

Федеральное агентство связи Российской Федерации
Государственное образовательное учреждение
высшего профессионального образования
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»

А.Е. Костюкович

Методические указания
к лабораторной работе № 4
**«Изучение анализатора
протоколов Wireshark»**

Новосибирск – 2011

А.Е. Костюкович

Аннотация.

Методические указания к лабораторной работе для дисциплины «Информационные сервисы для СПС». Могут быть также использованы в процессе изучения дисциплин "Мультисервисные сети" и "Пакетная телефония".

В данной лабораторной работе студенту предоставляется возможность получить навыки работы с одним из самых известных анализаторов протоколов.

Кафедра АЭС

Ил. 15, список лит. - 13

Рецензент – Мелентьев О.Г.

По направлению – 210400 - Телекоммуникации

Утверждено редакционно-издательским советом СибГУТИ
в качестве методических указаний

© Сибирский государственный
университет телекоммуникаций
и информатики, 2011 г.

Оглавление		
		Стр.
1. Цель работы		
2. Описание основных возможностей анализатора Wireshark		
2.1. Установка анализатора Wireshark на Вашем компьютере		
2.2. Начало работы с Анализатором Wireshark. Основные возможности		
3. Порядок выполнения работы		
4. Правила оформления отчета		
5. Контрольные вопросы		
6. Литература		

1. Цель работы:

- 1.1. Выполнить инсталляцию программы анализатора протоколов Wireshark на Вашем компьютере
- 1.2. На примере трассировки процесса PING – изучить основные возможности анализатора протоколов Wireshark и Приобрести навыки трассировки протоколов.
- 1.3. Выполнить анализ сделанных трассировок и отразить это в отчете

2. Анализатор протоколов Wireshark. Описание основных возможностей.

Wireshark — это приложение-анализатор, которое «знает» структуру самых различных сетевых протоколов, и поэтому позволяет разобрать сетевой пакет, отображая значение каждого поля протокола любого уровня.

Wireshark – позволяет перехватывать и расшифровывать все известные протоколы, использующие в качестве транспорта среду Ethernet.

Любая информация, передаваемая в кадрах Ethernet с Вашего компьютера или на Ваш компьютер – перехватывается приложением Wireshark, записывается на Ваш диск и может быть впоследствии Вами проанализирована со всех позиций – на предмет информационной безопасности (наличия на Вашем компьютере программ-шпионов и других нежелательных приложений), загрузки интерфейса доступа к Вашему провайдеру (измерения скорости передачи, наличия фонового трафика, объемов переданного и принятого трафика и т.п.) и т.д.

Данная программа широко используется для поиска и устранения различных неисправностей, изучения сетевых протоколов и т.д.

С основными возможностями этой программы Вы познакомитесь ближе, выполнив данную работу!

Работа с данным приложением начинается с установки анализатора Wireshark на Вашем Компьютере.

2.1 Установка анализатора Wireshark на Вашем Компьютере

2.1.1 Скачайте программу для инсталляции анализатора Wireshark на Вашем с сайта разработчика - <http://www.wireshark.org/download.html> .

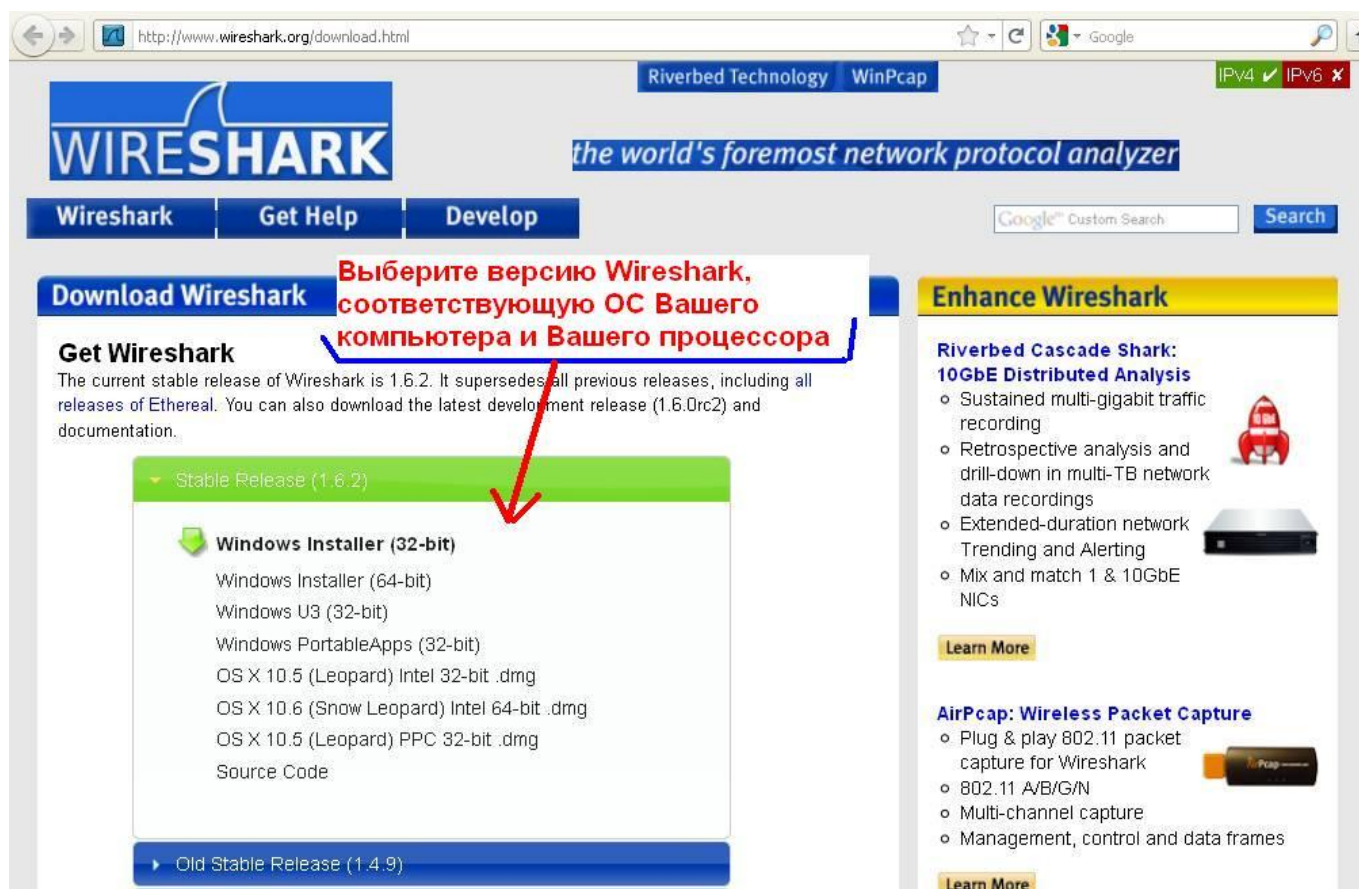


Рисунок 1 - Окно сайта разработчика программы анализатора Wireshark

Внимание!!! Для корректной установки и последующей работы – перед скачиванием программы определитесь с версией Wireshark, соответствующей версии программно-аппаратных средств Вашего компьютера.

