ЛАБОРАТОРНАЯ РАБОТА № 15

**Использование Wireshark для анализа Protocol Data Units**

**Цель работы.** Провести анализ Protocol Data Units с использованием Wireshark.

**КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ**

**ICMP - протокол**

Протокол управления сообщениями Интернета (ICMP – Internet Control Message Protocol) - спутник протокола IP. ICMP — протокол сетевого уровня. Однако он сам не передает сообщения непосредственно данных канальному уровню. Эти сообщения первыми инкапсулируются в дейтаграммы IP перед переходом к более низкому уровню [(рисунок1).](http://www.intuit.ru/department/network/internetprot/6/internetprot_6.html#image.6.1)

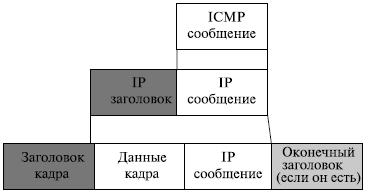


Рисунок 1 **–** Инкапсуляция сообщения ICMP

Значение поля протокола в дейтаграмме IP — это "1", оно указывает, что данные IP — это ICMP-сообщение.

### Типы сообщений ICMP

ICMP-сообщения разделены на две широкие категории: отчет об ошибке сообщения и запрос, как это показано на [рисунке 2.](http://www.intuit.ru/department/network/internetprot/6/internetprot_6.html#image.6.2)

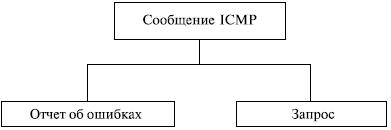


Рисунок 2 **–** Сообщения ICMP

Сообщение об ошибке переносит данные о проблемах, возникающих при обмене сообщениями, с которыми маршрутизатор или хост (пункт назначения) могут столкнуться, когда они обрабатывают пакет IP.

Сообщения запроса помогают хосту или сетевому менеджеру получить заданную информацию от маршрутизатора или другого хоста. Например, узлы могут обнаружить их соседей. Также хосты могут обнаружить и узнать о маршрутизаторах на их сети, и маршрутизаторы могут помочь узлу переадресовывать его сообщения. [Таблица 1.](http://www.intuit.ru/department/network/internetprot/6/internetprot_6.html#table.6.1) перечисляет ICMP-сообщения в каждой категории.

|  |  |  |
| --- | --- | --- |
| Таблица 1 – ICMP сообщения | | |
| **Категория** | **Тип** | **Сообщение** |
|  | 3 | Конечный пункт не достижим |
| 4 | подавление источника |
| 11 | Время истекло |
| 12 | Проблемы параметров |
| 5 | Переназначение |
| 8 или 0 | Эхо запрос и ответ |
| 13 или 14 | Метка времени запрос и ответ |
| 17 или 18 | Маска адреса запрос и ответ |
| 10 или 9 | Маршрутизатор затребование и извещение |

### 

### Формат сообщения ICMP

ICMP-сообщение имеет 8-байтовый заголовок и раздел данных переменного размера. Хотя общий формат заголовка различен для каждого типа сообщения, первые 4 байта — общие для всех. Как показывает рисунок 3, первое поле, ICMP, определяет тип сообщения. Поле кода определяет основание для конкретного типа сообщения. Последнее общее поле – это поле контрольной суммы. Остальная часть заголовка задана для каждого типа сообщения.



Рисунок 3 **–** Основной формат ICMP

Раздел данных в сообщениях об ошибках доставляет информацию для нахождения первоначального пакета, который содержит ошибку. В сообщениях запроса раздел данных доставляет дополнительную информацию, основанную на типе запроса.

### 

### Сообщения ошибки ICMP

Одна из главных обязанностей ICMP состоит в том, чтобы известить об ошибках. Хотя технологии передачи сегодня предоставляют для передачи все более и более достоверные среды, ошибки все еще существуют и должны быть обработаны. IP, как обсуждалось ранее, является ненадежным протоколом. ICMP был частично предназначен для компенсирования этого недостатка. Однако ICMP не исправляет ошибки, он просто извещает о них. Исправление ошибки оставляют протоколам высокого уровня. Сообщения об ошибках всегда посылают первоначальному источнику, потому что единственная информация, доступная в дейтаграмме о маршруте — адреса IP пункта назначения и источник. ICMP использует исходный адрес IP, чтобы послать сообщение об ошибках источнику дейтаграммы. Обрабатываются пять типов ошибок [(рисунок 4):](http://www.intuit.ru/department/network/internetprot/6/internetprot_6.html#image.6.4)

* пункт назначения недостижим;
* подавление источника;
* время истекло;
* проблемы параметра;
* переназначение.



