

САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО

КАФЕДРА КОМПЬЮТЕРНЫХ СИСТЕМ И ПРОГРАММНЫХ ТЕХНОЛОГИЙ

**Отчёт по лабораторной работе №2**

**Курс: «Защита информации»**

**Тема: «Исследование сетевого трафика протокола FTP»**

Выполнил студент:

Бояркин Никита Сергеевич

Группа: 43501/3

Проверил:

Новопашенный Андрей Гелиевич

Санкт-Петербург  
2017 г.

# Содержание

<b>1</b>	<b>Лабораторная работа №2</b>	<b>2</b>
1.1	Цель работы . . . . .	2
1.2	Программа работы . . . . .	2
1.3	Конфигурация сети . . . . .	2
1.4	Ход работы . . . . .	2
1.4.1	Протокол FTP . . . . .	2
1.4.2	Установление управляющего соединения . . . . .	3
1.4.3	Аутентификация . . . . .	3
1.4.4	Активный режим FTP . . . . .	4
1.4.5	Пассивный режим FTP . . . . .	5
1.5	Вывод . . . . .	6
1.6	Приложение 1. Активный режим FTP . . . . .	7
1.6.1	Передача данных . . . . .	7
1.7	Приложение 2. Пассивный режим FTP . . . . .	8
1.7.1	Передача данных . . . . .	8

# Лабораторная работа №2

## 1.1 Цель работы

Получение навыков по исследованию сетевого трафика.

## 1.2 Программа работы

При помощи программы Wireshark продемонстрировать сетевой трафик для:

- Протокола FTP
  - В пассивном режиме
  - В активном режиме
  - Установление соединения и авторизация

## 1.3 Конфигурация сети

```
Адаптер Ethernet Ethernet:
DNS-суффикс подключения . . . . . :
Описание. . . . . : Intel(R) Ethernet Connection (2) I218-V
Физический адрес. . . . . : 4C-CC-6A-25-CC-59
DHCP включен. . . . . : Да
Автонастройка включена. . . . . : Да
Локальный IPv6-адрес канала . . . : fe80::b5e4:68bb:4d4c:fad7%11(Основной)
IPv4-адрес. . . . . : 192.168.0.106(Основной)
Маска подсети . . . . . : 255.255.255.0
Аренда получена. . . . . : 11 марта 2017 г. 9:59:41
Срок аренды истекает. . . . . : 11 марта 2017 г. 22:59:42
Основной шлюз. . . . . : 192.168.0.1
DHCP-сервер. . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 38587498
DUID клиента DHCPv6 . . . . . : 00-01-00-01-1F-76-F1-20-4C-CC-6A-25-CC-59
DNS-серверы. . . . . : 192.168.0.1
NetBios через TCP/IP. . . . . : Включен
```

Рис. 1.1: Сетевые параметры компьютера

## 1.4 Ход работы

### 1.4.1 Протокол FTP

В отличие от большинства других протоколов, при работе с протоколом FTP создается два типа соединений, первое служит для аутентификации и передачи команд, второе — для передачи данных. По второму соединению определяется режим работы, он может быть активным, а может быть пассивным. Отличаются они между собой стороной выступающей инициатором подключения для передачи данных и портами, на которых эта передача собственно производится. При нормальном или активном FTP, управляющее соединение иницируется со стороны клиента, а подключение для передачи данных иницируется со стороны сервера. В пассивном режиме, как управляющее соединение так и соединение для передачи данных иницируется клиентом.

Для демонстрации работы протокола FTP был выбран сервер `ftp://ftp.funet.fi` (193.166.3.2).

## 1.4.2 Установление управляющего соединения

Первый этап - установление TCP соединения с 21 портом сервера (управляющее соединение):

Source	Destination	Protocol	Length	Info
192.168.0.106	193.166.3.2	TCP	66	52686 → 21 [SYN] Seq=1044297971 win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
193.166.3.2	192.168.0.106	TCP	66	21 → 52686 [SYN, ACK] Seq=929890115 Ack=1044297972 win=49640 Len=0 MSS=1460 WS=1 SACK_PERM=1
192.168.0.106	193.166.3.2	TCP	54	52686 → 21 [ACK] Seq=1044297972 Ack=929890116 win=8192 Len=0

Рис. 1.2: Установление TCP соединения с 21 портом сервера

Стандартная процедура проверки достижимости сервера. Применяется для всех протоколов, использующих TCP. Аналогичное установление соединения происходит с потоком данных после аутентификации и перехода в активный/пассивный режим.