Для установления соответствия – определите на своем компьютере:

- Тип ОС (Windows, Linux, ...) и
- Разрядность процессора – 32-х или 64-х разрядный.

Разрядность процессора определяется разрядностью шины данных. Большинство компьютеров возрастом не старше 2-х лет являются 64-х разрядными. На таких компьютерах будут работать обе версии Wireshark – и 32-х и 64-х разрядные.

Если же у Вас 32-х разрядный процессор, или Вы не уверены в том, какой у Вас процессор – то Вам необходимо скачать 32-х разрядную версию Wireshark.

Для Windows это - <http://wiresharkdownloads.riverbed.com/wireshark/win32/wireshark-win32-1.6.2.exe>

2.1.2 **Запустите процесс инсталляции на Вашем компьютере**. Следуйте подсказкам по умолчанию, подтверждая установку всех предлагаемых компонент, нажатием кнопки “**NEXT**”, и по завершении всех процессов инсталляции – с программой можно работать.

Внимание!!! Рассматривайте эту программу не только как приложение, которое надо изучить для выполнения лабораторных работ, но **в первую очередь, как приложение, которое будет полезно Вам** как на Вашем домашнем компьютере, так и в работе по получаемой специальности (Wireshark – наиболее широко используемый и доступный анализатор-сниффер как в среде системных администраторов, так и среди хакеров).

2.2 **Начало работы с Анализатором Wireshark. Основные возможности.**

Чтобы запустить данное приложение необходимо два раза щелкнуть по соответствующему ярлыку в папке с установленной программой.

Все возможности данной программы невозможно изучить в масштабах одной лабораторной работы.

В данной работе Wireshark используется в качестве инструмента для анализа сетевых пакетов, генерируемых Web-приложениями и некоторыми другими службами.

Однако, поскольку фильтры в процессе выполнения данной работы не используются, то после окончания работы программы Wireshark, на Вашем диске остается файл в котором хранятся все перехваченные пакеты от всех сетевых служб, запущенных и активных в данный момент на Вашем компьютере (**даже от тех служб, о которых Вы не подозреваете!**).

Ниже приводятся лишь краткое описание работы с программой для выполнения лабораторной работы.

Главное окно программы Wireshark представлено на рисунке 2.

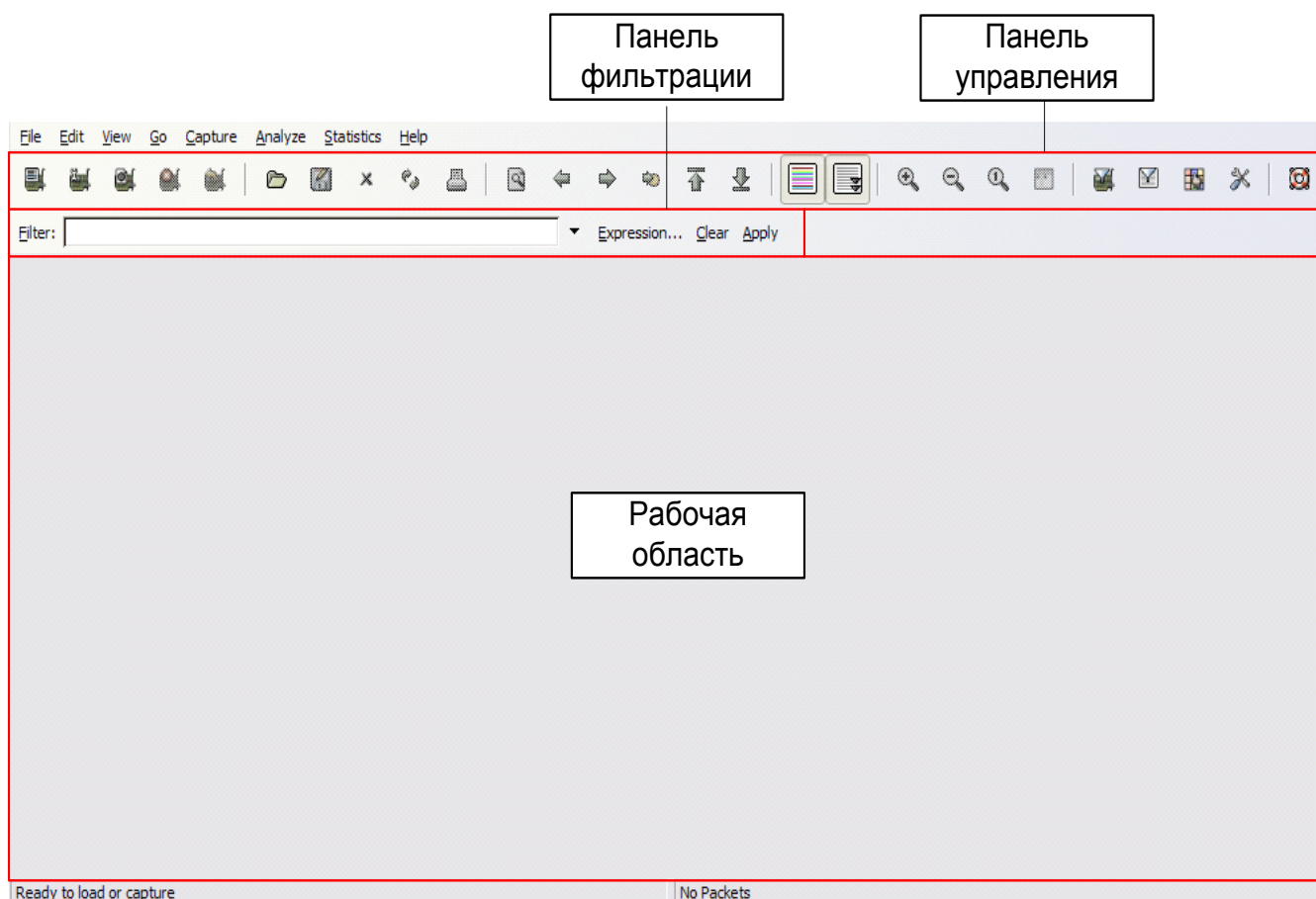


Рисунок 2 - Главное окно программы-анализатора Wireshark

Панель управления позволяет управлять основными возможностями приложения, например, начать перехват сетевых пакетов, открыть сохраненную ранее сессию перехвата пакетов и т.д.

