

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:

Ерниязов Т.Е.

Группа: 43501/3

Проверил:

Новопашенный А.Г.

Санкт-Петербург
2018 г.

Содержание

1	Лабораторная работа №2	2
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	7

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

```
настройка протокола IP для windows

Ethernet adapter Сетевое подключение Bluetooth:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Ethernet adapter Подключение по локальной сети:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::98dc:a34b:531a:c304%13
    IPv4-адрес. . . . . : 192.168.0.105
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.0.1

Туннельный адаптер isatap.{068CDECD-51A9-44F3-8865-6D5FFB3DFA26}:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Туннельный адаптер Подключение по локальной сети* 12:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Туннельный адаптер isatap.{7E82D5E7-222B-409B-8509-795D76264FD9}:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :
```

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 в активном режиме был выбран сервер ftp://ftp.funet.fi, а для пассивного - sourceware.org.

1.4.2 Установление управляющего соединения

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

173	48.038125	192.168.0.105	195.208.113.150	TCP	66	55148 → 21 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=1 SACK_PERM=1
174	48.039530	195.208.113.150	192.168.0.105	TCP	66	21 → 55148 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1 WS=16
175	48.039563	192.168.0.105	195.208.113.150	TCP	54	55148 → 21 [ACK] Seq=1 Ack=1 Win=8192 Len=0

Рис. 1.2: Установление TCP соединения с 21 портом сервера

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.

203	52.590648	192.168.0.105	195.208.113.150	FTP	66	Request: USER stud5
▶ Frame 203: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0 ▶ Ethernet II, Src: lmk (c8:0a:a9:d0:5c:0a), Dst: Tp-LinkT_91:26:1c (64:70:02:91:26:1c) ▶ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 195.208.113.150 ▶ Transmission Control Protocol, Src Port: 55148, Dst Port: 21, Seq: 1, Ack: 77, Len: 12 ▶ File Transfer Protocol (FTP) ▶ USER stud5\r\n Request command: USER Request arg: stud5						

Рис. 1.3: Отправка имени пользователя командой USER

205	52.592527	195.208.113.150	192.168.0.105	FTP	87	Response: 331 Password required for stud5
207	52.790433	192.168.0.105	195.208.113.150	TCP	54	55148 → 21 [ACK] Seq=13 Ack=110 Win=8083
▶ Frame 205: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface 0 ▶ Ethernet II, Src: Tp-LinkT_91:26:1c (64:70:02:91:26:1c), Dst: lmk (c8:0a:a9:d0:5c:0a) ▶ Internet Protocol Version 4, Src: 195.208.113.150, Dst: 192.168.0.105 ▶ Transmission Control Protocol, Src Port: 21, Dst Port: 55148, Seq: 77, Ack: 13, Len: 33 ▶ File Transfer Protocol (FTP) ▶ 331 Password required for stud5\r\n Response code: User name okay, need password (331) Response arg: Password required for stud5						

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.

327	87.230397	192.168.0.105	195.208.113.150	FTP	68 Request: PASS NFhtkrf
▶ Frame 327: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 0 ▶ Ethernet II, Src: lmk (c8:0a:a9:d0:5c:0a), Dst: Tp-LinkT_91:26:1c (64:70:02:91:26:1c) ▶ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 195.208.113.150 ▶ Transmission Control Protocol, Src Port: 55148, Dst Port: 21, Seq: 13, Ack: 110, Len: 14 ▶ File Transfer Protocol (FTP)					
▶ PASS NFhtkrf\r\n Request command: PASS Request arg: NFhtkrf					

Рис. 1.5: Отправка пароля командой PASS

328	87.242533	195.208.113.150	192.168.0.105	FTP	80 Response: 230 User stud5 logged in
▶ Frame 328: 80 bytes on wire (640 bits), 80 bytes captured (640 bits) on interface 0 ▶ Ethernet II, Src: Tp-LinkT_91:26:1c (64:70:02:91:26:1c), Dst: lmk (c8:0a:a9:d0:5c:0a) ▶ Internet Protocol Version 4, Src: 195.208.113.150, Dst: 192.168.0.105 ▶ Transmission Control Protocol, Src Port: 21, Dst Port: 55148, Seq: 110, Ack: 27, Len: 26 ▶ File Transfer Protocol (FTP)					
▶ 230 User stud5 logged in\r\n Response code: User logged in, proceed (230) Response arg: User stud5 logged in					