## 1.4.3 Аутентификация

Следующий этап - аутентификация клиента с помощью имени пользователя и пароля. Имя пользователя отправляется на сервер командой USER, а пароль - командой PASS.

Хост, обеспечивающий FTP-сервис, может предоставить анонимный доступ к FTP. Пользователи обычно входят в систему как «anonymous» в качестве имени пользователя. Хотя обычно пользователей просят прислать адрес их электронной почты вместо пароля, никакой проверки фактически не производится. Многие FTP-хосты, предоставляющие обновления программного обеспечения, поддерживают анонимный доступ.

No.	Time	Source	Destination	Protocol	Length	Info
11823	27.890467	192.168.0.106	193.166.3.2	FTP	70	Request: USER anonymous
11825	27.913679	193.166.3.2	192.168.0.106	FTP	1465	Response: 331-welcome to the FUNET anonymous ftp archive
15743	33.459202	192.168.0.106	193.166.3.2	FTP	68	Request: PASS x@x.com
15744	33.481581	193.166.3.2	192.168.0.106	FTP	82	Response: 230 Any password will work

+	Frame 11823: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
+	Ethernet II, Src: Micro-St_25:cc:59 (4c:cc:6a:25:cc:59), Dst: Tp-LinkT_63:b5:cc (c0:4a:00:63:b5:cc)
+	Internet Protocol Version 4, Src: 192.168.0.106, Dst: 193.166.3.2
+	Transmission Control Protocol, Src Port: 52686, Dst Port: 21, Seq: 1044297986, Ack: 929890433, Len: 16
+	File Transfer Protocol (FTP)
+	USER anonymous\r\n
+	Request command: USER
+	Request arg: anonymous

Рис. 1.3: Отправка имени пользователя командой USER

No.	Time	Source	Destination	Protocol	Length	Info
11823	27.890467	192.168.0.106	193.166.3.2	FTP	70	Request: USER anonymous
11825	27.913679	193.166.3.2	192.168.0.106	FTP	1465	Response: 331-welcome to the FUNET anonymous ftp archive
15743	33.459202	192.168.0.106	193.166.3.2	FTP	68	Request: PASS x@x.com
15744	33.481581	193.166.3.2	192.168.0.106	FTP	82	Response: 230 Any password will work

+	Frame 11825: 1465 bytes on wire (11720 bits), 1465 bytes captured (11720 bits) on interface 0
+	Ethernet II, Src: Tp-LinkT_63:b5:cc (c0:4a:00:63:b5:cc), Dst: Micro-St_25:cc:59 (4c:cc:6a:25:cc:59)
+	Internet Protocol Version 4, Src: 193.166.3.2, Dst: 192.168.0.106
+	Transmission Control Protocol, Src Port: 21, Dst Port: 52686, Seq: 929890433, Ack: 1044298002, Len: 1411
+	File Transfer Protocol (FTP)
+	331-welcome to the FUNET anonymous ftp archive\r\n
+	Response code: user name okay, need password (331)
+	Response arg: welcome to the FUNET anonymous ftp archive
+	331- \r\n
+	331-Serving freely distributable files with FTP since 1990\r\n
+	331-\r\n

Рис. 1.4: Реакция сервера на правильное имя пользователя

Реакция сервера на имя пользователя - это FTP пакет с кодом 331 (имя пользователя корректно). Если имя пользователя не существует, то специальный FTP пакет с кодом ошибки не посылается (только на следующем этапе проверки пары имени пользователя и пароля). Это сделано для того, чтобы клиент не мог определить какие пользователи существуют на сервере.

