

Санкт-Петербургский Политехнический Университет Петра Великого
Институт компьютерных наук и технологий
Кафедра компьютерных систем и программных технологий

Отчёт по лабораторной работе №2
Дисциплина: Защита информации
Тема: Исследование сетевого трафика

Выполнил студент группы 43501/3

_____ Круминьш Д.В.
(подпись)

Преподаватель

_____ Новопашенный А.Г.
(подпись)

Санкт-Петербург
2017 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
1.5	Вывод	9

Лабораторная работа №2

1.1 Цель работы

Продолжение получения навыков по исследованию сетевого трафика.

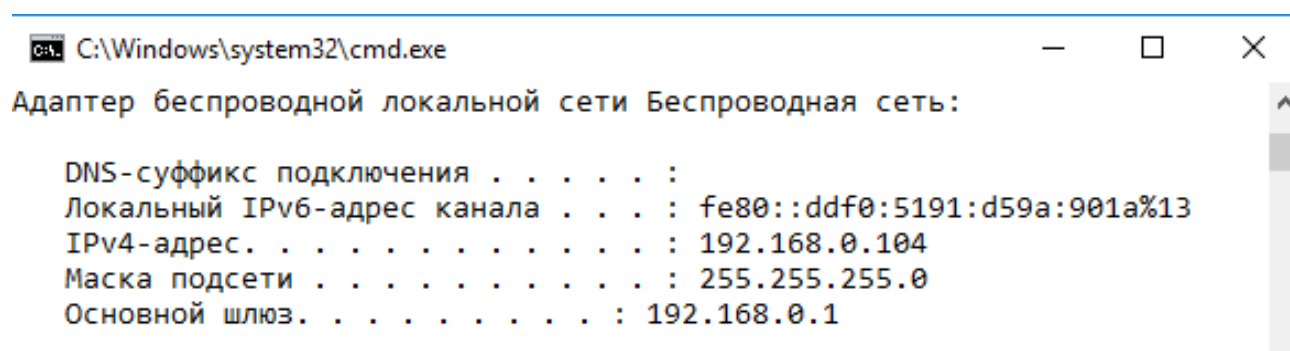
1.2 Программа работы

При помощи анализатора сетевого трафика Wireshark продемонстрировать в сети работу протокола FTP, в частности:

- пассивный режим,
- активный режим,
- рассмотреть его безопасность.

1.3 Конфигурация сети

Опыты проводились используя ПК, конфигурация которого представлена ниже.



```
C:\Windows\system32\cmd.exe
Адаптер беспроводной локальной сети Беспроводная сеть:

DNS-суффикс подключения . . . . . :
Локальный IPv6-адрес канала . . . : fe80::ddf0:5191:d59a:901a%13
IPv4-адрес. . . . . : 192.168.0.104
Маска подсети . . . . . : 255.255.255.0
Основной шлюз. . . . . : 192.168.0.1
```

Рис. 1.1: Конфигурация ПК

1.4 Ход работы

1.4.1 Протокол FTP

FTP может работать в активном или пассивном режиме, от выбора которого зависит способ установки соединения. В активном режиме клиент создаёт управляющее TCP-соединение с сервером и отправляет

серверу свой IP-адрес и произвольный номер клиентского порта, после чего ждёт, пока сервер не запустит TCP-соединение с этим адресом и номером порта. В случае, если клиент находится за брандмауэром и не может принять входящее TCP-соединение, может быть использован пассивный режим. В этом режиме клиент использует поток управления, чтобы послать серверу команду PASV, и затем получает от сервера его IP-адрес и номер порта, которые затем используются клиентом для открытия потока данных с произвольного клиентского порта к полученному адресу и порту.

Пассивный режим

Подключение будет происходить согласно приведенной на рисунке 1.2 схеме. В качестве ftp-сервера был выбран **ftp.neva.ru**.