Панель фильтра дает возможность отфильтровать ненужные пакеты и оставить только необходимые. Фильтрацию можно осуществить, написав в соответствующем поле маску фильтрации (например, «SIP|UDP» - будут отображаться только пакеты, содержащие поля протоколов SIP и UDP).

В рабочей области – отображаются перехваченные пакеты (верхняя часть рабочей области) и расшифровка каждого поля сетевого пакета (нижняя часть рабочей области).

В пункте меню **Capture** (фиксация, перехват) выберите **Options**.
У Вас откроется следующее окно:

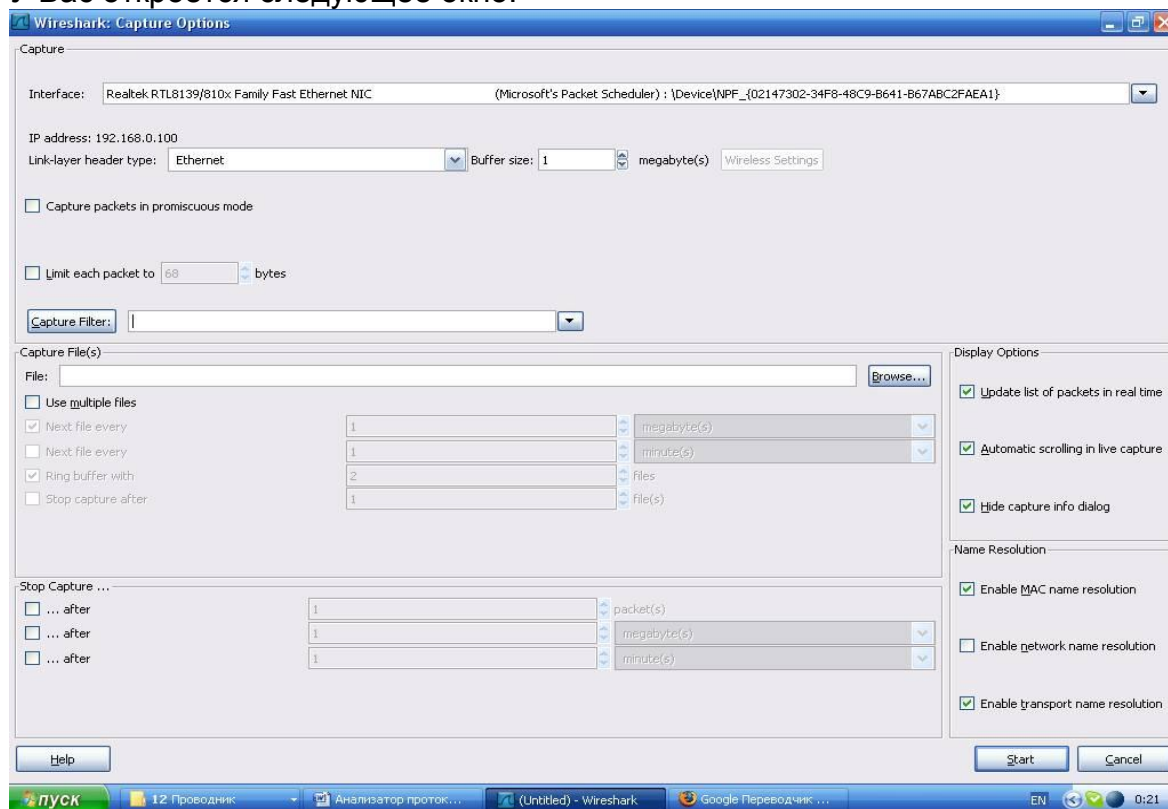



Рисунок 3 – Окно **Options** в меню **Capture** (фиксация, перехват)

Для того, чтобы следить за процессом перехвата всех пакетов (**без фильтрации**) – выберите режим **«Capture packets in promiscuous mode»** (Перехват всех пакетов без разбора) – для этого **уберите галочку** в соответствующем окне.

Чтобы начать перехват пакетов нажмите на значок  (**Start**) главной панели, либо кнопку **«Start»** в окне **Capture – Options**.

В появившемся списке сетевых интерфейсов выберите тот интерфейс, **для которого параметр «Packets» постоянно увеличивается** (это означает, что на данном интерфейсе **наблюдается активность**).

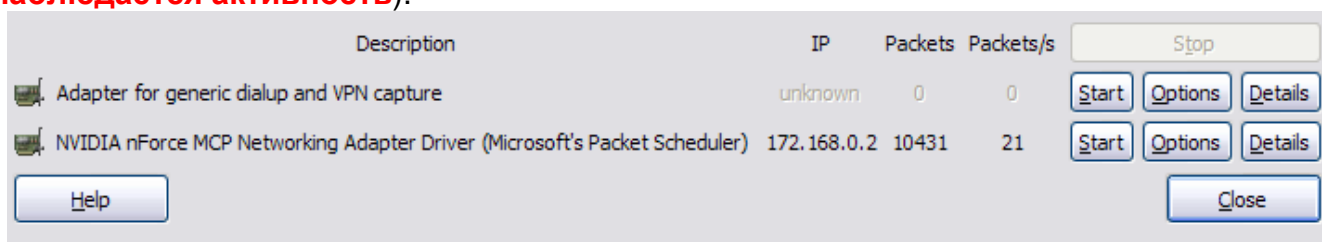



Рисунок 4 – Выбор активного сетевого интерфейса

Для начала перехвата нажмите кнопку **«Start»** **для активного сетевого интерфейса**.

Для остановки перехвата пакетов необходимо нажать на значок  (**Stop**) на панели управления.

3. Порядок выполнения работы

Для понимания работы с анализатором, в данной лабораторной работе мы будем исследовать простейшие коммуникационные процессы, которые Вы запустите на Вашем компьютере.

В качестве таких процессов исследуем процесс **Ping** («прозвонка» соединения с удаленным хостом).

Этот процесс наиболее часто используются для выявления проблем в транспортной сети. Процесс **Ping** использует для этих целей протокол ICMP.

Перехват и анализ сообщений протокола ICMP и будет целью данного пункта лабораторной работы.

Порядок выполнения ЛР - 4 следующий:

- 3.1. Запускаем процесс перехвата пакетов анализатором Wireshark
- 3.2. Запускаем исследуемый процесс Ping в командной строке интерфейса CLI и ожидаем окончания процесса Ping
- 3.3. Останавливаем процесс перехвата пакетов анализатором Wireshark
- 3.4. Копируем результаты выполнения команды Ping в отчет (файл в формате ЛР-4.doc)
- 3.5. Сохраняем результаты перехвата пакетов анализатором Wireshark в файле с именем ping.pcap
- 3.6. Производим небольшой анализ результатов перехвата пакетов
- 3.7. Оформляем отчет по данной работе и отправляем файл отчета ЛР-4.doc в адрес дистанционного деканата

3.1 Запускаем процесс перехвата пакетов анализатором Wireshark

3.1.1 В пункте меню **Capture** (фиксация, перехват) выберите **Options**.