No.	Time	Source	Destination	Protocol	Length	Info
11823	27.890467	192.168.0.106	193.166.3.2	FTP	70	Request: USER anonymous
11825	27.913679	193.166.3.2	192.168.0.106	FTP	1465	Response: 331-welcome to the FUNET anonymous ftp archive
15743	33.459202	192.168.0.106	193.166.3.2	FTP	68	Request: PASS x@x.com
15744	33.481581	193.166.3.2	192.168.0.106	FTP	82	Response: 230 Any password will work

+	Frame 15743: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0
+	Ethernet II, Src: Micro-St_25:cc:59 (4c:cc:6a:25:cc:59), Dst: Tp-LinkT_63:b5:cc (c0:4a:00:63:b5:cc)
+	Internet Protocol Version 4, Src: 192.168.0.106, Dst: 193.166.3.2
+	Transmission Control Protocol, Src Port: 52686, Dst Port: 21, Seq: 1044298002, Ack: 929891844, Len: 14
+	File Transfer Protocol (FTP)
+	PASS x@x.com\r\n
+	Request command: PASS
+	Request arg: x@x.com

Рис. 1.5: Отправка пароля командой PASS

No.	Time	Source	Destination	Protocol	Length	Info
11823	27.890467	192.168.0.106	193.166.3.2	FTP	70	Request: USER anonymous
11825	27.913679	193.166.3.2	192.168.0.106	FTP	1465	Response: 331-welcome to the FUNET anonymous ftp archive
15743	33.459202	192.168.0.106	193.166.3.2	FTP	68	Request: PASS x@x.com
15744	33.481581	193.166.3.2	192.168.0.106	FTP	82	Response: 230 Any password will work

+	Frame 15744: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
+	Ethernet II, Src: Tp-LinkT_63:b5:cc (c0:4a:00:63:b5:cc), Dst: Micro-St_25:cc:59 (4c:cc:6a:25:cc:59)
+	Internet Protocol Version 4, Src: 193.166.3.2, Dst: 192.168.0.106
+	Transmission Control Protocol, Src Port: 21, Dst Port: 52686, Seq: 929891844, Ack: 1044298016, Len: 28
+	File Transfer Protocol (FTP)
+	230 Any password will work\r\n
+	Response code: User logged in, proceed (230)
+	Response arg: Any password will work

Рис. 1.6: Реакция сервера на правильный пароль

Если пара имя пользователь и пароль правильная, то сервер возвращает FTP пакет с кодом 230 (пользователь идентифицирован), если нет, то 530 (вход не выполнен).

Стоит отметить, что ни имя пользователя, ни пароль не зашифровываются.