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

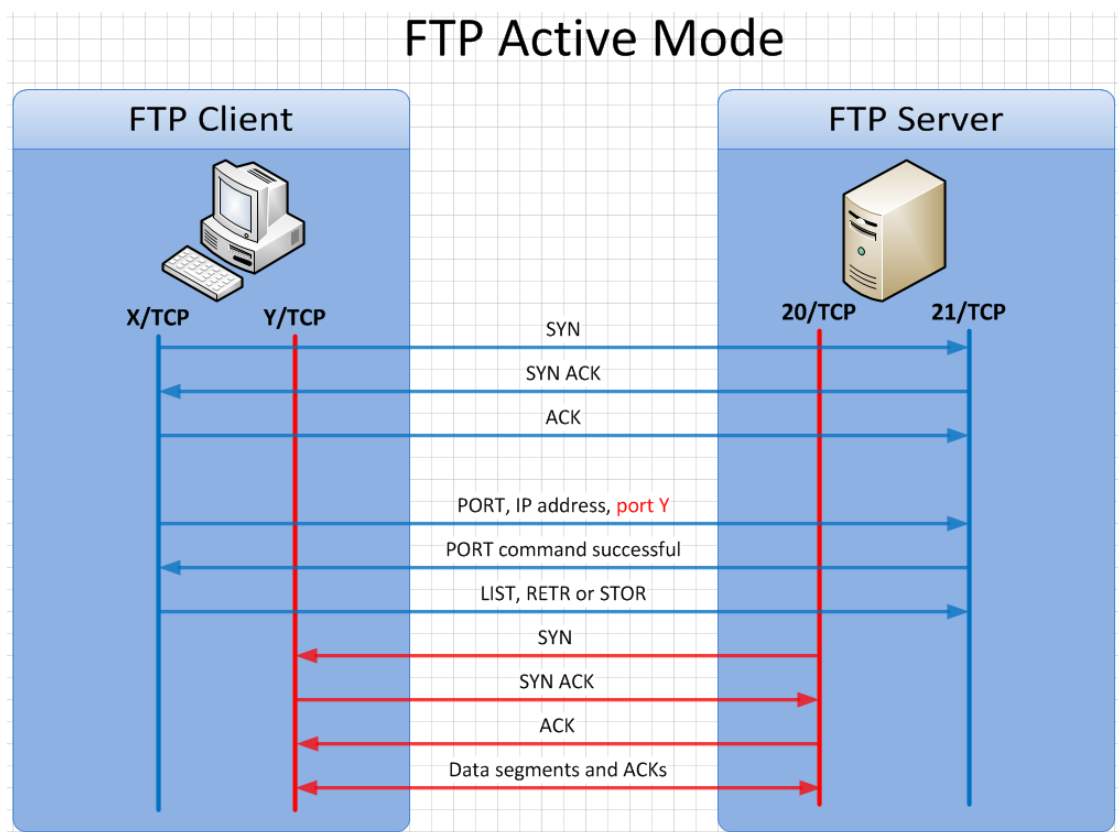


Рис. 1.7: Клиент-серверное взаимодействие в активном режиме FTP

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

В случае успешного перехода в активный режим сервер возвращает FTP пакет с кодом 200 (команда корректна). После этого становятся доступными команды LIST, PETR, STORE и др.

Запросим список файлов в текущей директории командой ls:

Заметим, что установление соединения канала данных инициируется сервером с 20 порта.

353	92.933695	192.168.0.105	195.208.113.150	FTP	82 Request: PORT 192,168,0,105,215,109
▶ Frame 353: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0 ▶ Ethernet II, Src: lmk (c8:0a:a9:d0:5c:0a), Dst: Tp-LinkT_91:26:1c (64:70:02:91:26:1c) ▶ Internet Protocol Version 4, Src: 192.168.0.105, Dst: 195.208.113.150 ▶ Transmission Control Protocol, Src Port: 55148, Dst Port: 21, Seq: 27, Ack: 136, Len: 28 ▶ File Transfer Protocol (FTP) ▶ PORT 192,168,0,105,215,109\r\n Request command: PORT Request arg: 192,168,0,105,215,109 Active IP address: 192.168.0.105 Active port: 55149					

Рис. 1.8: Переход в активный режим

354	92.935660	195.208.113.150	192.168.0.105	FTP	83 Response: 200 PORT command successful
▶ Frame 354: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0 ▶ Ethernet II, Src: Tp-LinkT_91:26:1c (64:70:02:91:26:1c), Dst: lmk (c8:0a:a9:d0:5c:0a) ▶ Internet Protocol Version 4, Src: 195.208.113.150, Dst: 192.168.0.105 ▶ Transmission Control Protocol, Src Port: 21, Dst Port: 55148, Seq: 136, Ack: 55, 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

