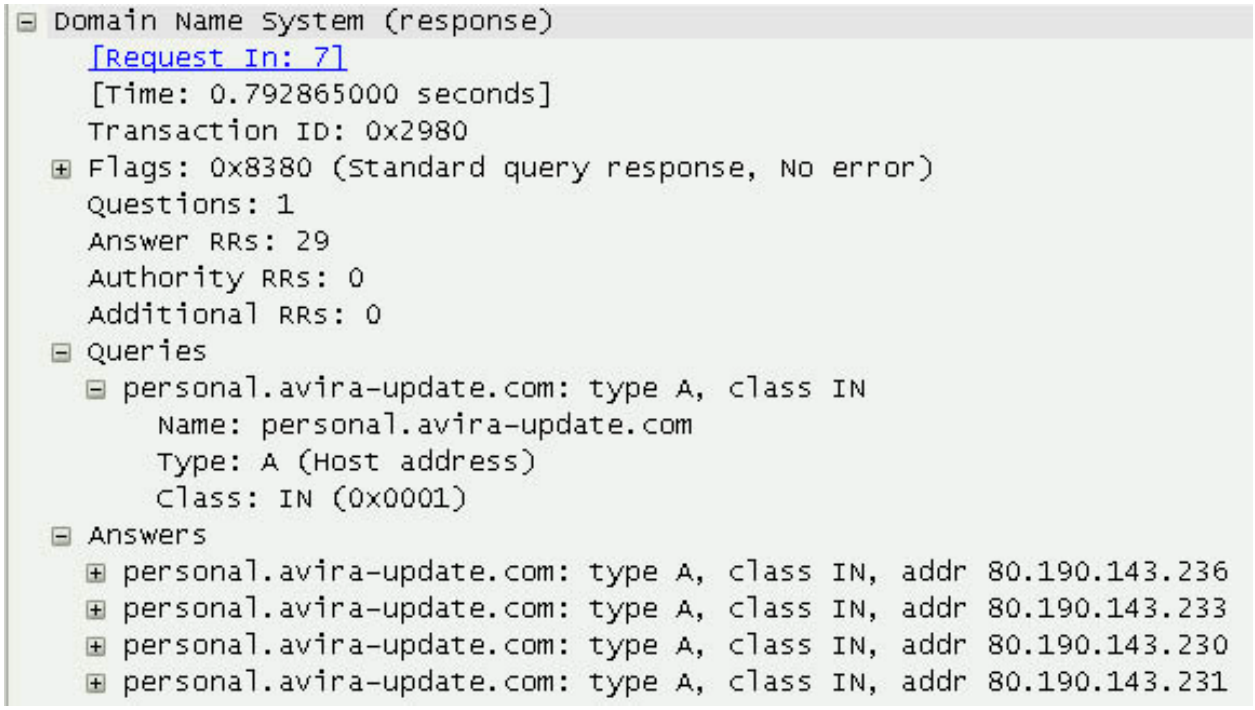
При анализе трафика необходимо произвести следующие действия:

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

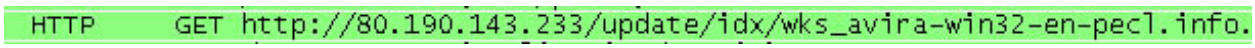


7.2 Посмотрев содержимое DNS-запроса и DNS-ответа выяснить и записать в отчёт следующую информацию:

- DNS имя сервера обновлений антивируса.
- Любые 5 сетевых адресов сервера обновлений.



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



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).

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

- Сетевой адрес компьютера.
- MAC-адрес компьютера.
- Сетевой адрес шлюза.
- MAC-адрес шлюза.
- IP-адрес прокси-сервера

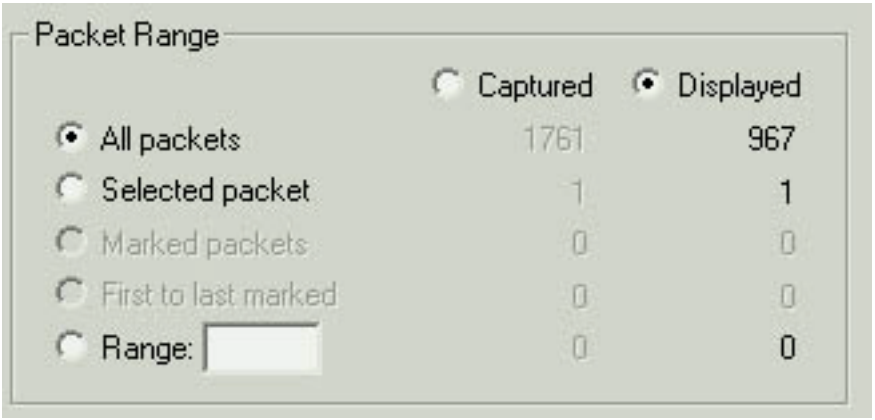
- DNS имя прокси-сервера.
- Сетевой адрес DNS-сервера.
- Протокол транспортного уровня, который использует сервис DNS.
- Порт, на который осуществляется DNS-запрос.
- Протокол транспортного уровня, который использует протокол HTTP.
- Порт, на который осуществляется запрос обновления антивируса по протоколу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