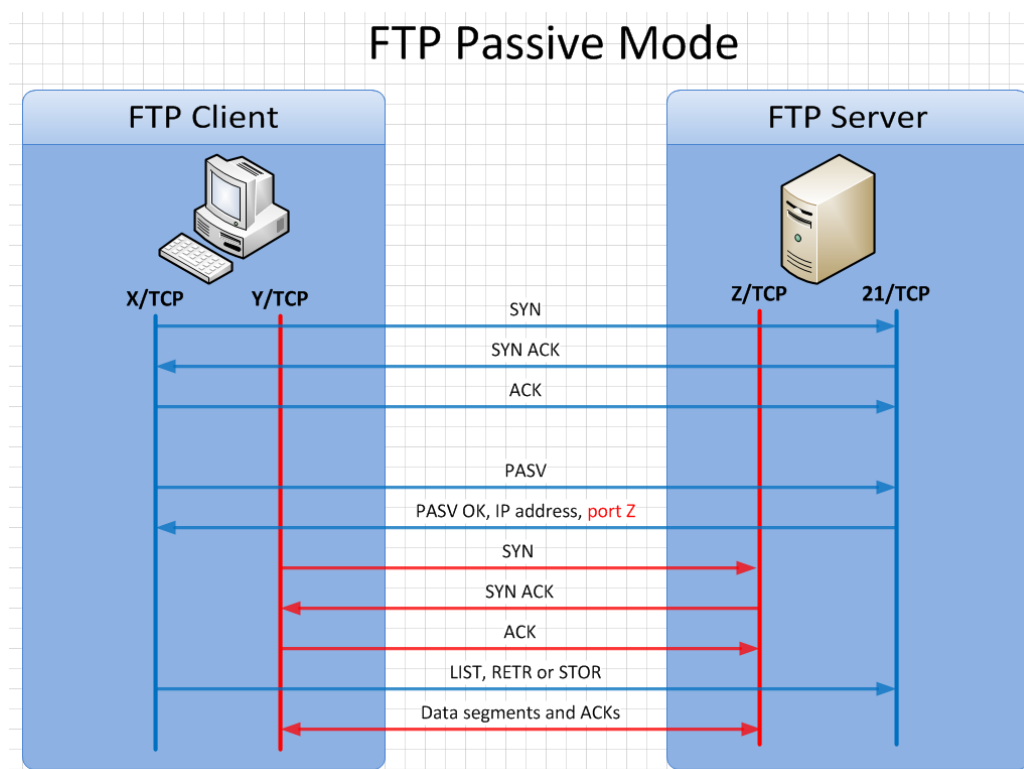


Рис. 1.2: Схема взаимодействия клиента и сервера при пассивном режиме

Сперва от произвольного порта клиента, создается управляющее tcp-соединения к 21 порту сервера. Механизм создания такого соединения был уже описан в предыдущей лабораторной работе. В данном случае такое соединения создалось с **192.168.0.104:52976** к **195.208.113.245:21**.

Time	Source	Destination	Protocol	Length	Info
0.005707	192.168.0.104	195.208.113.245	TCP	66	52976 → 21 [SYN] Seq=1864282806 Win=8192 Len=0 MSS=1460 WS=256
0.011031	195.208.113.245	192.168.0.104	TCP	66	21 → 52976 [SYN, ACK] Seq=4016046853 Ack=1864282807 Win=14600
0.011116	192.168.0.104	195.208.113.245	TCP	54	52976 → 21 [ACK] Seq=1864282807 Ack=4016046854 Win=16384 Len=0

Рис. 1.3: Пакеты для создания управляющего tcp-соединения

No.	Time	Source	Destination	Protocol	Length	Info
...	0.072149	192.168.0.104	195.208.113.245	FTP	60	Request: PASV
> Frame 21: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 > Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6) > Internet Protocol Version 4, Src: 192.168.0.104, Dst: 195.208.113.245 > Transmission Control Protocol, Src Port: 52976, Dst Port: 21, Seq: 1864282877, Ack: 4016047156, Len: 6						
Source Port: 52976 Destination Port: 21 [Stream index: 1] [TCP Segment Len: 6] Sequence number: 1864282877 [Next sequence number: 1864282883] Acknowledgment number: 4016047156 Header Length: 20 bytes						
> Flags: 0x018 (PSH, ACK) Window size value: 63 [Calculated window size: 16128] [Window size scaling factor: 256] Checksum: 0x2359 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 > [SEQ/ACK analysis]						
> File Transfer Protocol (FTP) > PASV\r\n Request command: PASV						

Рис. 14: Запрос перехода в пассивный режим

От клиента произошла отправка пакета с командой **PASV** для перехода в пассивный режим.