355	92.938828	192.168.0.105	195.208.113.150	FTP	60 Request: NLST
356	92.940559	195.208.113.150	192.168.0.105	TCP	74 20 → 55149 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK
357	92.940638	192.168.0.105	195.208.113.150	TCP	74 55149 → 20 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=
358	92.941989	195.208.113.150	192.168.0.105	TCP	66 20 → 55149 [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=3
359	92.942227	195.208.113.150	192.168.0.105	FTP	108 Response: 150 Opening ASCII mode data connection for
360	92.942678	195.208.113.150	192.168.0.105	FTP-DATA	110 FTP Data: 44 bytes
361	92.942678	195.208.113.150	192.168.0.105	TCP	66 20 → 55149 [FIN, ACK] Seq=45 Ack=1 Win=14608 Len=0 TS
362	92.942703	192.168.0.105	195.208.113.150	TCP	66 55149 → 20 [ACK] Seq=1 Ack=46 Win=66560 Len=0 TSval=
363	92.946650	192.168.0.105	195.208.113.150	TCP	66 55149 → 20 [FIN, ACK] Seq=1 Ack=46 Win=66560 Len=0 TS
364	92.947881	195.208.113.150	192.168.0.105	TCP	66 20 → 55149 [ACK] Seq=46 Ack=2 Win=14608 Len=0 TSval=
365	92.948256	195.208.113.150	192.168.0.105	FTP	77 Response: 226 Transfer complete
▶ Frame 356: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0 ▶ Ethernet II, Src: Tp-LinkT_91:26:1c (64:70:02:91:26:1c), Dst: lmk (c8:0a:a9:d0:5c:0a) ▶ Internet Protocol Version 4, Src: 195.208.113.150, Dst: 192.168.0.105 ▶ Transmission Control Protocol, Src Port: 20, Dst Port: 55149, Seq: 0, Len: 0					

Рис. 1.10: Запрос списка файлов

1.4.5 Пассивный режим FTP

Для подключения к sourceware.org воспользуемся утилитой telnet.
Данные в telnet передаются посимвольно:

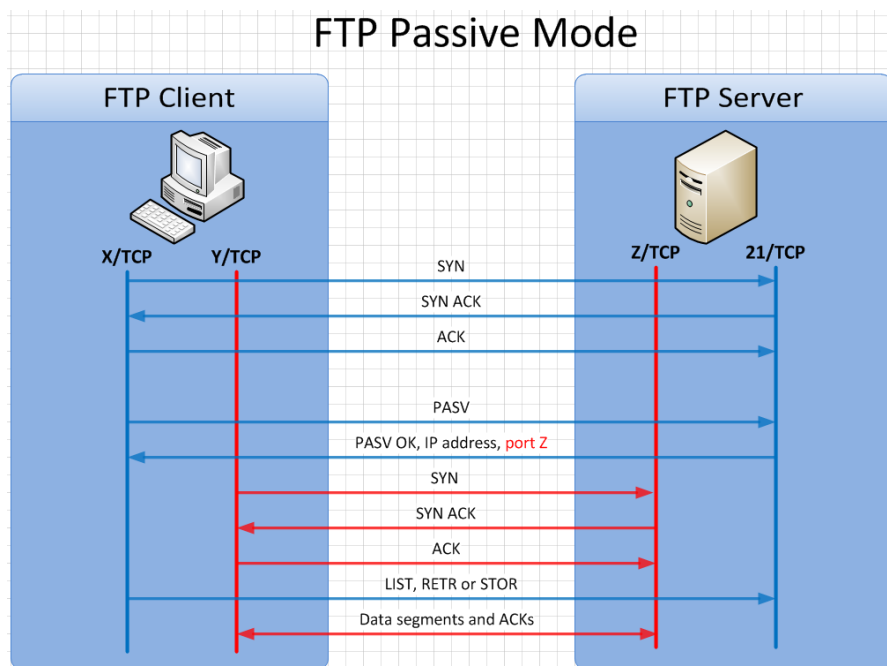


Рис. 1.11: Клиент-серверное взаимодействие в пассивном режиме FTP

6140	725.592980	192.168.0.105	209.132.180.131	FTP	55 Request: U
6141	725.768143	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=2 Win=14720 Len=0
6142	725.768157	192.168.0.105	209.132.180.131	FTP	55 Request: S
6143	725.941826	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=3 Win=14720 Len=0
6144	725.941845	192.168.0.105	209.132.180.131	FTP	55 Request: E
6145	726.115604	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=4 Win=14720 Len=0
6146	726.115631	192.168.0.105	209.132.180.131	FTP	55 Request: R
6148	726.289418	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=5 Win=14720 Len=0
6149	726.569222	192.168.0.105	209.132.180.131	FTP	55 Request:
6150	726.743874	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=6 Win=14720 Len=0
6165	729.729138	192.168.0.105	209.132.180.131	FTP	55 Request: a
6166	729.903211	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=7 Win=14720 Len=0
6167	729.960673	192.168.0.105	209.132.180.131	FTP	55 Request: n
6168	730.134358	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=8 Win=14720 Len=0
6170	730.440765	192.168.0.105	209.132.180.131	FTP	55 Request: o
6171	730.615392	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=9 Win=14720 Len=0
6172	730.720369	192.168.0.105	209.132.180.131	FTP	55 Request: n
6173	730.894393	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=10 Win=14720 Len=0
6174	731.033012	192.168.0.105	209.132.180.131	FTP	55 Request: y
6176	731.206721	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=11 Win=14720 Len=0
6177	731.639484	192.168.0.105	209.132.180.131	FTP	55 Request: m
6178	731.813285	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=12 Win=14720 Len=0
6179	731.960467	192.168.0.105	209.132.180.131	FTP	55 Request: o
6181	732.134313	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=13 Win=14720 Len=0
6182	732.215419	192.168.0.105	209.132.180.131	FTP	55 Request: u
6183	732.389199	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=14 Win=14720 Len=0
6184	732.448625	192.168.0.105	209.132.180.131	FTP	55 Request: s
6185	732.623225	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=15 Win=14720 Len=0
6186	733.007294	192.168.0.105	209.132.180.131	FTP	56 Request:
6187	733.181659	209.132.180.131	192.168.0.105	TCP	60 21 → 55262 [ACK] Seq=24 Ack=17 Win=14720 Len=0
6188	733.181922	209.132.180.131	192.168.0.105	FTP	129 Response: 331 Anonymous login ok, send your complete ema

Рис. 1.12: Посимвольная передача логина

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

6863	755.092784	209.132.180.131	192.168.0.105	FTP	106 Response: 227 Entering Passive Mode (209,132,180,131,39,92).
Frame 6863: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0 Ethernet II, Src: Tp-LinkT_91:26:1c (64:70:02:91:26:1c), Dst: lmk (c8:0a:a9:d0:5c:0a) Internet Protocol Version 4, Src: 209.132.180.131, Dst: 192.168.0.105 Transmission Control Protocol, Src Port: 21, Dst Port: 55262, Seq: 476, Ack: 47, Len: 52 File Transfer Protocol (FTP) 227 Entering Passive Mode (209,132,180,131,39,92).\r\n Response code: Entering Passive Mode (227) Response arg: Entering Passive Mode (209,132,180,131,39,92). Passive IP address: 209.132.180.131 Passive port: 10076					

Рис. 1.13: Переход в пассивный режим

Затем клиент инициирует установление соединения с произвольного порта на серверный порт, указанный в ответе на команду PASV ранее. Со второго терминала подключимся по полученному адресу:

7261	812.997173	192.168.0.105	209.132.180.131	TCP	66 55281 → 10076 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
7262	813.173849	209.132.180.131	192.168.0.105	TCP	66 10076 → 55281 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1360 SACK_PERM=1 WS=128
7263	813.173882	192.168.0.105	209.132.180.131	TCP	54 55281 → 10076 [ACK] Seq=1 Ack=1 Win=66560 Len=0
Frame 7261: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0 Ethernet II, Src: lmk (c8:0a:a9:d0:5c:0a), Dst: Tp-LinkT_91:26:1c (64:70:02:91:26:1c) Internet Protocol Version 4, Src: 192.168.0.105, Dst: 209.132.180.131 Transmission Control Protocol, Src Port: 55281, Dst Port: 10076, Seq: 0, Len: 0					

Рис. 1.14: Установление соединения по полученному адресу

Запросим данные по управляющему каналу. Сервер передаст их по каналу данных и инициирует закрытие соединения.