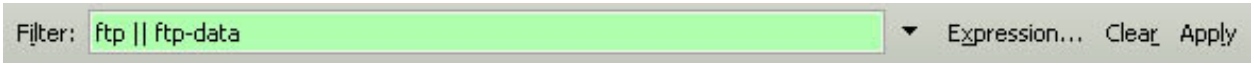
9. Заново запустить захват трафика.

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 фильтра выражение: “**ftp || ftp-data**”.



4.4 Нажать кнопку **Apply.**

11. Скачать файл с FTP-сервера.

Для того, чтобы скачать файл в адресной строке браузера необходимо набрать **ftp://172.16.1.10/file.zip** 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.
- MAC-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 X изображено окно, которое появляется при запуске программы.

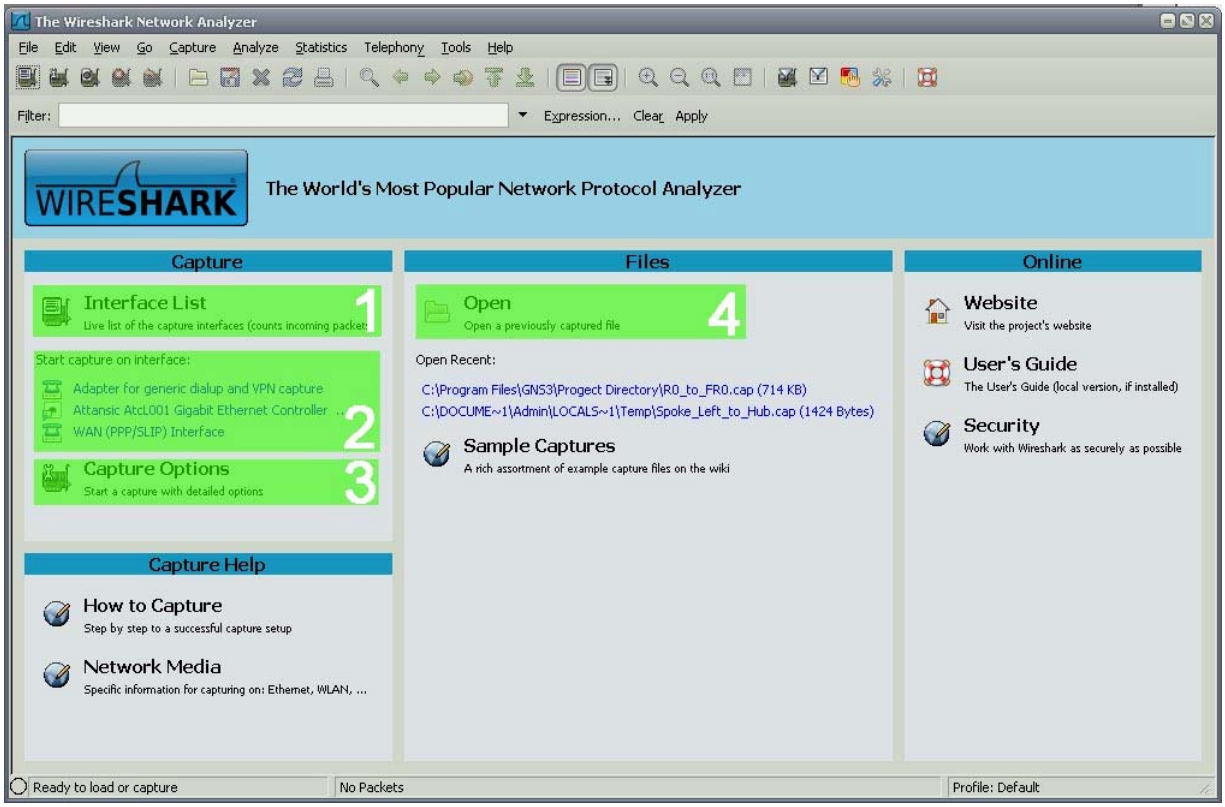


Рисунок 1. Стартовый интерфейс программы.