3.1.2 Для того, чтобы следить за процессом перехвата всех пакетов (**без фильтрации**) – выберите режим **«Capture packets in promiscuous mode»** (Перехват всех пакетов без разбора) – для этого **уберите галочку** в соответствующем окне.



3.1.3 Чтобы начать перехват пакетов нажмите на значок **(Start)** главной панели, либо кнопку **«Start»** в окне **Capture – Options**.

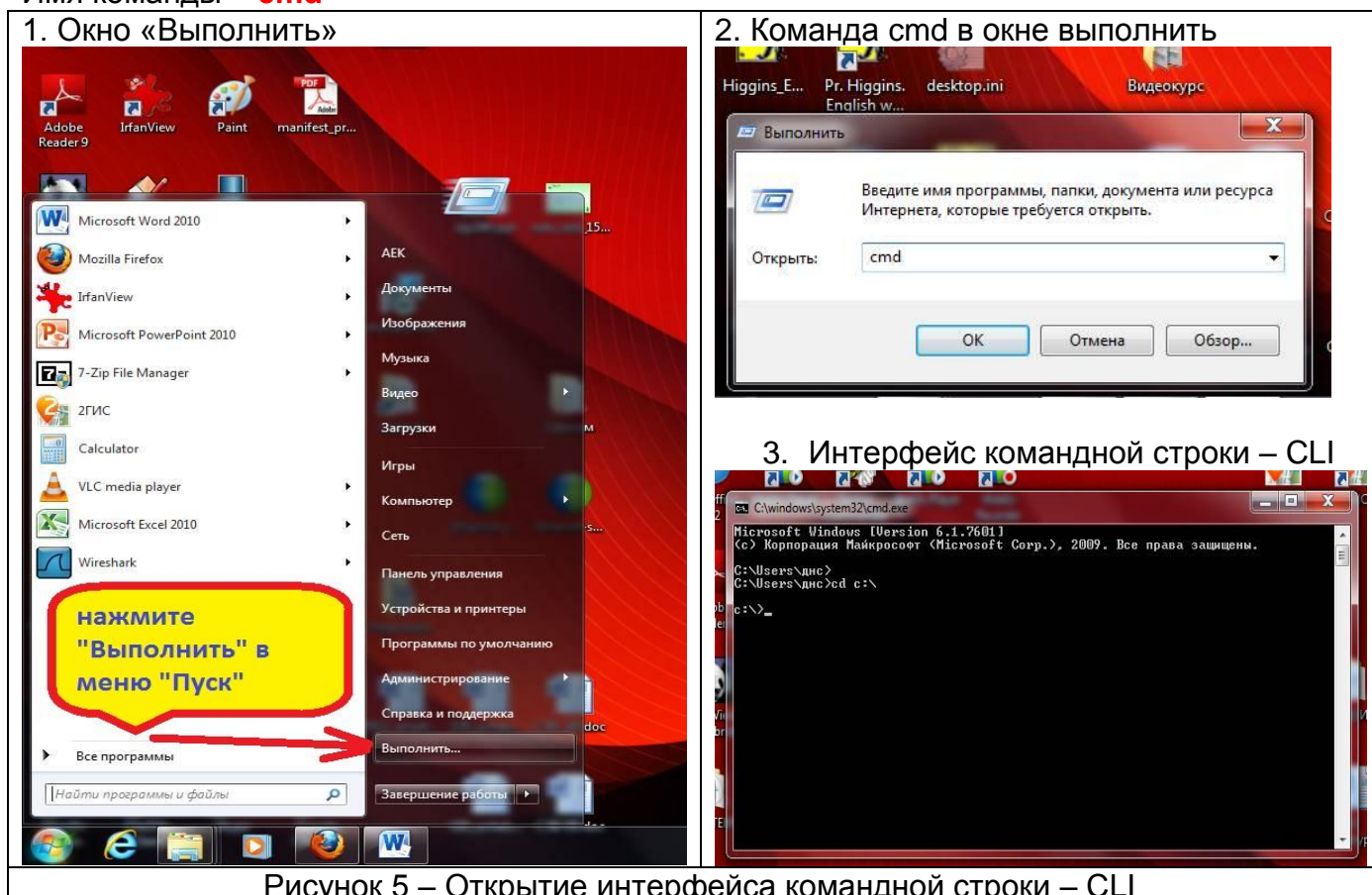
3.1.4 В появившемся списке сетевых интерфейсов выберите тот интерфейс, **для которого** параметр **«Packets»** постоянно увеличивается (это означает, что на данном интерфейсе **наблюдается активность**).

3.1.5 Для начала перехвата нажмите кнопку **«Start»** **для активного сетевого интерфейса**.

3.1.6 В рабочей области программы начнут сразу же появляться новые строчки. Каждая строчка – это сетевой пакет. Нажав на интересующую строчку, в нижнем окне появится расшифровка полей пакета в виде иерархического списка.

3.2 Запускаем процесс Ping в командной строке интерфейса CLI

Для запуска процесса Ping откройте на Вашем компьютере окно «Выполнить» в меню «Пуск» и наберите в этом окне имя команды перехода в режим командной строки (CLI). Имя команды – **cmd**



Таким образом, для запуска исследуемых коммуникационных процессов Вам необходимо открыть окно интерфейса командной строки – CLI, для чего надо последовательно выполнить пункты 1, 2 и 3 как показано на рис. 5

ВНИМАНИЕ!

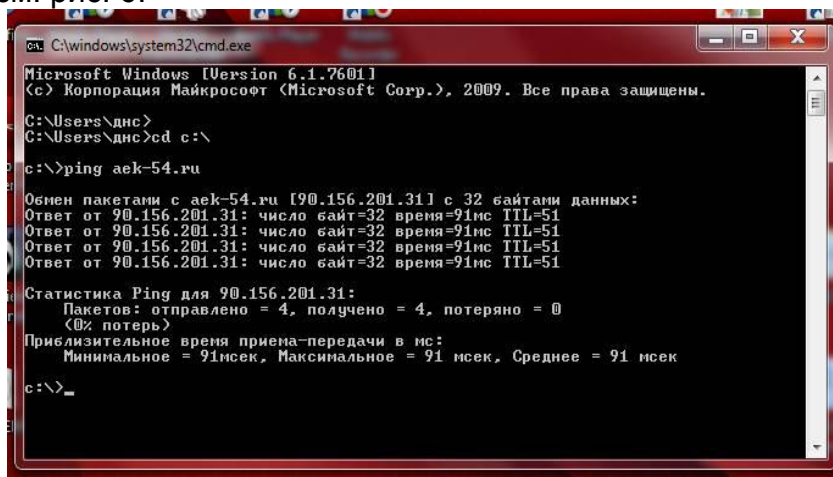
В Windows-7, команда «Выполнить» по умолчанию убрана из меню «Пуск».