#### 1.4.4 Активный режим FTP

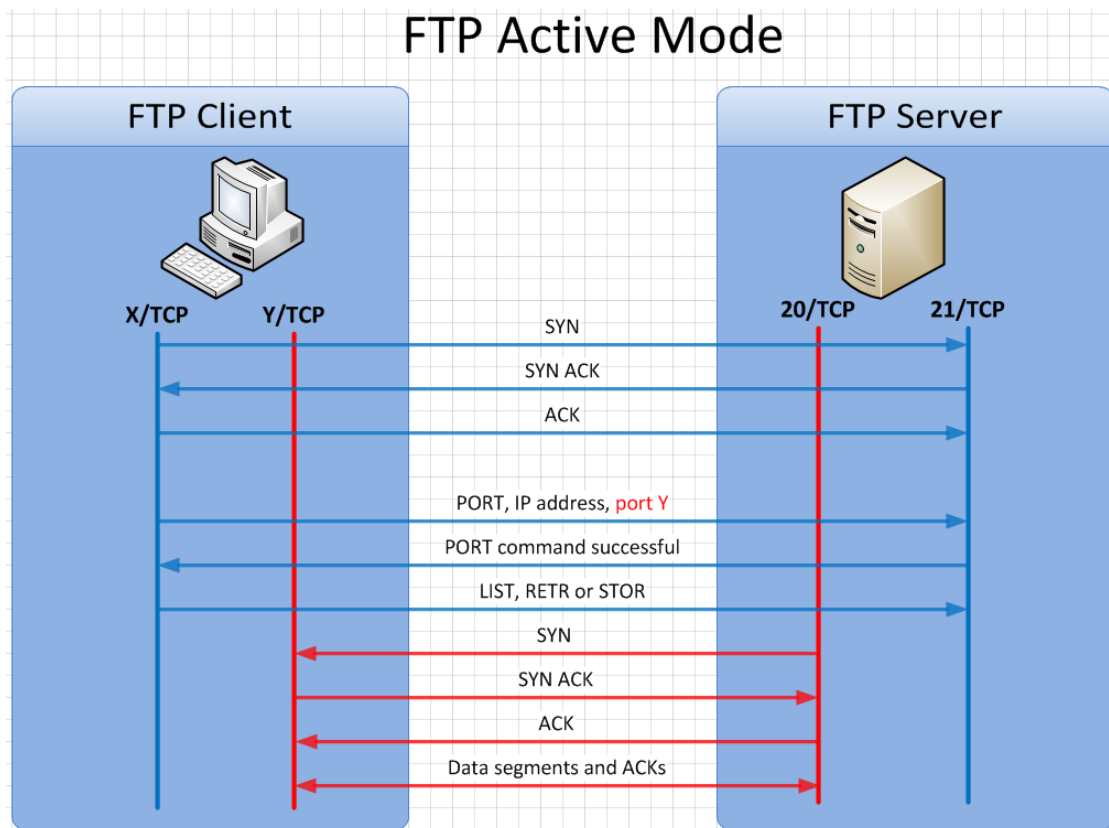


Рис. 1.7: Клиент-серверное взаимодействие в активном режиме FTP

Для перехода в активный режим клиент явно указывает собственный IP адрес (первые 4 байта аргумента) и порт подключения (последние 2 байта аргумента) командой PORT:

No.	Time	Source	Destination	Protocol	Length	Info
19672	40.922586	192.168.0.106	193.166.3.2	FTP	82	Request: PORT 192,168,0,106,205,207
19673	40.944983	193.166.3.2	192.168.0.106	FTP	83	Response: 200 PORT command successful

>	Frame 19672: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
>	Ethernet II, Src: Micro-St_25:cc:59 (4c:cc:6a:25:cc:59), Dst: Tp-LinkT_63:b5:cc (c0:4a:00:63:b5:cc)
>	Internet Protocol Version 4, Src: 192.168.0.106, Dst: 193.166.3.2
>	Transmission Control Protocol, Src Port: 52686, Dst Port: 21, Seq: 1044298016, Ack: 929891872, Len: 28
>	File Transfer Protocol (FTP)
>	PORT 192,168,0,106,205,207\r\n
>	Request command: PORT
>	Request arg: 192,168,0,106,205,207
>	Active IP address: 192.168.0.106
>	Active port: 52687

Рис. 1.8: Переход в активный режим

No.	Time	Source	Destination	Protocol	Length	Info
19672	40.922586	192.168.0.106	193.166.3.2	FTP	82	Request: PORT 192,168,0,106,205,207
19673	40.944983	193.166.3.2	192.168.0.106	FTP	83	Response: 200 PORT command successful

>	Frame 19673: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
>	Ethernet II, Src: Tp-LinkT_63:b5:cc (c0:4a:00:63:b5:cc), Dst: Micro-St_25:cc:59 (4c:cc:6a:25:cc:59)
>	Internet Protocol Version 4, Src: 193.166.3.2, Dst: 192.168.0.106
>	Transmission Control Protocol, Src Port: 21, Dst Port: 52686, Seq: 929891872, Ack: 1044298044, Len: 29
>	File Transfer Protocol (FTP)
>	200 PORT command successful\r\n
>	Response code: Command okay (200)
>	Response arg: PORT command successful

Рис. 1.9: Реакция сервера на успешный переход в активный режим

В случае успешного перехода в активный режим сервер возвращает FTP пакет с кодом 200 (команда корректна). После этого становятся доступными команды LIST, RETR, STORE и др. Установление соединения потока данных иницируется со стороны сервера после первой команды от клиента (аналогично уже рассмотренному в п. 1.4.2).