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.

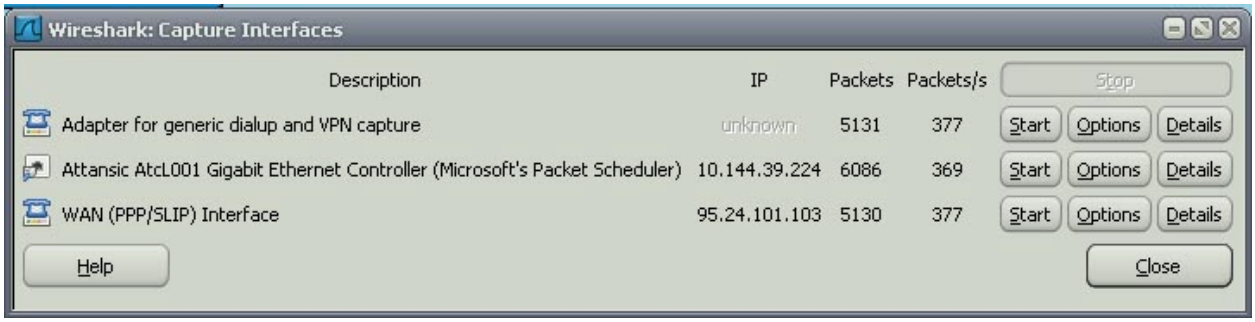


Рисунок 2. Список активных сетевых адаптеров.

Список активных адаптеров имеет вид интерактивной таблицы со следующими полями:

Поле таблицы	Описание
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.

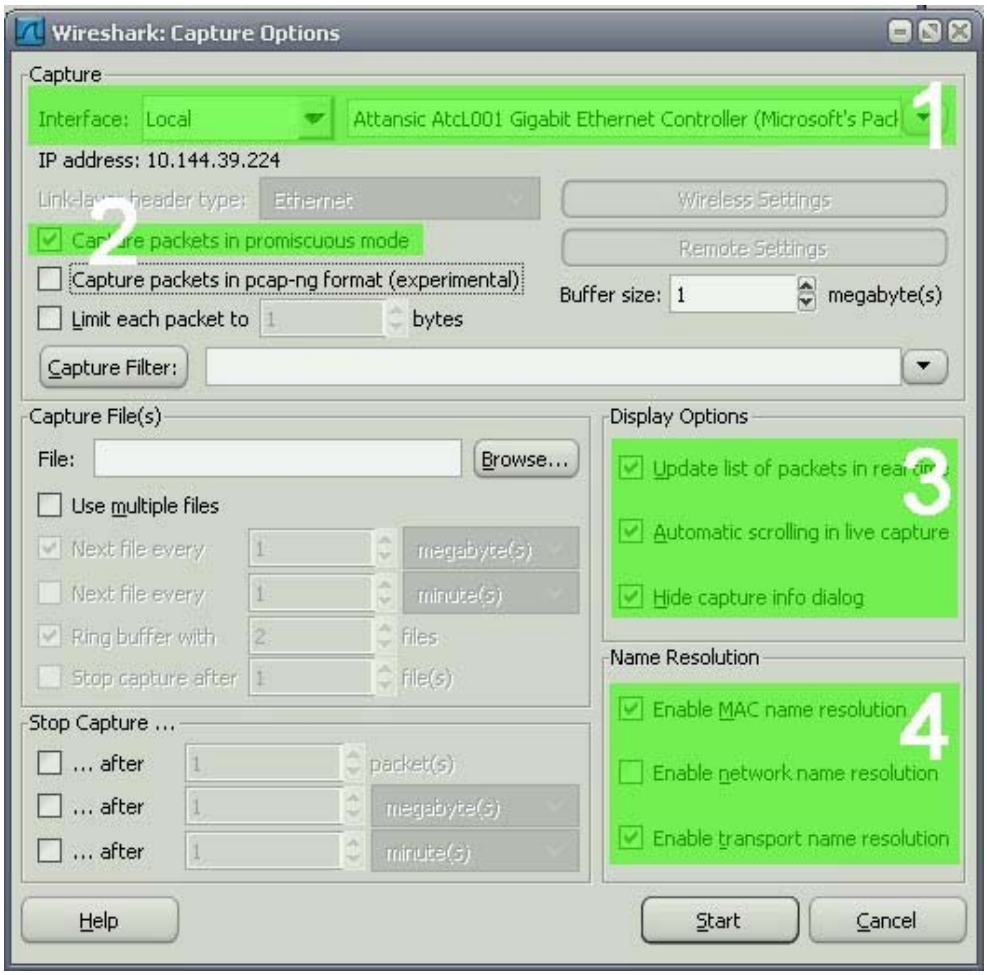


Рисунок 3. Окно настроек захвата сетевого трафика.