No.	Time	Source	Destination	Protocol	Length	Info
...	0.076968	195.208.113.245	192.168.0.104	FTP	108	Response: 227 Entering Passive Mode (195,208,113,245,231,105).
> Frame 22: 108 bytes on wire (864 bits), 108 bytes captured (864 bits) on interface 0 > Ethernet II, Src: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6), Dst: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd) > Internet Protocol Version 4, Src: 195.208.113.245, Dst: 192.168.0.104 > Transmission Control Protocol, Src Port: 21, Dst Port: 52976, Seq: 4016047156, Ack: 1864282883, Len: 54						
Source Port: 21 Destination Port: 52976 [Stream index: 1] [TCP Segment Len: 54] Sequence number: 4016047156 [Next sequence number: 4016047210] Acknowledgment number: 1864282883 Header Length: 20 bytes						
> Flags: 0x018 (PSH, ACK) Window size value: 29 [Calculated window size: 14848] [Window size scaling factor: 512] Checksum: 0x01ed [unverified] [Checksum Status: Unverified] Urgent pointer: 0 > [SEQ/ACK analysis]						
> File Transfer Protocol (FTP) > 227 Entering Passive Mode (195,208,113,245,231,105).\r\n Response code: Entering Passive Mode (227) Response arg: Entering Passive Mode (195,208,113,245,231,105). Passive IP address: 195.208.113.245 Passive port: 59241						

Рис. 15: Координаты для пассивного режима

Сервер в ответ на команду PASV передает координаты для подключения к нему клиента. Код 227 означает переход в пассивный режим. WireShark уже сразу показывает передаваемый адрес и порт для подключения, на самом деле эти данные передаются в виде 6 чисел (**h1,h2,h3,h4,p1,p2**). Первые 4 обозначают IP-адрес, а оставшиеся два для вычисления номера порта подключения.

Номер порта вычисляется по формуле **PASV port=(p1*256)+p2**, т.е. в данном случае **(231*256)+105=59241**.

После этого клиент пытается подключиться к серверу по указанным координатам. Подключение выполняется по стандартной схеме создания соединения по протоколу TCP.

No.	Time	Source	Destination	Protocol	Length	Info
...	0.077631	192.168.0.104	195.208.113.245	TCP	66	52977 → 59241 [SYN] Seq=3899798494 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1
...	0.084215	195.208.113.245	192.168.0.104	TCP	66	59241 → 52977 [SYN, ACK] Seq=766262532 Ack=3899798495 Win=14600 Len=0 MSS=1460
...	0.084318	192.168.0.104	195.208.113.245	TCP	54	52977 → 59241 [ACK] Seq=3899798495 Ack=766262533 Win=4194304 Len=0

Рис. 1.6: Набор пакетов, при установлении соединения(поток данных) в пассивном режиме

Активный режим

Подключение будет происходить согласно приведенной на рисунке 1.7 схеме. В качестве ftp-сервера был также выбран **ftp.neva.ru**, но для того чтобы подключение было именно в активном режиме в программе клиенте **FileZilla** были внесены соответствующие настройки.