Чтобы вернуть эту команду в меню «Пуск», вы можете воспользоваться инструкциями на сайте - <http://feyhoa.org.ua/archives/1064> .

Теперь надо запустить **коммуникационный процесс** Ping в окне интерфейса CLI.

Прозвонка сетевого соединения выполняется по конкретному IP-адресу, либо по доменному имени.

В данной работе для выполнения прозвонки будем использовать доменное имя сайта aek-54.ru, для чего вводим в окне интерфейса CLI команду: ping aek-54.ru и нажимаем клавишу Enter – см. рис. 6.



```
C:\windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\dnc>
C:\Users\dnc>cd c:\
c:\>ping aek-54.ru

Обмен пакетами с aek-54.ru [90.156.201.31] с 32 байтами данных:
Ответ от 90.156.201.31: число байт=32 время=91мс TTL=51
Ответ от 90.156.201.31: число байт=32 время=91мс TTL=51
Ответ от 90.156.201.31: число байт=32 время=91мс TTL=51
Ответ от 90.156.201.31: число байт=32 время=91мс TTL=51

Статистика Ping для 90.156.201.31:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    <0% потерь>
    Приблизительное время приема-передачи в мс:
    Минимальное = 91мсек, Максимальное = 91 мсек, Среднее = 91 мсек


c:\>_
```

Рисунок 6 – Ввод команды **ping aek-54.ru** и отображение результата прозвонки

В ответ на ввод команды прозвонки появляется отклик системы, отображающий результат посылки 4-х пакетов ICMP в адрес сайта aek-54.ru.

В данном случае прозвонка соединения прошла успешно, т.е. указанный сайт доступен с Вашего компьютера.

3.3 Останавливаем процесс перехвата пакетов анализатором Wireshark

Для остановки перехвата пакетов необходимо нажать на значок  (Stop) на панели управления.

3.4 Копируем результатов выполнения команды Ping в отчет

Для копирования результатов выполнения команды Ping в отчет можно использовать любой из двух способов:

1. Копирование через буфер обмена

- 3.4.1 Выделить в окне интерфейса CLI результаты выполнения команды Ping, для чего надо в данном окне нажать правую кнопку мыши и выбрать пункт «Выделить все»
- 3.4.2 Нажав клавишу Enter, скопировать содержимое окна CLI в буфер обмена
- 3.4.3 Открыть в редакторе MS'Word файл отчета, присвоив ему имя ЛР-4.doc
- 3.4.4 Скопировать содержимое буфера обмена в файл отчета, нажав «Ctrl+V»

После этих операций мы получим следующий результат:

```
c:\>ping aek-54.ru
Обмен пакетами с aek-54.ru [90.156.201.31] с 32 байтами данных:
Ответ от 90.156.201.31: число байт=32 время=91мс TTL=51
Ответ от 90.156.201.31: число байт=32 время=91мс TTL=51
Ответ от 90.156.201.31: число байт=32 время=91мс TTL=51
Ответ от 90.156.201.31: число байт=32 время=91мс TTL=51
```

Статистика Ping для 90.156.201.31:

Пакетов: отправлено = 4, получено = 4, потеряно = 0
(0% потерь)

Приблизительное время приема-передачи в мс:

Минимальное = 91мсек, Максимальное = 91 мсек, Среднее = 91 мсек

c:\>

2. Второй способ копирования – через функцию Print Screen – скопировать экранную форму с окном CLI и вставить ее в файл отчета, как показано на рис. 6.

3.5 Сохраняем результаты перехвата пакетов анализатором Wireshark в файле с именем ping.pcap

Для сохранения результатов перехвата пакетов выберите в пункте меню **File** главной панели пункт **Save as:**

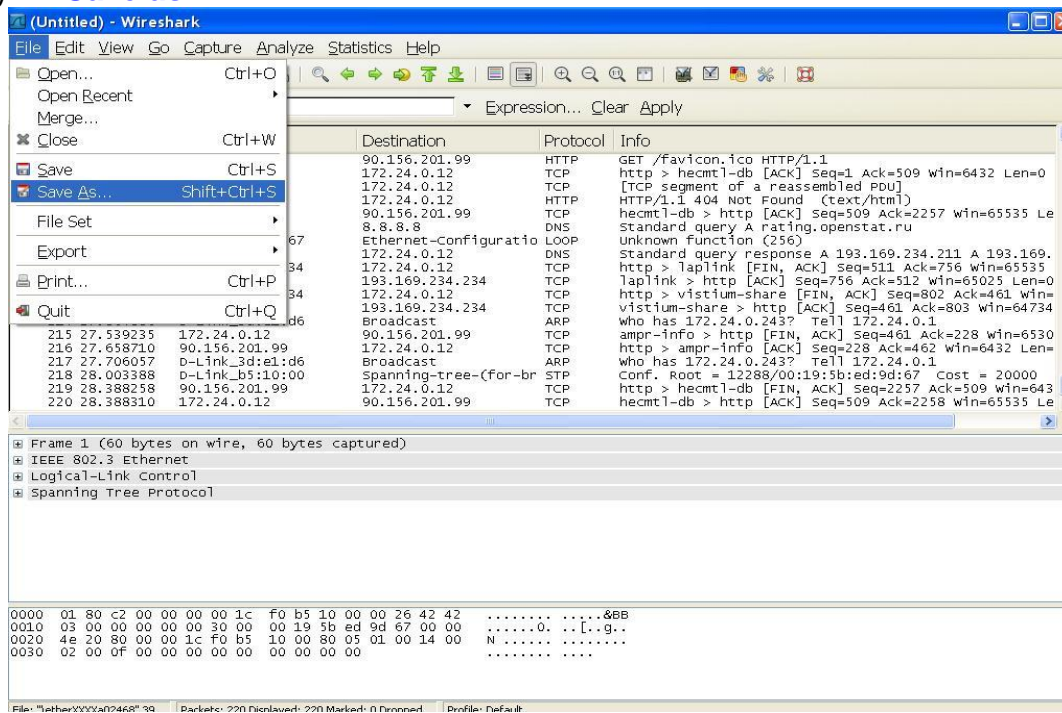


Рисунок 7 – сохранение результатов перехвата пакетов

Присвойте сохраняемому файлу имя и выберите расширение сохраняемого файла – **ping-aek.pcap**, (вариант Wireshark/tcpdump..., который обычно предлагается по умолчанию).