Выделенная область	Описание и функции
1	Выбор интерфейса для захвата трафика. 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	**Capture 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.
3	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. **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.
4	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. Примечание: если включена опция преобразования сетевых имён, то в некоторых случаях программа выводит DNS имя вместо MAC-адреса. **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**

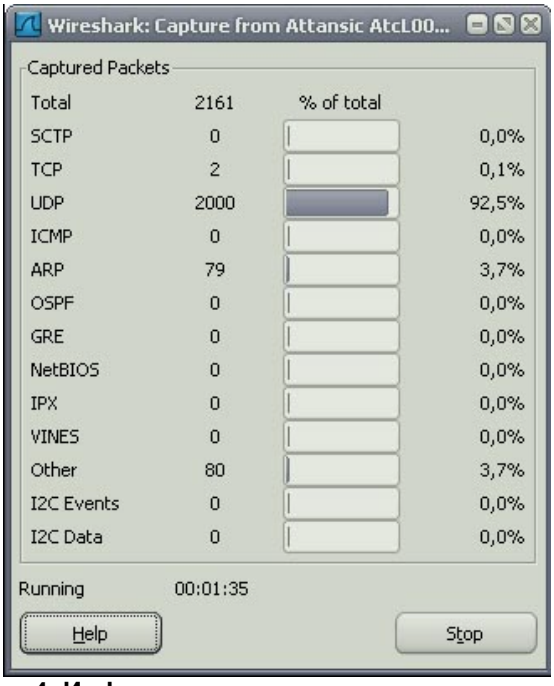


Рисунок 4. Информационно-диалоговое окно захвата.

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.