#### 1.4.5 Пассивный режим FTP

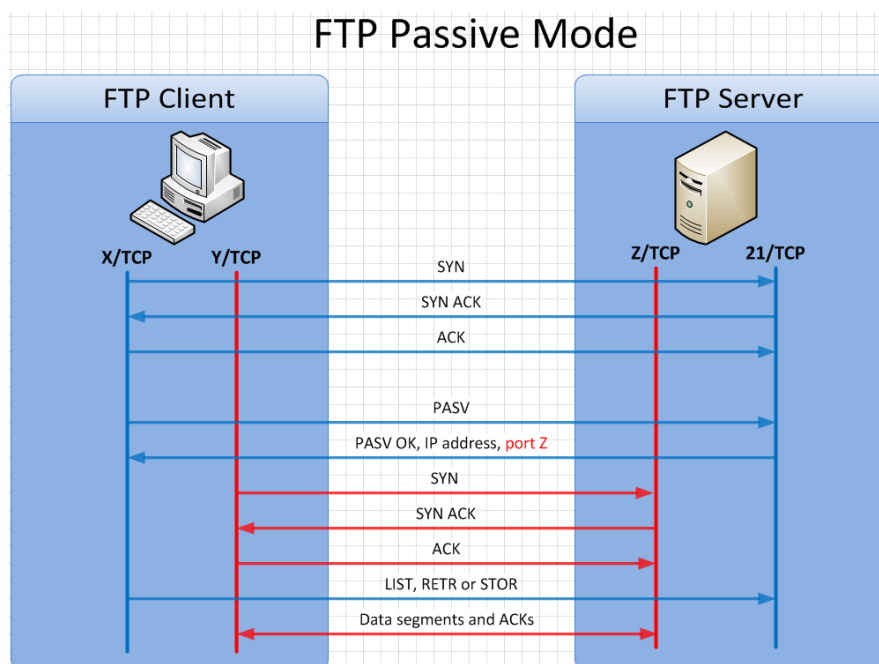


Рис. 1.10: Клиент-серверное взаимодействие в пассивном режиме FTP

Для перехода в пассивный режим клиент отправляет на сервер FTP пакет с единственной командой PASV:

No.	Time	Source	Destination	Protocol	Length	Info
3957	5.490896	192.168.0.106	193.166.3.2	FTP	60	Request: PASV
3958	5.512566	193.166.3.2	192.168.0.106	FTP	103	Response: 227 Entering Passive Mode (193,166,3,2,153,104)

```

> Frame 3957: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
> Ethernet II, Src: Micro-St_25:cc:59 (4c:cc:6a:25:cc:59), Dst: Tp-LinkT_63:b5:cc (c0:4a:00:63:b5:cc)
> Internet Protocol Version 4, Src: 192.168.0.106, Dst: 193.166.3.2
> Transmission Control Protocol, Src Port: 53054, Dst Port: 21, Seq: 802491085, Ack: 3990001957, Len: 6
✓ File Transfer Protocol (FTP)
  PASV\r\n
    Request command: PASV

```

Рис. 1.11: Переход в пассивный режим

В ответ сервер посылает FTP пакет с кодом 227 (переход в пассивный режим) и парой значений: IP адрес (первые 4 байта аргумента) и порт подключения (последние 2 байта аргумента):

No.	Time	Source	Destination	Protocol	Length	Info
3957	5.490896	192.168.0.106	193.166.3.2	FTP	60	Request: PASV
3958	5.512566	193.166.3.2	192.168.0.106	FTP	103	Response: 227 Entering Passive Mode (193,166,3,2,153,104)

```

> Frame 3958: 103 bytes on wire (824 bits), 103 bytes captured (824 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_63:b5:cc (c0:4a:00:63:b5:cc), Dst: Micro-St_25:cc:59 (4c:cc:6a:25:cc:59)
> Internet Protocol Version 4, Src: 193.166.3.2, Dst: 192.168.0.106
> Transmission Control Protocol, Src Port: 21, Dst Port: 53054, Seq: 3990001957, Ack: 802491091, Len: 49
✓ File Transfer Protocol (FTP)
  227 Entering Passive Mode (193,166,3,2,153,104)\r\n
    Response code: Entering Passive Mode (227)
    Response arg: Entering Passive Mode (193,166,3,2,153,104)
    Passive IP address: 193.166.3.2
    Passive port: 39272

```

Рис. 1.12: Реакция сервера на успешный переход в пассивный режим

После этого клиент инициирует установление соединения потока данных (аналогично уже рассмотренному в п. 1.4.2). После установления соединения потока данных становятся доступными команды LIST, PETR, STORE и др.