Сохраненный файл с перехваченными Вами пакетами необходимо выслать как приложение к отчету по данной лабораторной работе.

Внимание:

Для правильного выполнения лабораторной работы необходимо соблюдать **следующие условия:**

1. Запускать приложение Wireshark (кнопка “START”) надо до запуска исследуемого процесса, а завершать приложение Wireshark (кнопка “STOP”) надо после остановки Вами исследуемого процесса. В этом случае в сохраняемом файле будут пакеты, соответствующие всему сеансу исследуемого процесса.
2. Следить, чтобы длительность работы Wireshark по перехвату пакетов не превышала 1 минуты. Для усвоения основных навыков работы этого достаточно! Превышение работы Wireshark приведет к тому, что размеры файла с перехваченными пакетами будут настолько большими, что это не позволит Вам не только передать Ваш файл в качестве приложения к отчету, но и забьет Ваш диск до полной остановки ОС. Например, для скорости Вашего интерфейса – 100 Мбит/с в каждую секунду будут перехватываться пакеты с общим объемом до 12 Мбайт, следовательно, за час работы Wireshark (3600 с) на Ваш диск набьется пакетов до 43-х Гбайт!!!

3.6 Анализ результатов перехвата пакетов

По умолчанию анализатор перехватывает все пакеты, от служб, которые работают на Вашем компьютере, поэтому вначале анализа, необходимо научиться работать с фильтрами, выбирая интересующие Вас протоколы.

В данном случае нас интересует протокол **ICMP**, используемый процессом Ping.

Чтобы отфильтровать пакеты протокола ICMP, введите в окне **Filter** маску **ICMP** и нажмите «Enter». Когда маска введена правильно, поле ввода подсвечивается **зеленым** цветом, в противном случае – **красным**.

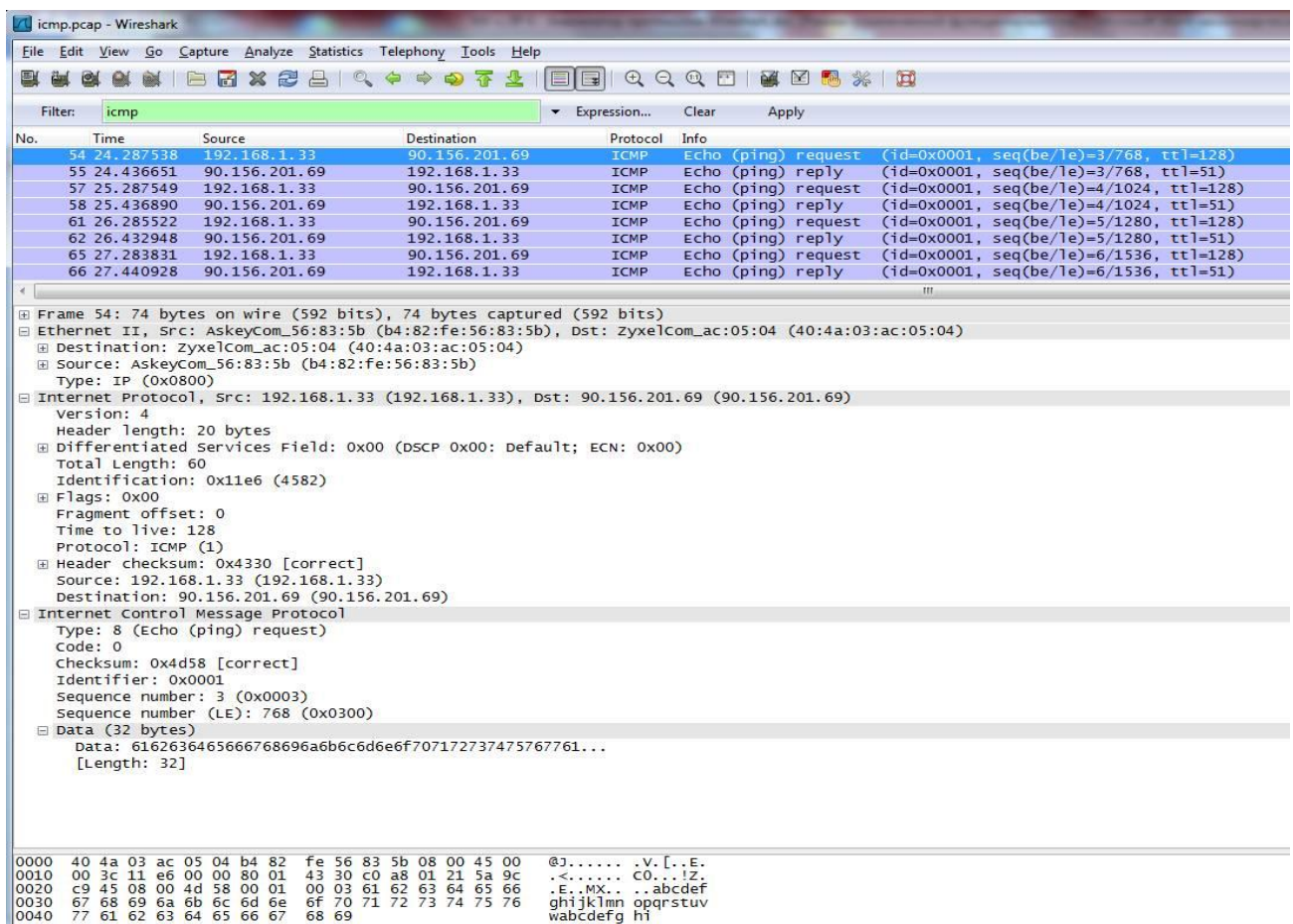


Рисунок 8 – Фильтрация пакетов ICMP из общего потока перехваченных пакетов

The screenshot shows the Wireshark interface with a filter set to 'icmp'. The packet list pane displays several ICMP Echo (ping) requests and replies. The packet details pane for packet 55 is expanded, showing the following structure:

- Ethernet II**: Src: ZyxelCom_ac:05:04 (40:4a:03:ac:05:04), Dst: AskeyCom_56:83:5b (b4:82:fe:56:83:5b)
- Internet Protocol**: Src: 90.156.201.69 (90.156.201.69), Dst: 192.168.1.33 (192.168.1.33)
- Internet Control Message Protocol**: Type: 0 (Echo (ping) reply), Code: 0, Checksum: 0x5558 [correct], Identifier: 0x0001, Sequence number: 3 (0x0003), Sequence number (LE): 768 (0x0300)
- Data**: 32 bytes

Red annotations in the image include:

- A red arrow pointing to the ICMP layer in the details pane, labeled "Ответный пакет ICMP".
- A red arrow pointing to the "Type: 0 (Echo (ping) reply)" field, labeled "Имя и тип пакета ICMP".
- A red arrow pointing to the "Data" field, labeled "Поле данных пакета ICMP".