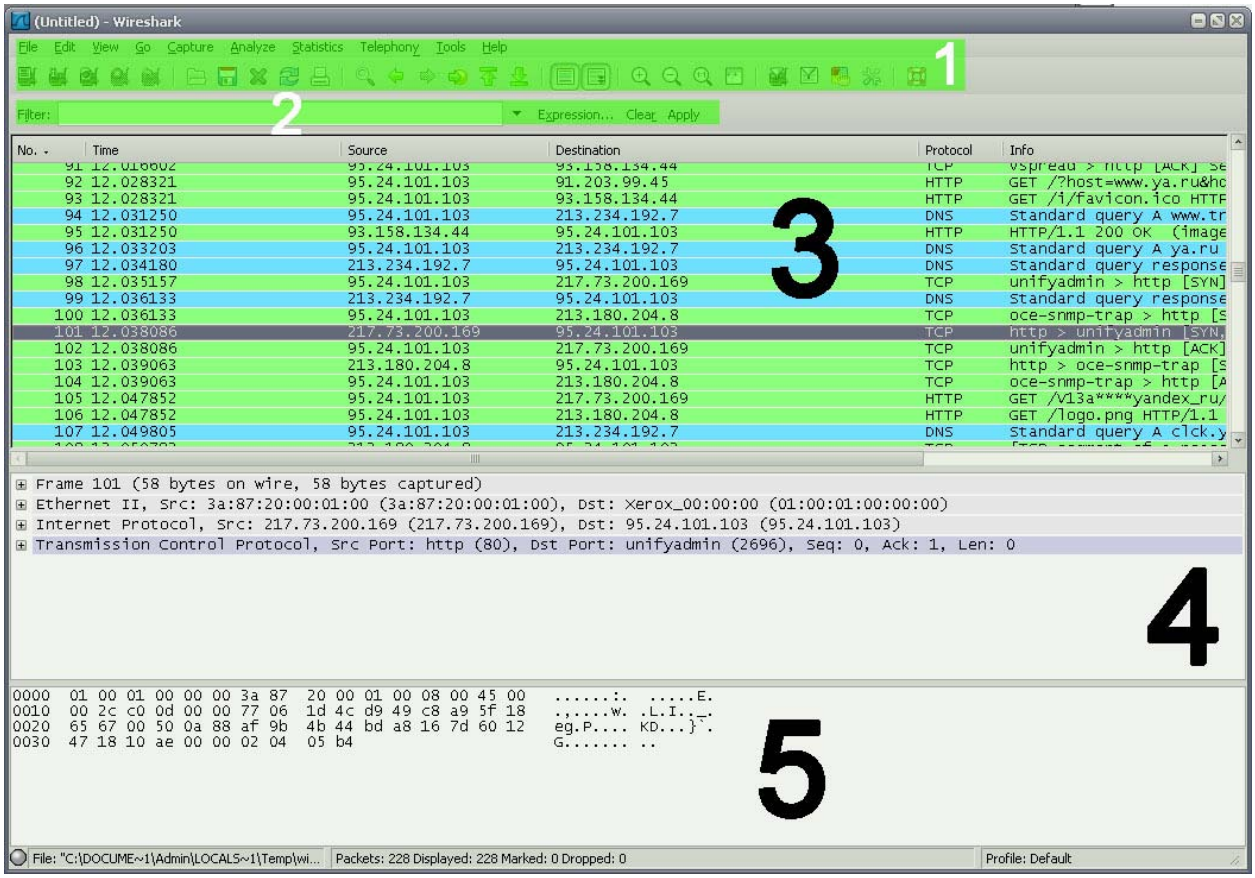


Рисунок 5. Окно отображения захваченного трафика.

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…	Закрыть текущий отчёт о захваченном трафике.
9		Reload…	View / Reload…	Закрыть 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.

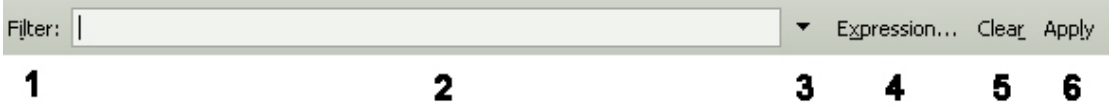


Рисунок 7. Панель фильтра.

№	Кнопка / Поле	Название Кнопки / поля	Функции кнопки / поля
1	Filter:	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…	Expression…	Вызов диалогового окна, позволяющего выбирать фильтры из базы данных программы.
5	Clear	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 8. Фильтр введён правильно.

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 HTTP показан на рисунках X-У.

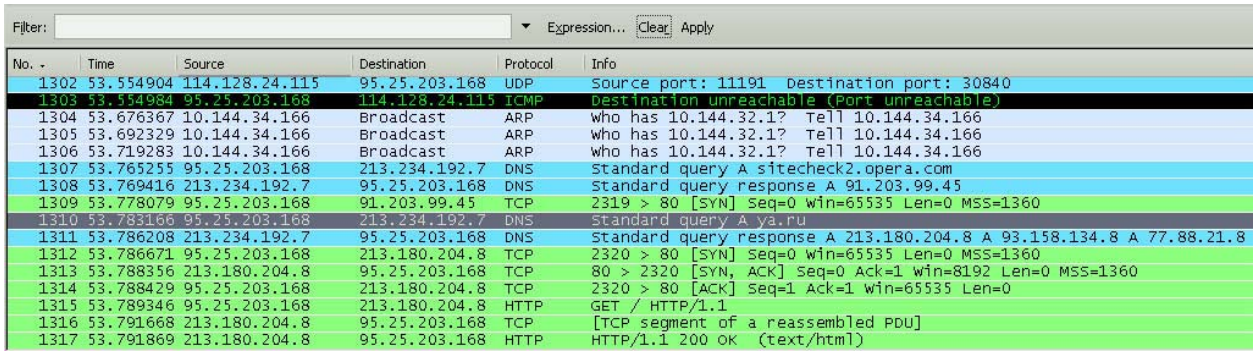


Рисунок 10. Вывод программы до применения фильтра.