Рисунок 4 **–** Типы сообщений отчета об ошибках

Все сообщения об ошибках содержат раздел данных [(рисунок 5)](http://www.intuit.ru/department/network/internetprot/6/internetprot_6.html#image.6.5), который включает заголовок IP первоначальной дейтаграммы плюс первые 8 байт данных в этой дейтаграмме. Первоначальный заголовок дейтаграммы добавляется, чтобы дать первоначальному источнику, который получает сообщение об ошибках, информацию непосредственно о самой дейтаграмме. Включены 8 байт данных, потому что, согласно форматам UDP- и TCP-протоколов, первые 8 байт обеспечивают информацию о номерах порта (UDP и TCP) и порядковом номере (TCP). Эта информация необходима, чтобы источник мог сообщить протоколам (TCP или UDP) об ошибке. ICMP формирует пакет данных об ошибке, который затем инкапсулируется в дейтаграмму IP (см. [(рисунок 5).](http://www.intuit.ru/department/network/internetprot/6/internetprot_6.html#image.6.5)

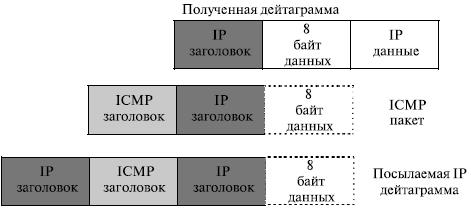


Рисунок 5 **–** Содержание поля данных для сообщения об ошибках

**FTP - протокол**

FTP представляет самый простой способ обмена файлами между удаленными компьютерами и используется для загрузки или отгрузки файлов на другой компьютер. Это стандартный протокол интернета, оптимизированный для передачи данных через сети TCP/IP. Для надежной передачи данных FTP устанавливает соединение клиент/сервер с использованием двух портов TCP на компьютере-клиенте и сервере. Первый порт называется FTР Control и обеспечивает начало сеанса и контроль ошибок; второй порт называется FTP Data и обеспечивает непосредственную передачу данных между клиентом и сервером. Служба FTP использует хорошо известный порт 21 для операций контроля и порт 20 для передачи данных. Клиентские порты TCP присваиваются динамически при создании сеанса.

"Хорошо известные" номера портов зарезервированы организацией ICANN (Internet Corporation for Assigned Names and Numbers) для использования конечными точками приложения, которые устанавливают связь через протоколы TCP или UDP. Каждый тип приложения имеет свой собственный и, следовательно, "хорошо известный" номер порта. Когда приложение на одном клиенте устанавливает соединение с другим клиентом, оно указывает на конкретное приложение посредством номера порта. Известные порты лежат в диапазоне от 0 до 1023, зарегистрированные порты – с 1024 по 49 151, а оставшиеся порты, вплоть до 65 535, используются в качестве динамических или частных портов. Вы можете сменить номер порта, используемый любой службой IIS, включая SMTP и NNTP. Это делается из соображений безопасности в небольшой частной сети; однако большинство хакеров используют сканеры портов для нахождения открытых портов.

Служба FTP позволяет пользователям загружать с сайта файлы, например, руководства по использованию товаров, сотрудникам отдела продаж работать с заказами или отчетами, находясь в отъезде или в пути. Однако за эти возможности можно заплатить немалую цену. Протокол FTP осуществляет передачу всех данных, включая имена пользователей и пароли, через сеть в открытом виде, что открывает доступ к локальной файловой системе любому пользователю в сети, если не обеспечена должная защита (право на локальный вход требуется каждому пользователю, подключающемуся к FTP-серверу).