Рисунок 9 – Расшифровка ответного пакета ICMP

Теперь приведем некоторые результаты анализа пакетов ICMP:

3.6.1 В окне рисунков 8 и 9 мы видим детальную информацию о заголовках транспортных протоколов Ethernet и IPv4. Вы можете использовать данную информацию также для понимания процессов расшифровки пакетов Ethernet-IP-UDP и др. в контрольной работе по данной дисциплине.

Приведем пример анализа заголовков протоколов **Ethernet-IP**.

Начнем с полей протокола Ethernet (см. рис.10).

Поле Destination содержит информацию о получателе сообщения, Source – об источнике. Поле Type идентифицирует протокол верхнего уровня, поместивший свои данные в Ethernet пакет.

В нашем случае – это протокол IPv4 (Type=0800'hex).

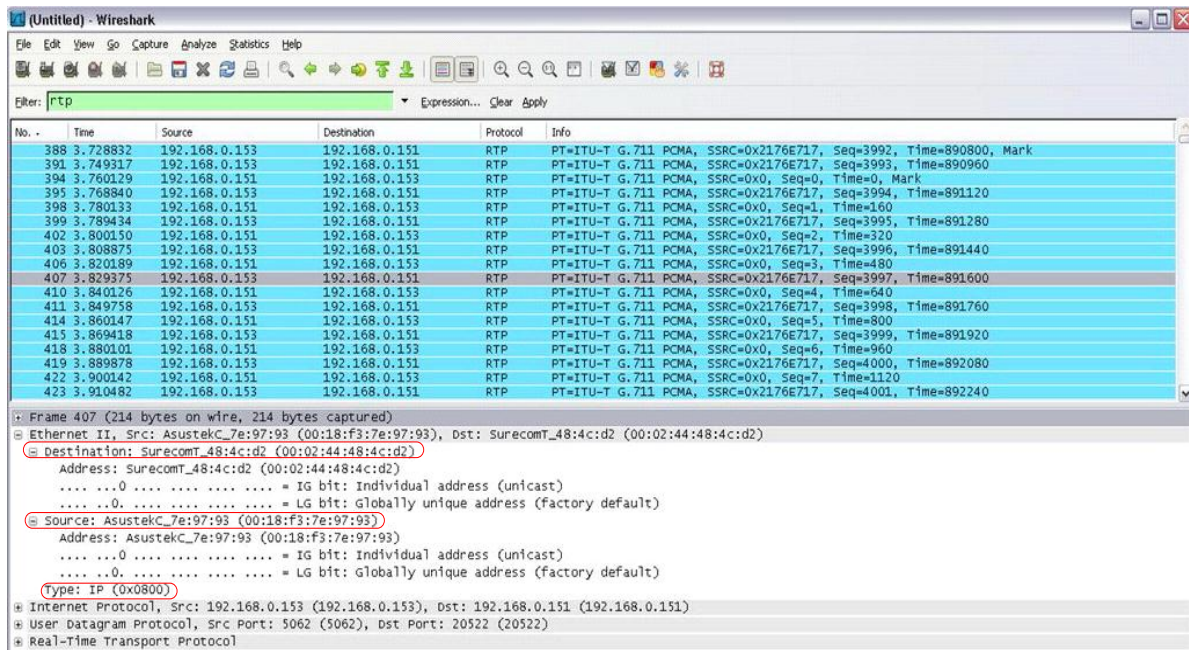


Рисунок 10 - Поля протокола Ethernet

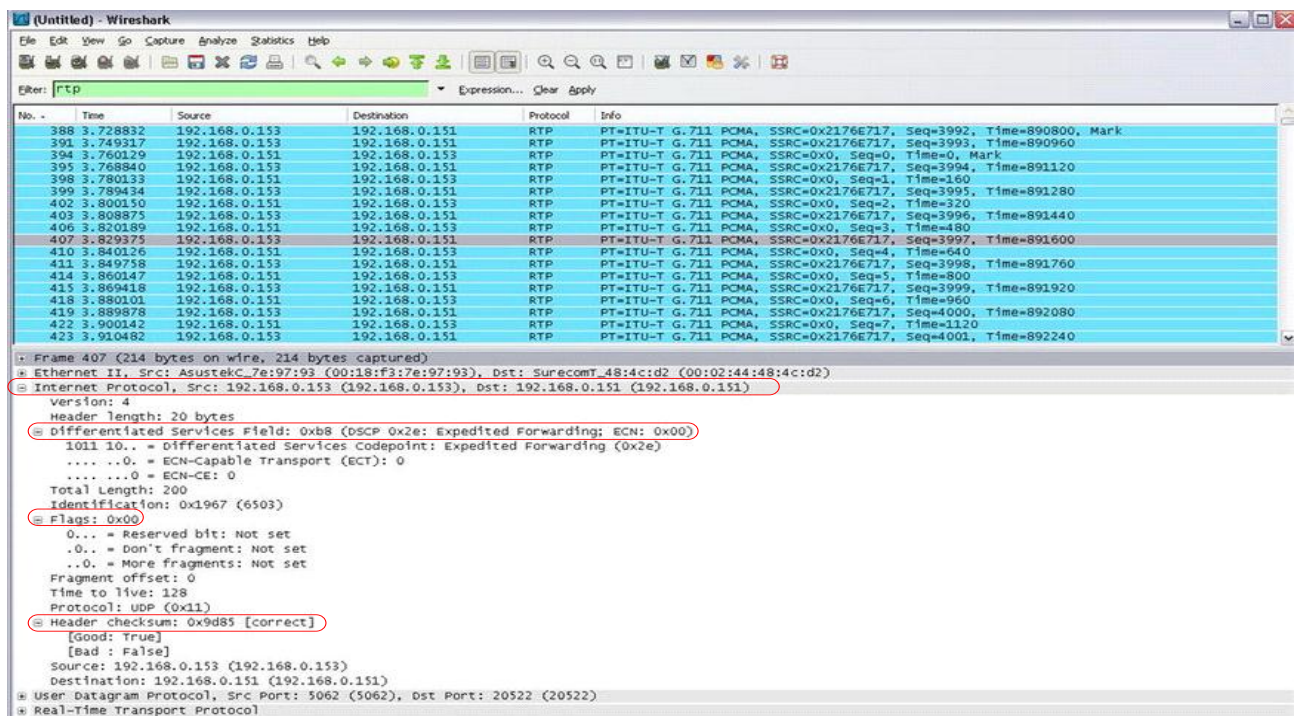


Рисунок 11 - Поля протокола IP

В полях протокола IP содержится информация об IP-адресе источника (Src) и получателя (Dst), версии протокола (в нашем случае – IPv.4) и длине заголовка (20 байт).