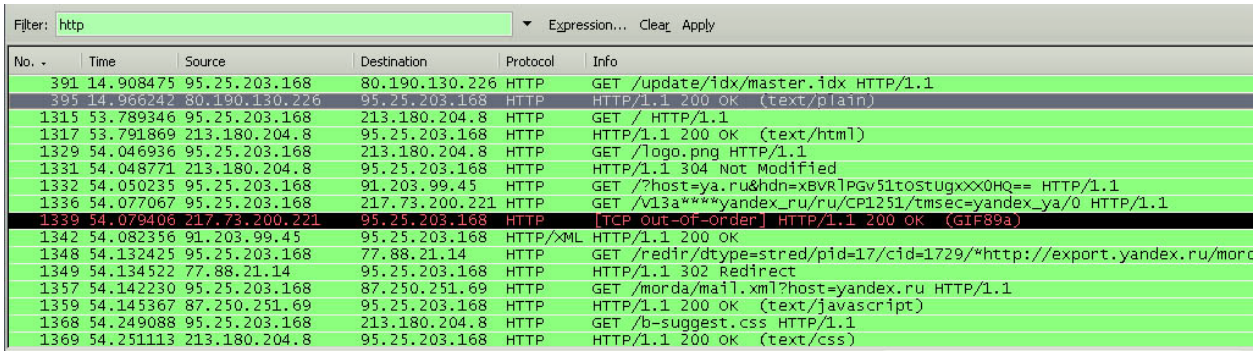


Рисунок 11. Вывод программы после применения фильтра.

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 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 (ACK) протокола TCP
tcp.port	Порт источника или получателя в сегменте протокола TCP.
tcp.dstport	Порт получателя в сегменте протокола TCP.
tcp.srcport	Порт источника в сегменте протокола TCP.
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.

Оператор		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 **eth.dst==ff:ff:ff:ff:ff:ff** 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 TCP, 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 X 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.

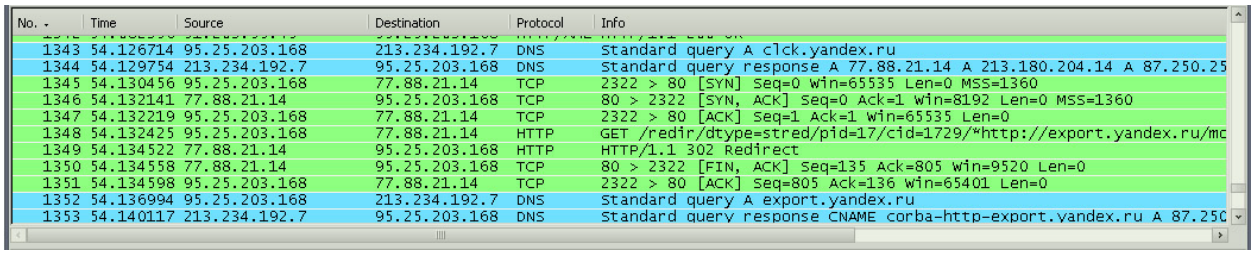


Рисунок 12. После списка захваченных PDU.

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.

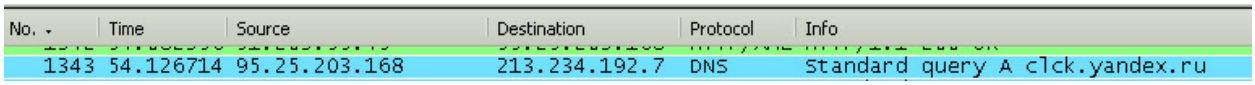


Рисунок 13. Пример записи в списке захваченных PDU.

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.

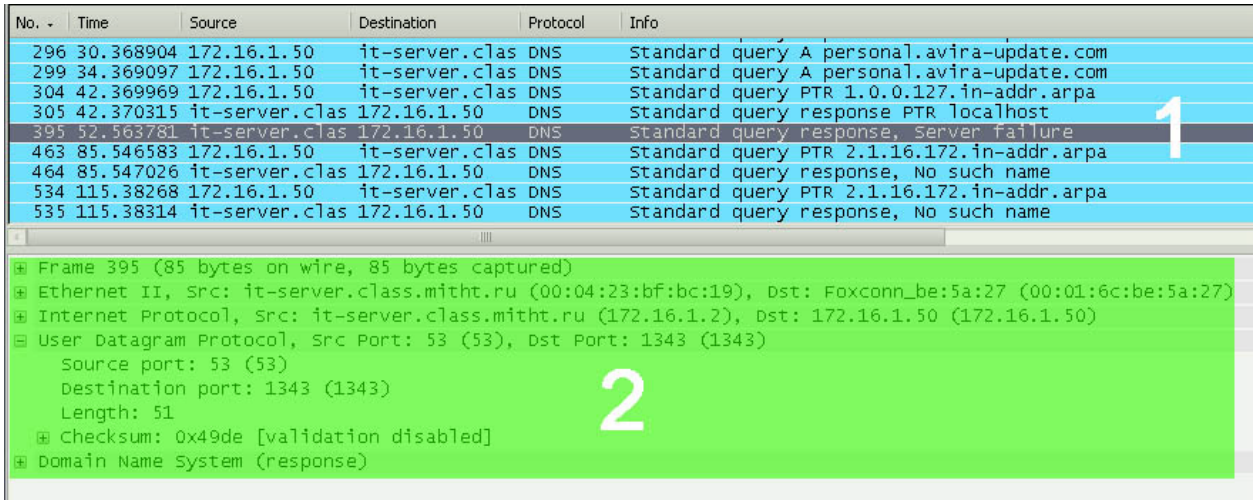


Рисунок 14. Информационное поле программы.

