

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

Защита информации

Отчет по лабораторной работе №2

Исследование сетевого трафика

Работу выполнил:
Раскин Андрей
Группа: 43501/3
Преподаватель:
Новопашенный Андрей Гелиевич

Санкт-Петербург
2017

1 Цель работы

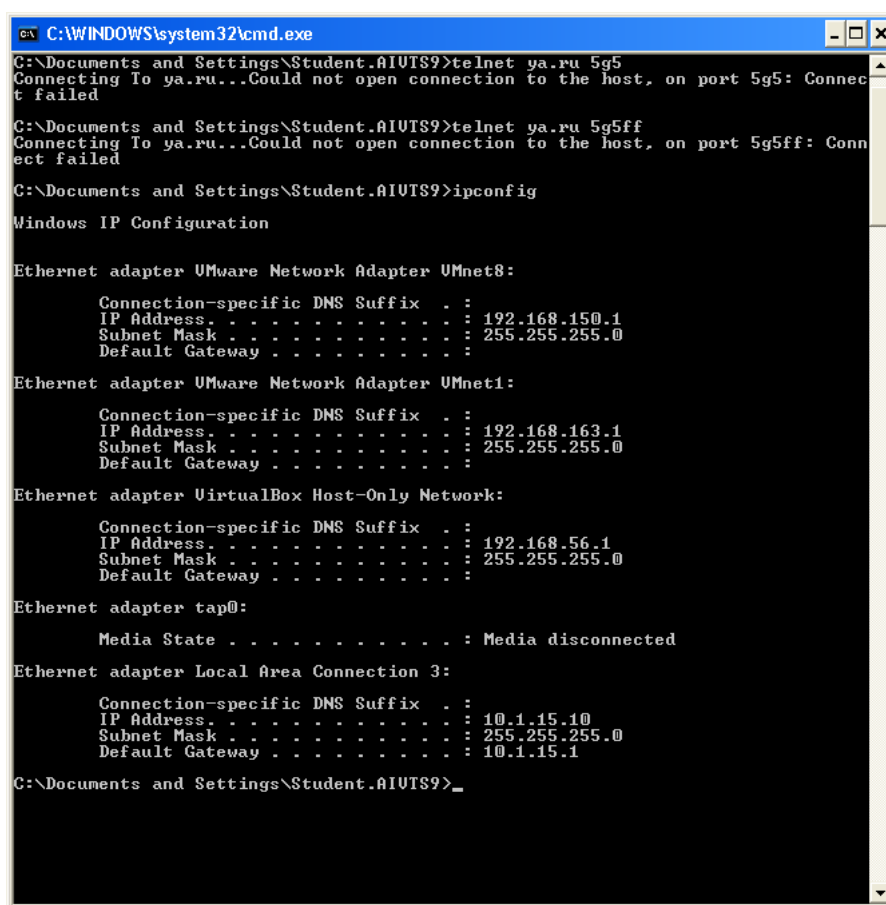
Закрепление навыков работы в программе Wireshark и знаний о некоторых сетевых протоколах.

2 Программа работы

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

1. пассивный режим,
2. активный режим,
3. безопасность протокола.

3 Конфигурация компьютера в сети



```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Student.AIUTS9>telnet ya.ru 5g5
Connecting To ya.ru...Could not open connection to the host, on port 5g5: Connection failed
C:\Documents and Settings\Student.AIUTS9>telnet ya.ru 5g5ff
Connecting To ya.ru...Could not open connection to the host, on port 5g5ff: Connection failed
C:\Documents and Settings\Student.AIUTS9>ipconfig

Windows IP Configuration

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.150.1
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.163.1
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 192.168.56.1
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 

Ethernet adapter tap0:

    Media State . . . . .             : Media disconnected

Ethernet adapter Local Area Connection 3:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 10.1.15.10
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 10.1.15.1

C:\Documents and Settings\Student.AIUTS9>
```

Рис. 1: Конфигурация сети

4 Ход работы

4.1 Протокол FTP

Имеется два режима – активный и пассивный. В первом случае клиент создает управляющее соединение и ждет, когда сервер запустит TCP-соединение с заданными адресом и номером порта. В пассивном режиме, когда клиент не может принять входящее TCP-соединение, клиент отправляет серверу команду PASV, получает от сервера его IP-адрес и номер порта, которые затем использует для открытия потока данных с произвольного клиентского порта к полученным адресу и порту сервера.

4.2 Пассивный режим



Рис. 2: Схема работы протокола ftp в пассивном режиме

Клиент запрашивает у сервера переход в пассивный режим командой PASV, перед этим подключившись к серверу по TCP через 21й порт и авторизовавшись.