Протокол не [шифруется](http://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5), при [аутентификации](http://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) передаются [логин](http://ru.wikipedia.org/w/index.php?title=%D0%9B%D0%BE%D0%B3%D0%B8%D0%BD_%28%D1%83%D1%87%D0%B5%D1%82%D0%BD%D0%B0%D1%8F_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D1%8C%29&action=edit&redlink=1) и [пароль](http://ru.wikipedia.org/wiki/%D0%9F%D0%B0%D1%80%D0%BE%D0%BB%D1%8C) открытым текстом. В случае построения сети с использованием [хаба](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BA%D0%BE%D0%BD%D1%86%D0%B5%D0%BD%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80) злоумышленник при помощи пассивного [сниффера](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7%D0%B0%D1%82%D0%BE%D1%80_%D1%82%D1%80%D0%B0%D1%84%D0%B8%D0%BA%D0%B0) может перехватывать логины и пароли находящихся в том же [сегменте сети](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D0%B3%D0%BC%D0%B5%D0%BD%D1%82_%D1%81%D0%B5%D1%82%D0%B8) пользователей FTP, или, при наличии специального ПО, получать передаваемые по FTP файлы без авторизации. При построении сети на [свитчах](http://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D0%BA%D0%BE%D0%BC%D0%BC%D1%83%D1%82%D0%B0%D1%82%D0%BE%D1%80) задача злоумышленника усложняется, но взлом всё равно возможен ([MAC-спуфинг](http://ru.wikipedia.org/wiki/MAC-%D1%81%D0%BF%D1%83%D1%84%D0%B8%D0%BD%D0%B3" \o "MAC-спуфинг), переполнение таблицы адресов). Чтобы предотвратить перехват трафика, необходимо использовать протокол шифрования данных [SSL](http://ru.wikipedia.org/wiki/SSL), который поддерживается многими современными FTP-серверами и некоторыми FTP-клиентами.

Процесс нешифрованной авторизации проходит в несколько этапов (символы \r\n означают перевод строки):

Установка TCP-соединения с сервером (обычно на 21 порт)

Посылка команды USER *логин*\r\n

Посылка команды PASS *пароль*\r\n

Если к серверу разрешён анонимный доступ (как правило, лишь для загрузки данных с сервера), то в качестве логина используется ключевое слово «anonymous» или «ftp», а в качестве пароля — адрес [электронной почты](http://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0):

USER anonymous\r\n

PASS someone@email\r\n

После успешной авторизации можно посылать на сервер другие команды.

**Основные команды FTP**

* ABOR — Прервать передачу файла
* CDUP — Сменить директорию на вышестоящую.
* CWD — Сменить директорию.
* DELE — Удалить файл (DELE filename).
* EPSV - Войти в расширенный пассивный режим. Применяется вместо PASV.
* HELP — Выводит список команд принимаемых сервером.
* LIST — Возвращает список файлов директории. Список передается через соединение данных (20 порт).
* MDTM — Возвращает время модификации файла.
* MKD — Создать директорию.
* MLST — Возвращает список файлов директории в более кратком формате чем LIST. Список передается через соединение данных (20 порт).
* NOOP — Пустая операция
* PASV — Войти в пассивный режим. Сервер вернет адрес и порт к которому нужно подключиться чтобы забрать данные. Передача начнется при введении следующих команд RETR, LIST и тд.
* PORT — Войти в активный режим. Например PORT 12,34,45,56,78,89. В отличие от пассивного режима для передачи данных сервер сам подключается к клиенту.
* PWD — Возвращает текущую директорию.
* QUIT — Отключиться
* REIN — Реинициализировать подключение
* RETR — Скачать файл. Перед RETR должна быть команда PASV или PORT.
* RMD — Удалить директорию
* RNFR и RNTO — Переименовать файл. RNFR — что переименовывать, RNTO — во что.
* SIZE — Возвращает размер файла
* STOR — Закачать файл. Перед STOR должна быть команда PASV или PORT.
* SYST — Возвращает тип системы(UNIX, WIN, …)
* TYPE — Установить тип передачи файла(Бинарный, текстовый)
* USER — Имя пользователя для входа на сервер

**ВЫПОЛНЕНИЕ**

Выполнение команды ping 172.20.19.201 c локального компьютера, имеющего IP-адрес 172.20.8.207, приводит к обмену пакетами по протоколу ICMP.