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.

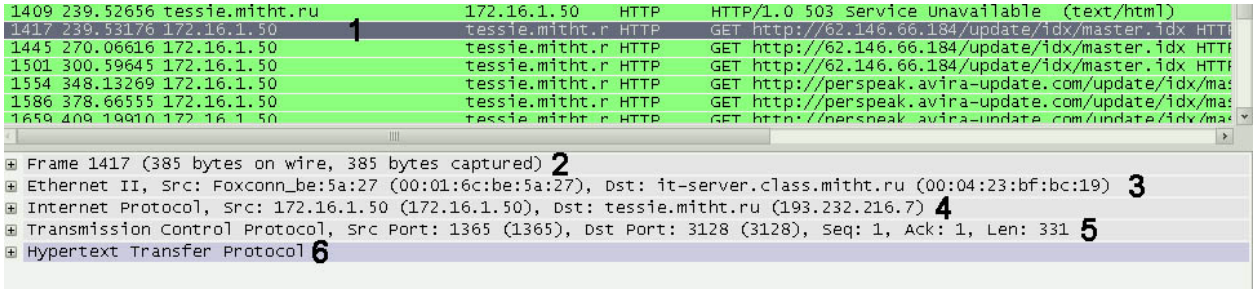


Рисунок 15. Информация о захваченном PDU протокола HTTP.

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	⊞ Frame 1417 В этом вложенном списке содержится справочная информация о захваченном PDU, такая как: время захвата, длинна PDU и т.д.
3	⊞ Ethernet II, В 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, В этом вложенном списке расположена информация о заголовке протокола транспортного (Transport) уровня. В данном случае это протокол TCP.
6	⊞ Hypertext Transfer Protocol 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

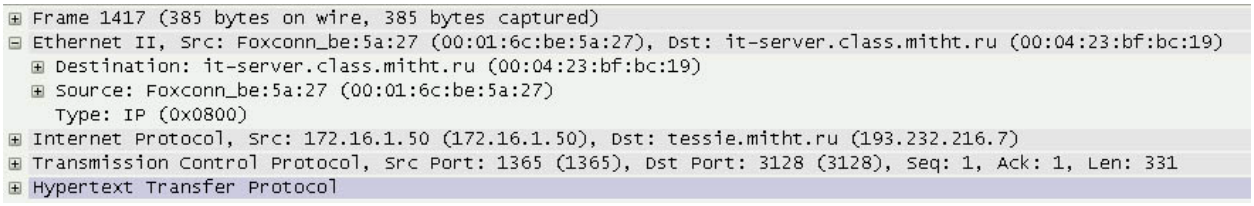


Рисунок 16. Поля заголовка кадра протокола Ethernet.

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.