7940	944.741642	209.132.180.131	192.168.0.105	FTP-DATA	751 FTP Data: 697 bytes
7941	944.741643	209.132.180.131	192.168.0.105	TCP	60 10076 → 55281 [FIN, ACK] Seq=698 Ack=5 Win=14720

Рис. 1.15: Передача данных

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.


```

> Frame 7943: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
> Ethernet II, Src: Tp-LinkT_91:26:1c (64:70:02:91:26:1c), Dst: lmk (c8:0a:a9:d0:5c:0a)
  Internet Protocol Version 4, Src: 209.132.180.131, Dst: 192.168.0.105
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 63
    Identification: 0xa717 (42775)
  > Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 41
    Protocol: TCP (6)
    Header checksum: 0x6388 [validation disabled]
    [Header checksum status: Unverified]
    Source: 209.132.180.131
    Destination: 192.168.0.105
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  Transmission Control Protocol, Src Port: 21, Dst Port: 55262, Seq: 800, Ack: 151, Len: 23
    Source Port: 21
    Destination Port: 55262
    [Stream index: 129]
    [TCP Segment Len: 23]
    Sequence number: 800 (relative sequence number)
    [Next sequence number: 823 (relative sequence number)]
    Acknowledgment number: 151 (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    000. .... = Reserved: Not set
    ...0 .... = Nonce: Not set
    ... 0... = Congestion Window Reduced (CWR): Not set
    .... 0... = ECN-Echo: Not set
    .... ..0. = Urgent: Not set
    .... ...1 = Acknowledgment: Set
    .... .... 1.. = Push: Set
    .... .... .0.. = Reset: Not set
    .... .... ..0. = Syn: Not set
    .... .... ...0 = Fin: Not set
    [TCP Flags: .....AP...]
    Window size value: 115
    [Calculated window size: 14720]
    [Window size scaling factor: 128]
    Checksum: 0xb5c9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
    TCP payload (23 bytes)
  File Transfer Protocol (FTP)
    226 Transfer complete\r\n
      Response code: Closing data connection (226)
      Response arg: Transfer complete

```

Рис. 1.16: Пакет с запрошенными данными

```

▷ Frame 7940: 751 bytes on wire (6008 bits), 751 bytes captured (6008 bits) on interface 0
▷ Ethernet II, Src: Tp-LinkT_91:26:1c (64:70:02:91:26:1c), Dst: lmk (c8:0a:a9:d0:5c:0a)
✦ Internet Protocol Version 4, Src: 209.132.180.131, Dst: 192.168.0.105
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▷ Differentiated Services Field: 0x28 (DSCP: AF11, ECN: Not-ECT)
        Total Length: 737
        Identification: 0xf841 (63553)
    ▷ Flags: 0x02 (Don't Fragment)
        Fragment offset: 0
        Time to live: 41
        Protocol: TCP (6)
        Header checksum: 0xf94 [validation disabled]
        [Header checksum status: Unverified]
        Source: 209.132.180.131
        Destination: 192.168.0.105
        [Source GeoIP: Unknown]
        [Destination GeoIP: Unknown]
✦ Transmission Control Protocol, Src Port: 10076, Dst Port: 55281, Seq: 1, Ack: 5, Len: 697
    Source Port: 10076
    Destination Port: 55281
    [Stream index: 149]
    [TCP Segment Len: 697]
    Sequence number: 1 (relative sequence number)
    [Next sequence number: 698 (relative sequence number)]
    Acknowledgment number: 5 (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
    ✦ Flags: 0x018 (PSH, ACK)
        000. .... = Reserved: Not set
        ...0 .... = Nonce: Not set
        .... 0... = Congestion Window Reduced (CWR): Not set
        .... .0.. = ECN-Echo: Not set
        .... ..0. = Urgent: Not set
        .... ...1 .... = Acknowledgment: Set
        .... .... 1... = Push: Set
        .... .... .0.. = Reset: Not set
        .... .... ..0. = Syn: Not set
        .... .... ...0 = Fin: Not set
        [TCP Flags: .....AP...]
    Window size value: 115
    [Calculated window size: 14720]
    [Window size scaling factor: 128]
    Checksum: 0xba4b [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
    ▷ [SEQ/ACK analysis]
        TCP payload (697 bytes)
FTP Data (c966dc72304c5e0fc0ad6694cd8685f7 autoconf-2.10-2.11.diff.gz\r\nfe332d45a554c81bd5a1a758ea2c53be autoconf-2.

```

Рис. 1.17: Пакет с кодом закрытия канала

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.