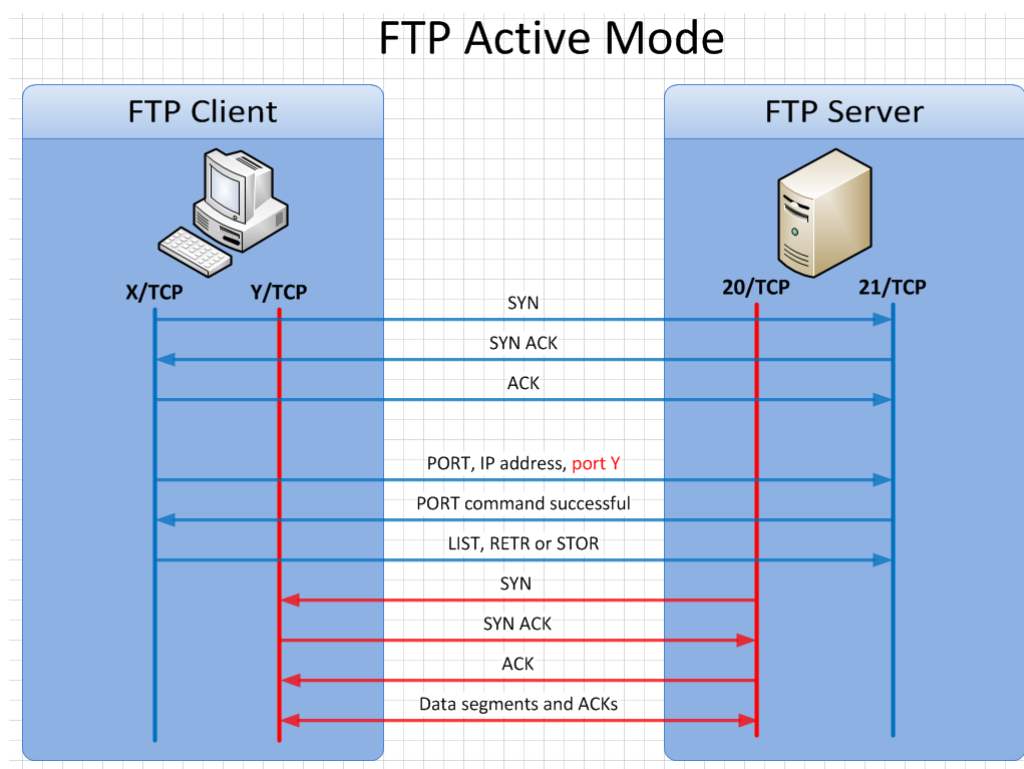


Рис. 1.7: Схема взаимодействия клиента и сервера при активном режиме

От произвольного порта клиента, создается управляющее tcp-соединения к 21 порту сервера. Пакеты которого приведены на рисунке 1.8.

No.	Time	Source	Destination	Protocol	Length	Info
3	1.674659	192.168.0.104	195.208.113.245	TCP	66	53425 → 21 [SYN] Seq=10084695 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	1.679572	195.208.113.245	192.168.0.104	TCP	66	21 → 53425 [SYN, ACK] Seq=3472245473 Ack=10084696 Win=14600 Len=0 MSS=1460
5	1.679655	192.168.0.104	195.208.113.245	TCP	54	53425 → 21 [ACK] Seq=10084696 Ack=3472245474 Win=16384 Len=0

Рис. 1.8: Пакеты для создания управляющего tcp-соединения

Теперь клиент сам указывает адрес и порт для подключения при помощи команды **PORT**. Адрес и порт передаются в виде (h1,h2,h3,h4,p1,p2).

No.	Time	Source	Destination	Protocol	Length	Info
...	1.733724	192.168.0.104	195.208.113.245	FTP	82	Request: PORT 192,168,0,104,208,178
> Frame 20: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0 > Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6) > Internet Protocol Version 4, Src: 192.168.0.104, Dst: 195.208.113.245 > Transmission Control Protocol, Src Port: 53425, Dst Port: 21, Seq: 10084766, Ack: 3472245776, Len: 28						
Source Port: 53425 Destination Port: 21 [Stream index: 1] [TCP Segment Len: 28] Sequence number: 10084766 [Next sequence number: 10084794] Acknowledgment number: 3472245776 Header Length: 20 bytes > Flags: 0x018 (PSH, ACK) Window size value: 63 [Calculated window size: 16128] [Window size scaling factor: 256] Checksum: 0x3eb2 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 > [SEQ/ACK analysis]						
> File Transfer Protocol (FTP) > PORT 192,168,0,104,208,178\r\n Request command: PORT Request arg: 192,168,0,104,208,178 Active IP address: 192.168.0.104 Active port: 53426						

Рис. 1.9: Координаты для активного режима

В случае успеха, сервер посылает соответствующий пакет об успешном выполнении команды PORT.

No.	Time	Source	Destination	Protocol	Length	Info
...	1.739123	195.208.113.245	192.168.0.104	FTP	83	Response: 200 PORT command successful
> Frame 21: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0 > Ethernet II, Src: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6), Dst: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd) > Internet Protocol Version 4, Src: 195.208.113.245, Dst: 192.168.0.104 > Transmission Control Protocol, Src Port: 21, Dst Port: 53425, Seq: 3472245776, Ack: 10084794, Len: 29						
Source Port: 21 Destination Port: 53425 [Stream index: 1] [TCP Segment Len: 29] Sequence number: 3472245776 [Next sequence number: 3472245805] Acknowledgment number: 10084794 Header Length: 20 bytes > Flags: 0x018 (PSH, ACK) Window size value: 29 [Calculated window size: 14848] [Window size scaling factor: 512] Checksum: 0x38de [unverified] [Checksum Status: Unverified] Urgent pointer: 0 > [SEQ/ACK analysis]						
> File Transfer Protocol (FTP) > 200 PORT command successful\r\n Response code: Command okay (200) Response arg: PORT command successful						

Рис. 1.10: Пакет с ответом об успешном выполнении команды PORT

Далее сервер устанавливает соединение на ранее высланный клиентом адрес и порт.