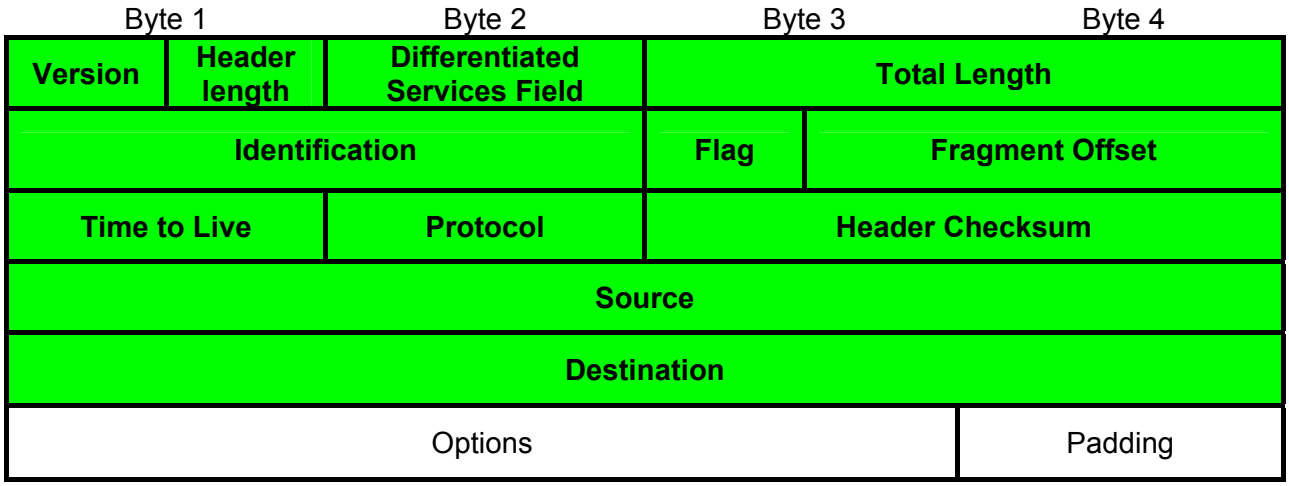
Поле	Описание
Destination	**Destination: it-server.class.mitht.ru (00:04:23:bf:bc:19)** Интерпретация аналогична интерпретации информации из заголовка списка.
Source	**Source: Foxconn_be:5a:27 (00:01:6c:be:5a:27)** Интерпретация аналогична интерпретации информации из заголовка списка.
Type	**Type: IP (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 Type: **0x0806 –** ARP, **0x86DD** – 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.




```
⊞ 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
Time to Live	**Time to live: 128** – Максимально возможное количество сетевых устройств, которые могут обработать и передать пакет дальше по сети равняется 128.
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 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.

<table>
<tr><td></td><td colspan="2">2 Bytes</td><td>2 Bytes</td></tr>
<tr><td colspan="2">Source port</td><td colspan="2">Destination Port</td></tr>
<tr><td colspan="4">Sequence number</td></tr>
<tr><td colspan="4">Acknowledgement number</td></tr>
<tr><td>Header Length</td><td>(Reserved)</td><td>Flags</td><td>Window Size</td></tr>
<tr><td colspan="2">TCP Checksum</td><td colspan="2">Urgent Pointer</td></tr>
<tr><td colspan="4">Options (if any)</td></tr>
</table>

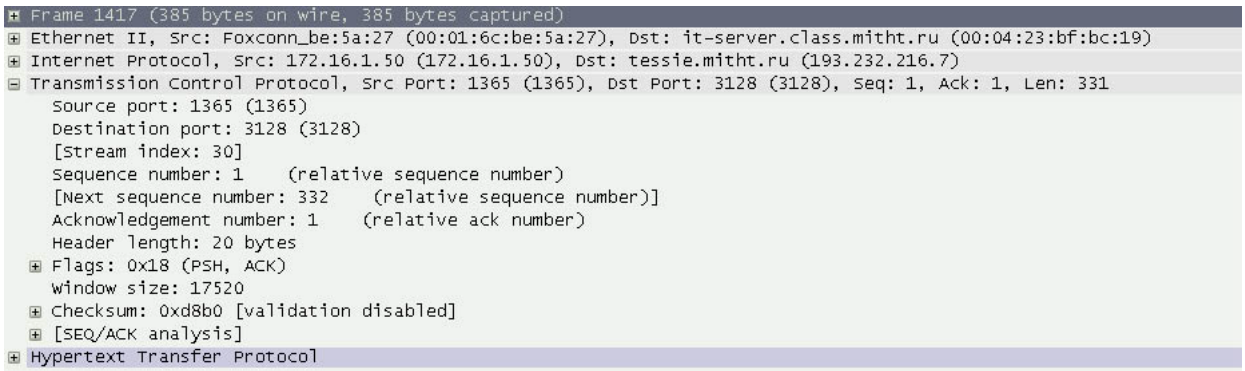


Рисунок 18. Поля заголовка сегмента TCP.

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
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 number**	**Sequence number: 1 (.relative sequence number)** **[Next sequence number: 332 (relative sequence number)]** **Acknowledgement number: 1 (relative ack 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 X.

Зелёным цветом выделены поля, выводимые программой.

2 Bytes	2 Bytes
Source Port	**Destination Port**
Length	**Checksum CRC**

```
⊞ 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
Source port	**Source Port: 1364 (1364)** Интерпретация аналогична интерпретации информации из заголовка списка.
Destination port	**Destination Port: 88 (88)** Интерпретация аналогична интерпретации информации из заголовка списка.
Length	Длина датаграммы.