## 1.5 Вывод

В ходе работы был исследован сетевой трафик протокола FTP в активном и пассивном режиме.

Протокол FTP не безопасен, потому что не поддерживает шифрование данных. Это обусловлено тем, что во времена создания протокола проблема защиты данных не была так актуальна. Для решения проблемы безопасности были созданы защищенные вариации FTP, такие как:

- FTPS
- SFTP
- FTP через SSH

В большинстве случаев используется пассивный режим FTP соединения. Это обусловлено тем, что в пассивном режиме все соединения инициирует клиент и поэтому к нему нет никаких требований, он может находиться за NAT и брандмауэром, а также не иметь выделенного IP-адреса.

В активном режиме основная проблема возникает у клиента. Если брандмауэр настроен отбрасывать не инициированные изнутри входящие соединения, то сервер не сможет установить соединение для передачи данных. А так как порт для данных является динамическим, то возникают определенные сложности с настройкой брандмауэра. Наиболее правильным будет указать в клиенте диапазон используемых портов и создать для них разрешающее правило брандмауэра.

## 1.6 Приложение 1. Активный режим FTP

### 1.6.1 Передача данных

Рассмотрим процесс передачи данных в активном режиме. В этом режиме мы должны наблюдать, что установление соединения канала данных инициируется сервером с 20 порта (рис 1.7).

Рассмотрим полный процесс получения информации о каталоге (команда LIST):

Source	Destination	Protocol	Length	Info	Source port	Destination port
192.168.0.106	193.166.3.2	FTP	80	Request: PORT 192,168,0,106,227,9	58118	21
193.166.3.2	192.168.0.106	FTP	83	Response: 200 PORT command successful	21	58118
192.168.0.106	193.166.3.2	FTP	60	Request: LIST	58118	21
193.166.3.2	192.168.0.106	TCP	66	20 → 58121 [SYN] Seq=886803464 win=49640 Len=0 MSS=1460 WS=1 SACK_I	20	58121
192.168.0.106	193.166.3.2	TCP	66	58121 → 20 [SYN, ACK] Seq=3045168389 Ack=886803465 win=8192 Len=0	58121	20
193.166.3.2	192.168.0.106	TCP	60	20 → 58121 [ACK] Seq=886803465 Ack=3045168390 win=49640 Len=0	20	58121
193.166.3.2	192.168.0.106	FTP	84	Response: 150 Connecting to port 58121	21	58118
193.166.3.2	192.168.0.106	FTP-DATA	679	FTP Data: 625 bytes	20	58121
193.166.3.2	192.168.0.106	TCP	60	20 → 58121 [FIN, ACK] Seq=886804090 Ack=3045168390 win=49640 Len=0	20	58121
192.168.0.106	193.166.3.2	TCP	54	58121 → 20 [ACK] Seq=3045168390 Ack=886804091 win=65536 Len=0	58121	20
193.166.3.2	192.168.0.106	FTP	93	Response: 226-Options: -1	21	58118
192.168.0.106	193.166.3.2	TCP	54	58118 → 21 [ACK] Seq=110543292 Ack=596459411 win=8066 Len=0	58118	21
192.168.0.106	193.166.3.2	TCP	54	58121 → 20 [FIN, ACK] Seq=3045168390 Ack=886804091 win=65536 Len=0	58121	20
193.166.3.2	192.168.0.106	TCP	60	20 → 58121 [ACK] Seq=886804091 Ack=3045168391 win=49640 Len=0	20	58121

Рис. 1.13: Процесс передачи данных в активном режиме

В первую очередь, клиент посылает на сервер (по управляющему каналу) команду PORT с информацией (IP + port) для последующего подключения канала данных. Сервер отвечает кодом 200 (команда успешно выполнена), после чего клиентом отправляется команда LIST. Затем, сервер инициирует установку соединения данных с 20 порта на клиентский порт, указанный в команде PORT ранее. Как только соединение данных установлено, клиенту отправляется сообщение с кодом 150 (подготавливается открытие канала), а также результат операции получения каталога. Финальным этапом является завершение соединения канала данных: клиенту отправляется сообщение с кодом 226 (закрытие канала, обмен завершен успешно), а канал данных обменивается флагами FIN и соединение завершается.