No.	Time	Source	Destination	Protocol	Length	Info
...	1.747404	195.208.113.245	192.168.0.104	TCP	74	20 → 53426 [SYN] Seq=2309645482 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=4181604155 TSecr=0 WS=
...	1.747497	192.168.0.104	195.208.113.245	TCP	74	53426 → 20 [SYN, ACK] Seq=3647981253 Ack=2309645483 Win=65535 Len=0 MSS=1460 WS=128 SACK_PERM=1 T
...	1.753948	195.208.113.245	192.168.0.104	TCP	66	20 → 53426 [ACK] Seq=2309645483 Ack=3647981254 Win=14848 Len=0 TSval=4181604163 TSecr=1038004791

Рис. 1.11: Набор пакетов, при установлении соединения(поток данных) в активном режиме

Безопасность

FTP-аутентификация использует схему имя пользователя/пароль для предоставления доступа. Имя пользователя посылается серверу командой **USER**, а пароль – командой **PASS**. Если предоставленная клиентом информация принята сервером, то сервер отправит клиенту приглашение и начинается сессия.

В случае если пользователь не вводит логин и пароль, то если сервер поддерживает эту особенность, можно войти в систему без предоставления учётных данных. Но на самом деле логин и пароль все таки предоставляются серверу. Логин в данном случае является **anonymous**. Пароль может быть любым, сервер скорее всего не будет проверять его.

No.	Time	Source	Destination	Protocol	Length	Info
...	2.531626	192.168.0.104	195.208.113.245	FTP	70	Request: USER anonymous
> Frame 34: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0 > Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6) > Internet Protocol Version 4, Src: 192.168.0.104, Dst: 195.208.113.245 > Transmission Control Protocol, Src Port: 53575, Dst Port: 21, Seq: 1226796778, Ack: 1820591233, Len: 16 Source Port: 53575 Destination Port: 21 [Stream index: 9] [TCP Segment Len: 16] Sequence number: 1226796778 [Next sequence number: 1226796794] Acknowledgment number: 1820591233 Header Length: 20 bytes > Flags: 0x018 (PSH, ACK) Window size value: 64 [Calculated window size: 16384] [Window size scaling factor: 256] Checksum: 0x365e [unverified] [Checksum Status: Unverified] Urgent pointer: 0 > [SEQ/ACK analysis] > File Transfer Protocol (FTP) > USER anonymous\r\n Request command: USER Request arg: anonymous						

Рис. 1.12: Пакет с логином для подключения

Передаваемый логин не был как либо зашифрован.

No.	Time	Source	Destination	Protocol	Length	Info
...	2.535964	195.208.113.245	192.168.0.104	FTP	129	Response: 331 Anonymous login ok, send your complete email address as your password
...	2.536201	192.168.0.104	195.208.113.245	FTP	71	Request: PASS tipo_parol
...	2.542161	195.208.113.245	192.168.0.104	FTP	104	Response: 230 Anonymous access granted, restrictions apply
> Frame 35: 129 bytes on wire (1032 bits), 129 bytes captured (1032 bits) on interface 0 > Ethernet II, Src: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6), Dst: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd) > Internet Protocol Version 4, Src: 195.208.113.245, Dst: 192.168.0.104 > Transmission Control Protocol, Src Port: 21, Dst Port: 53575, Seq: 1820591233, Ack: 1226796794, Len: 75 Source Port: 21 Destination Port: 53575 [Stream index: 9] [TCP Segment Len: 75] Sequence number: 1820591233 [Next sequence number: 1820591308] Acknowledgment number: 1226796794 Header Length: 20 bytes > Flags: 0x018 (PSH, ACK) Window size value: 29 [Calculated window size: 14848] [Window size scaling factor: 512] Checksum: 0x22c7 [unverified] [Checksum Status: Unverified] Urgent pointer: 0 > [SEQ/ACK analysis] > File Transfer Protocol (FTP) > 331 Anonymous login ok, send your complete email address as your password\r\n Response code: User name okay, need password (331) Response arg: Anonymous login ok, send your complete email address as your password						

Рис. 1.13: Ответ сервера на пакет с логином

В ответ, сервер прислал пакет с кодом 331, сообщая о корректности имени пользователя и о необходимости выслать пароль.