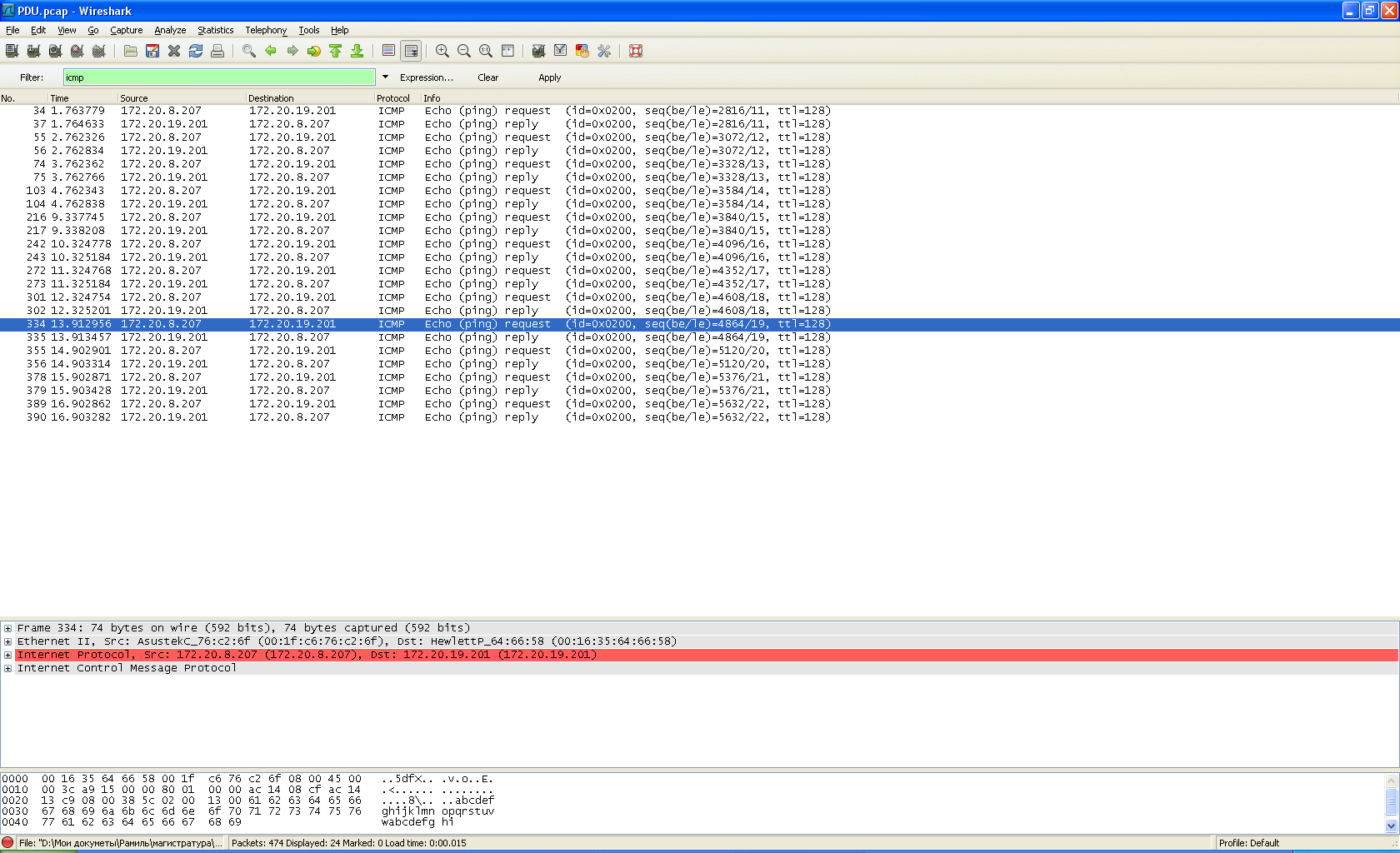


Рисунок 6 – Список переданных пакетов ICMP

На рисунке 7 приведен пример выполнения загрузки файлов с FTP-сервера с использованием команды get.



Рисунок 7 – Выполнение запросов к FTP-серверу через командную строку Windows

На рисунке 8 показан обмен пакетами при выполнении аутентификации пользователя

на FTP-сервере. Логин и пароль передаются в открытом виде, т.е. не имеют никакой

криптографической защиты.