Далее следует информация о классе обслуживания DSCP, общая длина пакета (200) и его идентификатор.

Поле флагов, содержащее информацию о времени жизни пакета (128) и о протоколе верхнего уровня, поместившего свои данные в IP-пакет (UDP).

Затем следует контрольная сумма заголовка (Header checksum).

- 3.6.2 На рис.8 в нижней части рабочей области показана расшифровка первого пакета ICMP (Echo request - тип 8), отправленного с адреса 192.168.1.33 на адрес 90.156.201.69
- 3.6.3 На рис.9 в нижней части рабочей области показана расшифровка второго пакета ICMP (сообщение ответа Echo reply - тип 0), отправленного в ответ с адреса 90.156.201.69 на адрес 192.168.1.33
- 3.6.4 Оба сообщения имеют одинаковое поле данных, что подтверждает успешность результата прозвонки – что послали, то в ответ и получили
- 3.6.5 Через пункт меню – **Statistics – IO-Graphs** мы можем видеть скорость передачи пакетов ICMP в бит/с – см. рис.12

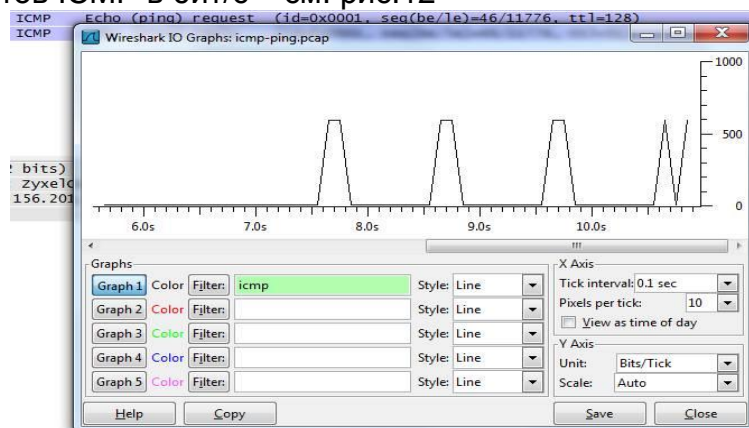


Рисунок 12 – скорость передачи пакетов ICMP

Для получения удобного отображения – настройте правильно параметры разрешения – Tick interval и Pixels per tick, а также единицы отображения пакетов (Unit) – Bits/Tick.

Например, выбрав другой временной масштаб (параметр Tick interval=0,01sec) Вы можете различать во времени каждый из переданных и принятых пакетов ICMP.

- 3.6.6 Анализатор протоколов позволяет более наглядно рассмотреть схему передачи информации. Для этого через пункт меню – **Statistics – Flow-Graph** мы можем видеть порядок обмена пакетами ICMP между хостами с адресами 192.168.1.33 и 90.156.201.69:

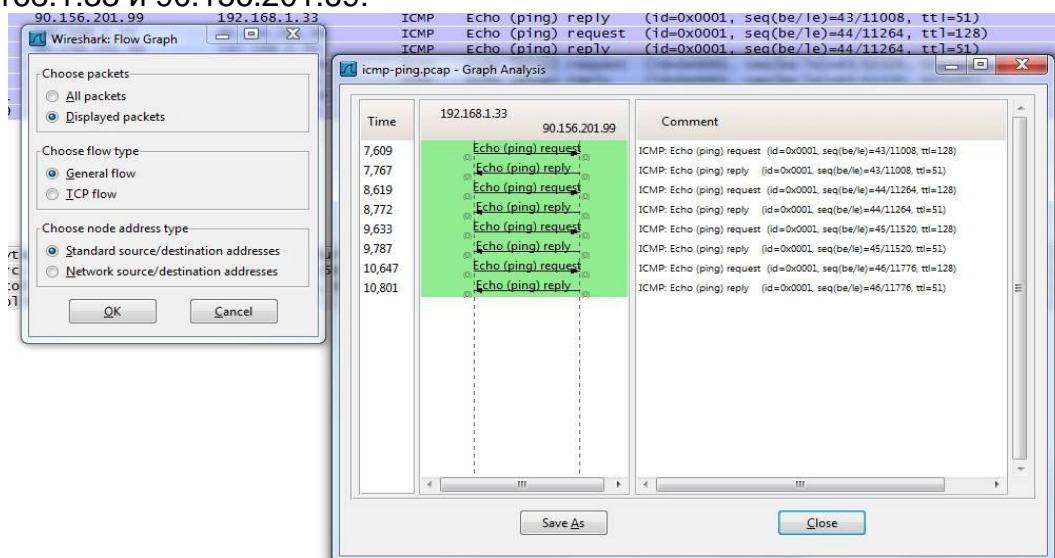


Рисунок 13 – Порядок обмена пакетами ICMP

Для выполнения данной работы этого достаточно, но Вы не останавливайтесь на этом и глубже изучите все возможности перехвата и анализа пакетов от разных протоколов.

4. Правила оформления отчета

Отчет по лабораторной работе должен содержать:

- 4.1 Титульный лист: ФИО, № группы, название лабораторной работы.
- 4.2 Цель работы.
- 4.3 Результаты перехвата и анализа пакетов ICMP – по всем пунктам раздела 3. Привести соответствующие экранные формы **но с Вашими результатами!**
- 4.4 Комментарии и выводы по **всем пунктам** лабораторной работы.

Сохранить отчет в файле с именем ЛР-4.doc и выслать его в адрес дистанционного деканата.

В качестве подтверждения выполнения данной работы, необходимо вместе с файлом отчета выслать в одном архиве также файл с перехваченными пакетами (с расширением *.pcap).

5 Контрольные вопросы

- 5.1 Назначение анализатора Wireshark
- 5.2 Назначение полей протокола Ethernet
- 5.3 Назначение полей заголовка протокола IP
- 5.4 Назначение протокола ICMP
- 5.5 Сообщения протокола ICMP
- 5.6 Процессы, использующие протокол ICMP

6 Литература, рекомендуемая для выполнения лабораторной работы

- 6.1 Конспект лекций по дисциплине ИС СПС
- 6.2 Сайт разработчика Wireshark - <http://www.wireshark.org/download.html>
- 6.3 Документация по инсталляции Wireshark и требования к программно-аппаратным средствам - http://www.wireshark.org/docs/wsug_html_chunked/ChIntroPlatforms.html
- 6.4 Руководство пользователя Wireshark (онлайн-версия) - http://www.wireshark.org/docs/wsug_html_chunked/