Рассмотрим содержимое этих пакетов подробнее:

```
Internet Protocol Version 4, Src: 192.168.0.106, Dst: 193.166.3.2
Transmission Control Protocol, Src Port: 58118, Dst Port: 21, Seq: 1
File Transfer Protocol (FTP)
  PORT 192,168,0,106,227,9\r\n
    Request command: PORT
    Request arg: 192,168,0,106,227,9
    Active IP address: 192.168.0.106
    Active port: 58121
```

Рис. 1.14: Переход в активный режим

```
Internet Protocol Version 4, Src: 192.168.0.106, Dst: 193.166.3.2
Transmission Control Protocol, Src Port: 58118, Dst Port: 21, Seq: 1
File Transfer Protocol (FTP)
  LIST\r\n
    Request command: LIST
```

Рис. 1.15: Запрос на получение информации о каталоге

```
Internet Protocol Version 4, Src: 193.166.3.2, Dst: 192.168.0.106
Transmission Control Protocol, Src Port: 20, Dst Port: 58121, Seq: 1
  Source Port: 20
  Destination Port: 58121
  [Stream index: 18]
  [TCP Segment Len: 0]
  Sequence number: 886803464
  Acknowledgment number: 0
  Header Length: 32 bytes
  Flags: 0x002 (SYN)
```

Рис. 1.16: Запрос на установление соединения данных от FTP сервера



```
Internet Protocol Version 4, Src: 193.166.3.2, Dst: 192.168.0.106
Transmission Control Protocol, Src Port: 21, Dst Port: 58118, Seq: 596455
File Transfer Protocol (FTP)
  150 Connecting to port 58121\r\n
    Response code: File status okay; about to open data connection (150)
    Response arg: Connecting to port 58121
```

Рис. 1.17: Сообщение об успешном открытии канала данных

```
Internet Protocol Version 4, Src: 193.166.3.2, Dst: 192.168.0.106
Transmission Control Protocol, Src Port: 20, Dst Port: 58121, Seq:
FTP Data (-rw-rw-r-- 1 108 42 16677 Aug 18
```

Рис. 1.18: Результат выполнения запрашиваемой команды

## 1.7 Приложение 2. Пассивный режим FTP

### 1.7.1 Передача данных

Рассмотрим процесс передачи данных в пассивном режиме. В этом режиме мы должны наблюдать, что установление соединения канала данных инициируется клиентом на порт, указанный сервером в ответе на команду PASV (рис 1.10).

Рассмотрим полный процесс получения информации о каталоге (команда LIST):

Source	Destination	Protocol	Length	Info	Source port	Destination port
192.168.0.106	193.166.3.2	FTP	60	Request: PASV	58215	21
193.166.3.2	192.168.0.106	FTP	103	Response: 227 Entering Passive Mode (193,166,3,2,138,136)	21	58215
192.168.0.106	193.166.3.2	TCP	54	58215 → 21 [ACK] Seq=2768002206 Ack=2715235388 win=261816 Len=0	58215	21
192.168.0.106	193.166.3.2	TCP	66	58216 → 35464 [SYN] Seq=3120340623 win=65535 Len=0 MSS=1460 WS=8 S/	58216	35464
193.166.3.2	192.168.0.106	TCP	66	35464 → 58216 [SYN, ACK] Seq=2717166666 Ack=3120340624 win=49640 Lr	35464	58216
192.168.0.106	193.166.3.2	TCP	54	58216 → 35464 [ACK] Seq=3120340624 Ack=2717166667 win=262144 Len=0	58216	35464
192.168.0.106	193.166.3.2	FTP	60	Request: LIST	58215	21
193.166.3.2	192.168.0.106	FTP	84	Response: 150 Accepted data connection	21	58215
192.168.0.106	193.166.3.2	TCP	54	58215 → 21 [ACK] Seq=2768002212 Ack=2715235418 win=261784 Len=0	58215	21
193.166.3.2	192.168.0.106	FTP-DATA	679	FTP Data: 625 bytes	35464	58216
192.168.0.106	193.166.3.2	TCP	54	58216 → 35464 [ACK] Seq=3120340624 Ack=2717167292 win=261512 Len=0	58216	35464
193.166.3.2	192.168.0.106	TCP	60	35464 → 58216 [FIN, ACK] Seq=2717167292 Ack=3120340624 win=49640 Lr	35464	58216
193.166.3.2	192.168.0.106	FTP	93	Response: 226-Options: -l	21	58215
192.168.0.106	193.166.3.2	TCP	54	58215 → 21 [ACK] Seq=2768002212 Ack=2715235457 win=261744 Len=0	58215	21
192.168.0.106	193.166.3.2	TCP	54	58216 → 35464 [FIN, ACK] Seq=3120340624 Ack=2717167293 win=261512 Lr	58216	35464
193.166.3.2	192.168.0.106	TCP	60	35464 → 58216 [ACK] Seq=2717167293 Ack=3120340625 win=49640 Len=0	35464	58216