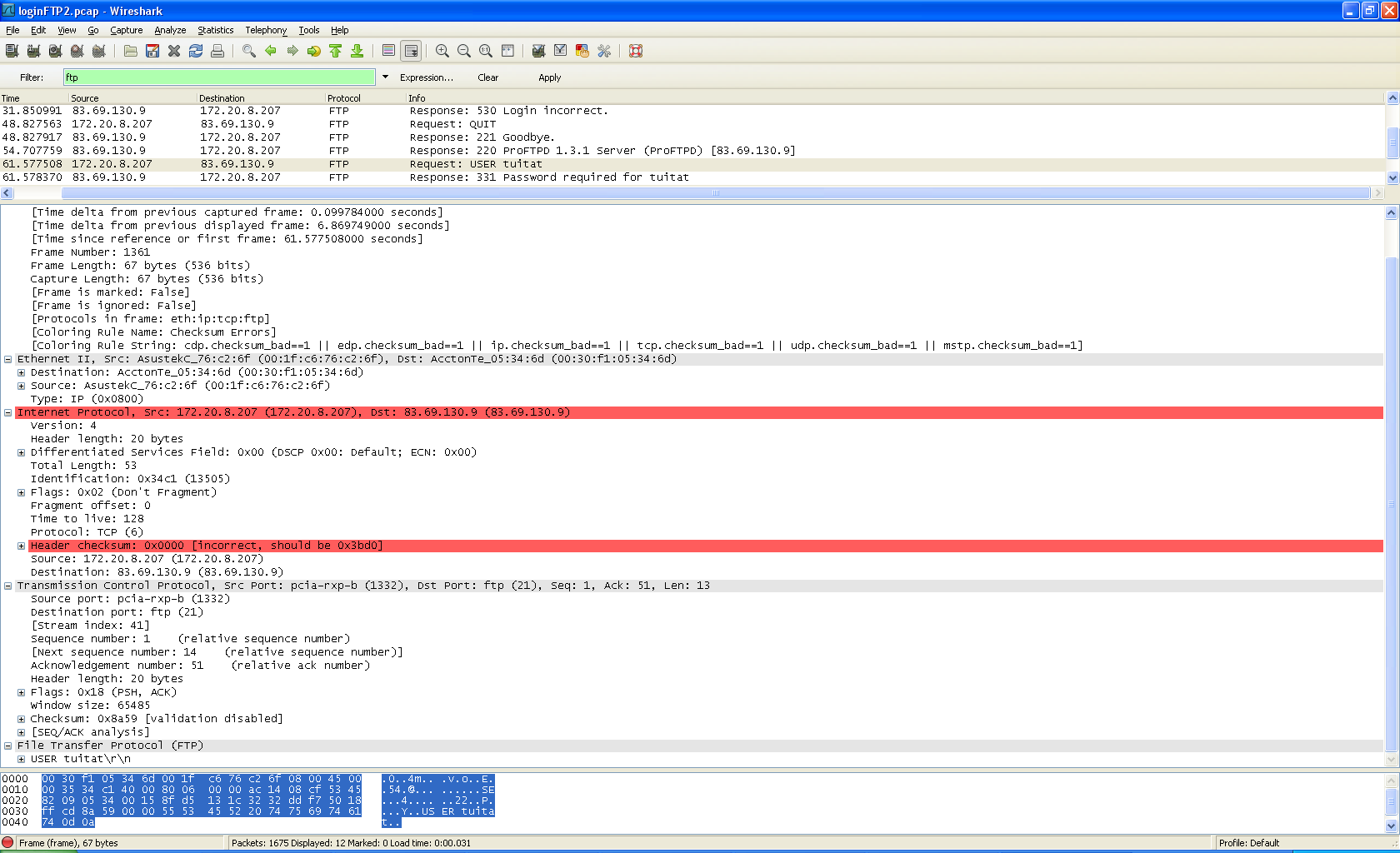


Рисунок 8 – Переданные FTP-пакеты при аутентификации

На рисунке 9 показана передача пакетов при выполнении команды get выполнение загрузки файла atmaruza.doc с FTP-сервера.