No.	Time	Source	Destination	Protocol	Length	Info
...	2.536201	192.168.0.104	195.208.113.245	FTP	71	Request: PASS tipo_parol
...	2.542161	195.208.113.245	192.168.0.104	FTP	104	Response: 230 Anonymous access granted, restrictions apply
...	2.547092	192.168.0.104	195.208.113.245	FTP	59	Request: PwD

```

> Frame 36: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 0
> Ethernet II, Src: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd), Dst: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6)
> Internet Protocol Version 4, Src: 192.168.0.104, Dst: 195.208.113.245
▼ Transmission Control Protocol, Src Port: 53575, Dst Port: 21, Seq: 1226796794, Ack: 1820591308, Len: 17
  Source Port: 53575
  Destination Port: 21
  [Stream index: 9]
  [TCP Segment Len: 17]
  Sequence number: 1226796794
  [Next sequence number: 1226796811]
  Acknowledgment number: 1820591308
  Header Length: 20 bytes
  > Flags: 0x018 (PSH, ACK)
  Window size value: 64
  [Calculated window size: 16384]
  [Window size scaling factor: 256]
  Checksum: 0xc827 [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > [SEQ/ACK analysis]
▼ File Transfer Protocol (FTP)
  ▼ PASS tipo_parol\r\n
    Request command: PASS
    Request arg: tipo_parol

```

Рис. 1.14: Пакет с паролем для подключения

В качестве пароля, в программе клиенте было введено **tipo_parol**. Пакет содержал пароль в не зашифрованном виде.

No.	Time	Source	Destination	Protocol	Length	Info
...	2.542161	195.208.113.245	192.168.0.104	FTP	104	Response: 230 Anonymous access granted, restrictions apply

```

> Frame 37: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0
> Ethernet II, Src: D-Link_3e:a6:d6 (f0:7d:68:3e:a6:d6), Dst: HonHaiPr_49:6d:bd (14:2d:27:49:6d:bd)
> Internet Protocol Version 4, Src: 195.208.113.245, Dst: 192.168.0.104
▼ Transmission Control Protocol, Src Port: 21, Dst Port: 53575, Seq: 1820591308, Ack: 1226796811, Len: 50
  Source Port: 21
  Destination Port: 53575
  [Stream index: 9]
  [TCP Segment Len: 50]
  Sequence number: 1820591308
  [Next sequence number: 1820591358]
  Acknowledgment number: 1226796811
  Header Length: 20 bytes
  > Flags: 0x018 (PSH, ACK)
  Window size value: 29
  [Calculated window size: 14848]
  [Window size scaling factor: 512]
  Checksum: 0xe5ae [unverified]
  [Checksum Status: Unverified]
  Urgent pointer: 0
  > [SEQ/ACK analysis]
▼ File Transfer Protocol (FTP)
  ▼ 230 Anonymous access granted, restrictions apply\r\n
    Response code: User logged in, proceed (230)
    Response arg: Anonymous access granted, restrictions apply

```

Рис. 1.15: Ответ сервера на пакет с паролем

В ответ, от сервера был получен пакет с кодом 230, сообщающий об успешной идентификации и возможности работать дальше.

1.5 Вывод

В данной лабораторной работе были рассмотрены режимы работы протокола ftp, а также его безопасность.

При работе с протоколом FTP создаются два соединения, первое для управления, а второе для передачи данных. Второе соединение определяет режим работы, он может быть активным или пассивным. Их отличие друг от друга является стороной которая выступает инициатором подключения для передачи данных и портами, на которые эта передача производится.

Пассивный режим является более безопасным для клиента. Так как если у пользователя настроен Firewall, то использование такого режима FTP может привести к возникновению ошибок, так как Firewall не позволит серверу подключиться к клиенту.

Протокол ftp не является безопасным, так как при его создании в 1971 году не было необходимости в защите данных. FTP не может зашифровать свой трафик, все передачи – открытый текст, имена пользователей, пароли, команды и данные могут быть прочитаны кем угодно, способным перехватить пакет по сети. Решением проблемы безопасности является использование защищенных вариаций FTP, таких как:

- **FTPS**
- **SFTP**