Рис. 1.19: Процесс передачи данных в пассивном режиме

В первую очередь, клиент посылает на сервер (по управляющему каналу) команду PASV, в результате чего возвращается информация (IP + port) с кодом 227 (переход в пассивный режим) для последующего подключения канала данных. Затем, клиент инициирует установление соединения данных с произвольного порта на серверный порт, указанный в ответе на команду PASV ранее. Как только соединение данных установлено, на сервер отправляется команда LIST. Затем, клиенту отправляется сообщение с кодом 150 (подготавливается открытие канала), а также результат операции получения каталога. Финальным этапом является завершение соединения канала данных: клиенту отправляется сообщение с кодом 226 (закрытие канала, обмен завершен успешно), а канал данных обменивается флагами FIN и соединение завершается.

Стоит отметить, что в отличие от активного режима, установление соединения канала данных производится перед отправлением команды LIST по управляющему каналу.

Рассмотрим содержимое этих пакетов подробнее:

```
Internet Protocol Version 4, Src: 193.166.3.2, Dst: 192.168.0.106
Transmission Control Protocol, Src Port: 21, Dst Port: 58215, Seq:
File Transfer Protocol (FTP)
  227 Entering Passive Mode (193,166,3,2,138,136)\r\n
    Response code: Entering Passive Mode (227)
    Response arg: Entering Passive Mode (193,166,3,2,138,136)
    Passive IP address: 193.166.3.2
    Passive port: 35464
```

Рис. 1.20: Переход в пассивный режим

```

Internet Protocol Version 4, Src: 192.168.0.106, Dst: 193.166.3.2
Transmission Control Protocol, Src Port: 58216, Dst Port: 35464, Seq: 3120340623, Len: 0
  Source Port: 58216
  Destination Port: 35464
  [Stream index: 11]
  [TCP Segment Len: 0]
  Sequence number: 3120340623
  Acknowledgment number: 0
  Header Length: 32 bytes
  Flags: 0x002 (SYN)

```

Рис. 1.21: Запрос на установление соединения данных от FTP клиента

```

Internet Protocol Version 4, Src: 192.168.0.106, Dst: 193.166.3.2
Transmission Control Protocol, Src Port: 58215, Dst Port: 21, Seq: 3120340623
File Transfer Protocol (FTP)
  LIST\r\n
  Request command: LIST

```

Рис. 1.22: Запрос на получение информации о каталоге

```

Internet Protocol Version 4, Src: 193.166.3.2, Dst: 192.168.0.106
Transmission Control Protocol, Src Port: 21, Dst Port: 58215, Seq: 3120340623
File Transfer Protocol (FTP)
  150 Accepted data connection\r\n
  Response code: File status okay; about to open data connection
  Response arg: Accepted data connection

```

Рис. 1.23: Сообщение об успешном открытии канала данных

```

Internet Protocol Version 4, Src: 193.166.3.2, Dst: 192.168.0.106
Transmission Control Protocol, Src Port: 35464, Dst Port: 58216, Seq: 3120340623
FTP Data (-rw-rw-r-- 1 108 42 16677 Aug 18 2015)

```

Рис. 1.24: Результат выполнения запрашиваемой команды