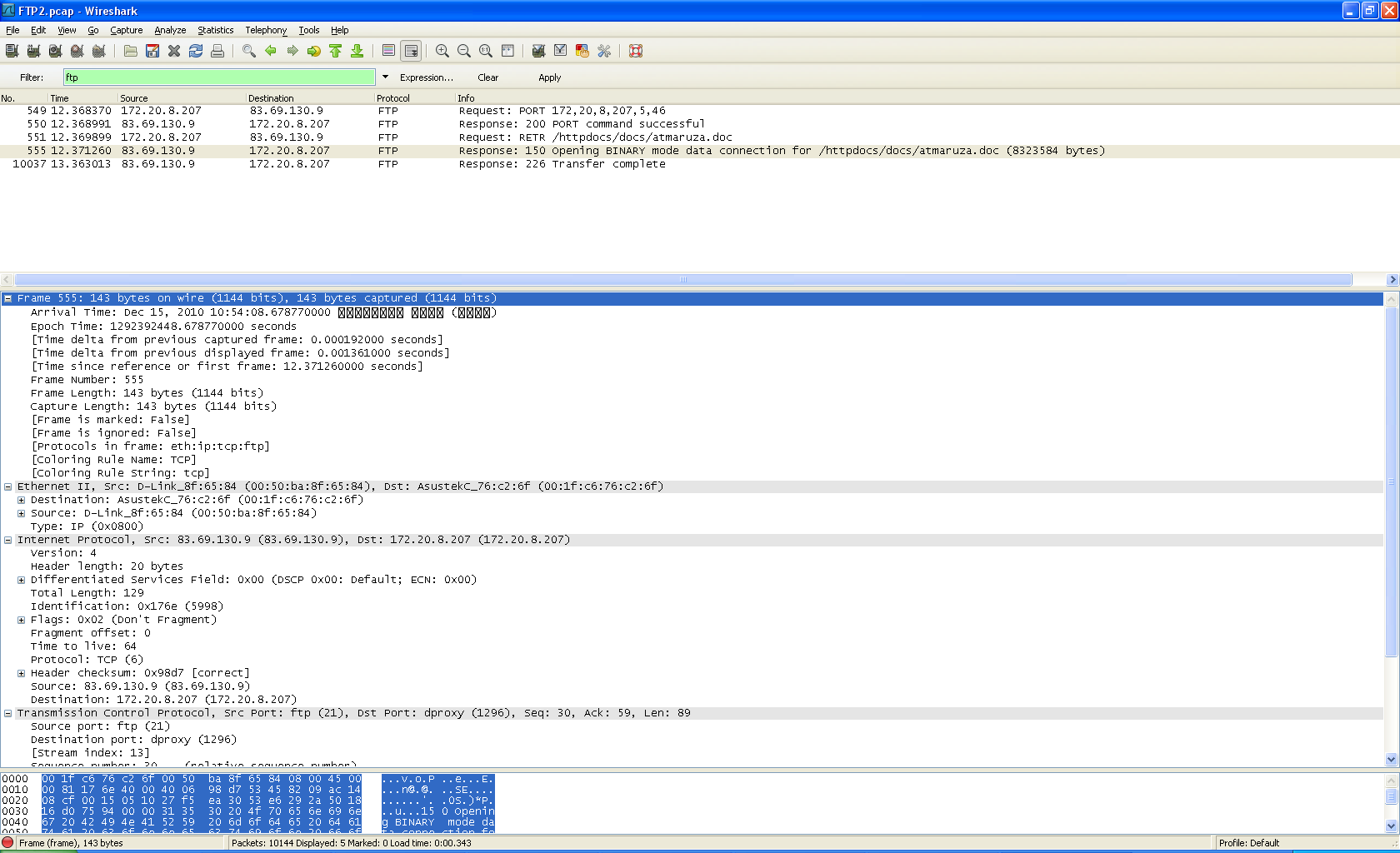


Рисунок 9 – Передаваемые пакеты при выполнении команды get

На рисунке 10. показан обмен пакетами информации FTP-DATA, загружаемой с FTP-сервера.

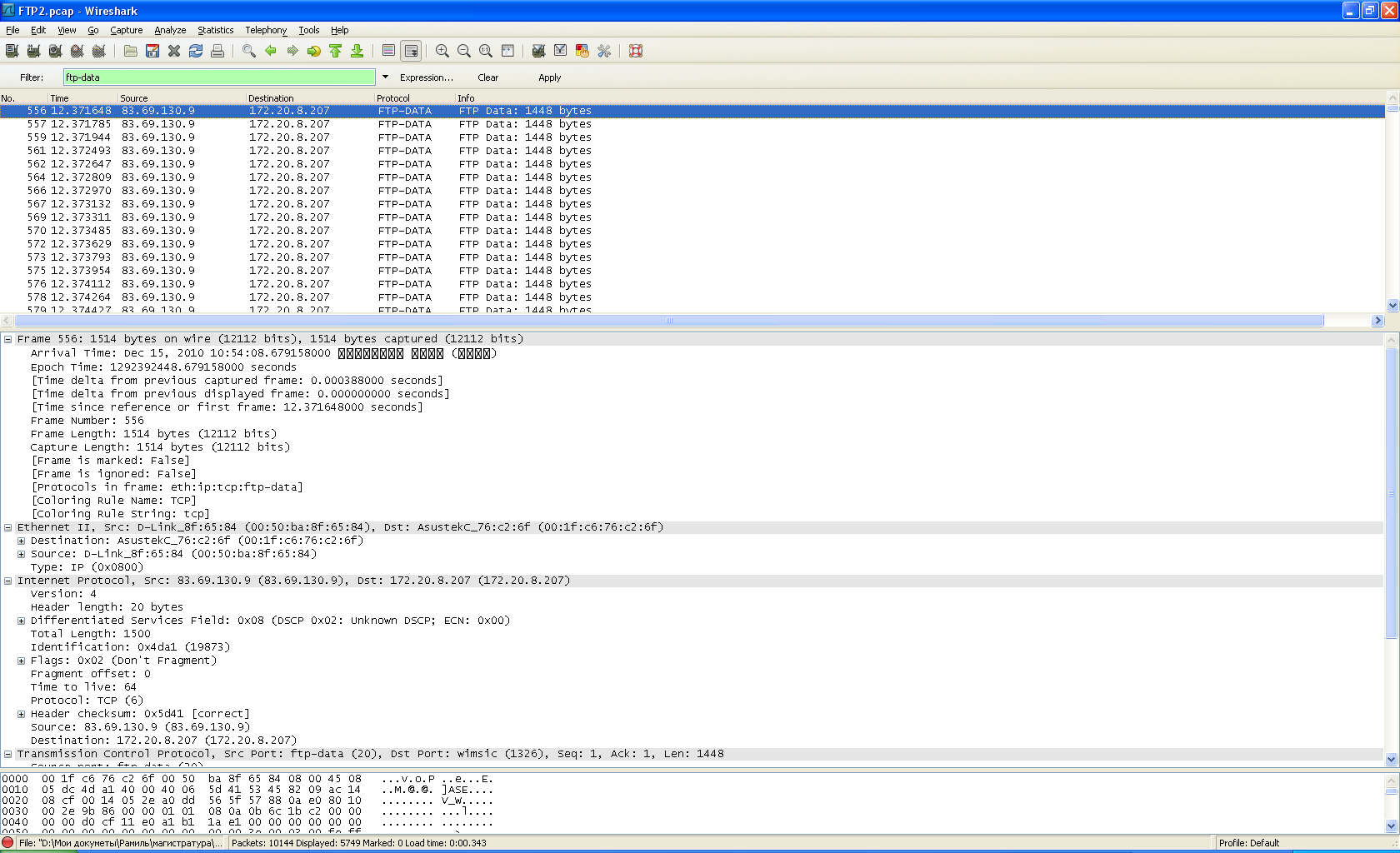


Рисунок 10 – Обмен пакетами FTP-DATA

**Содержание отчета**

1. Краткие теоретические сведения.
2. Информация об обмене ping сообщениями между компьютерами в локальной сети.
3. Информация об аутентификации и скачивание данных с FTP-сервера.
4. Анализ полученных результатов.

**Контрольные вопросы**

1. Опишите процесс обмена пакетов FTP-DATA.
2. Функции команды get.
3. Назначение FTP-пакетов.
4. Назначение пакетов ICMP.