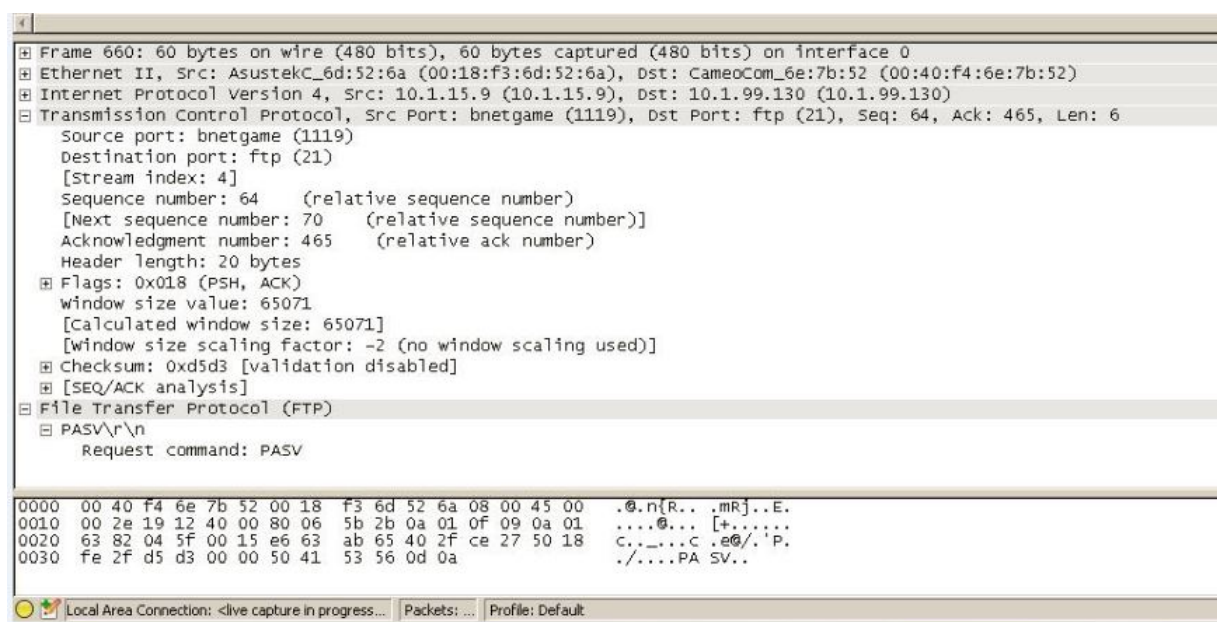


Рис. 3: Запрос от клиента на установку соединения

В ответ на команду PASV сервер передает клиенту IP адрес и 2 числа, из которых вычисляется номер порта для подключения к серверу.

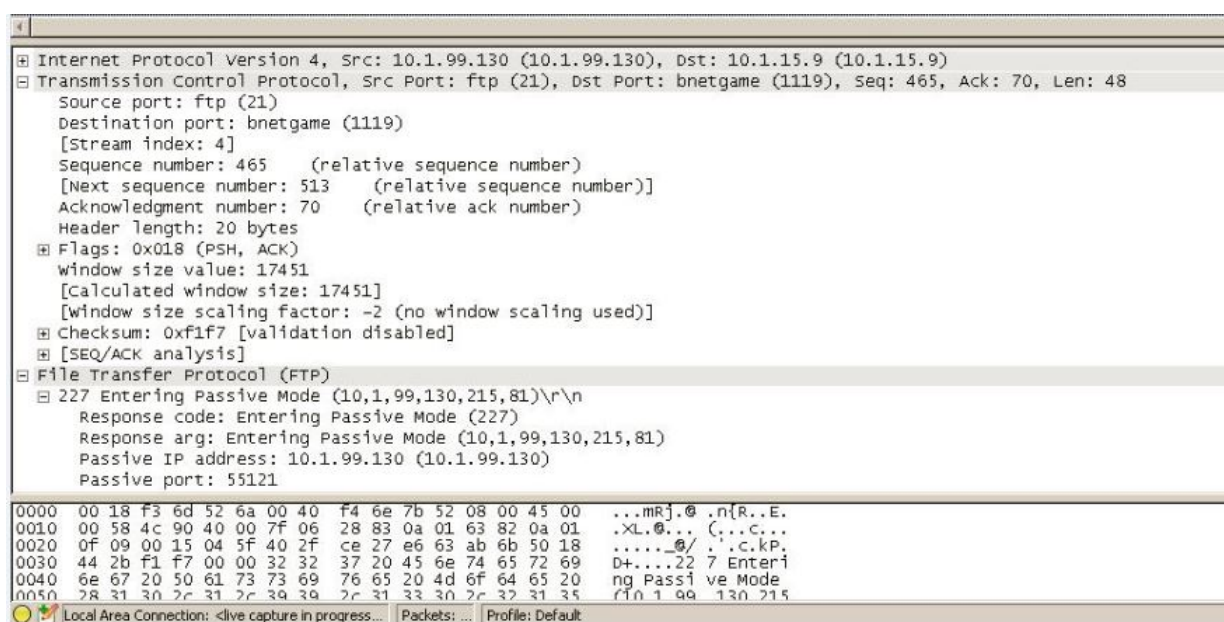


Рис. 4: Ответ сервера на команду PASV

Затем осуществляется подключение по данным IP адресу и номеру порта.

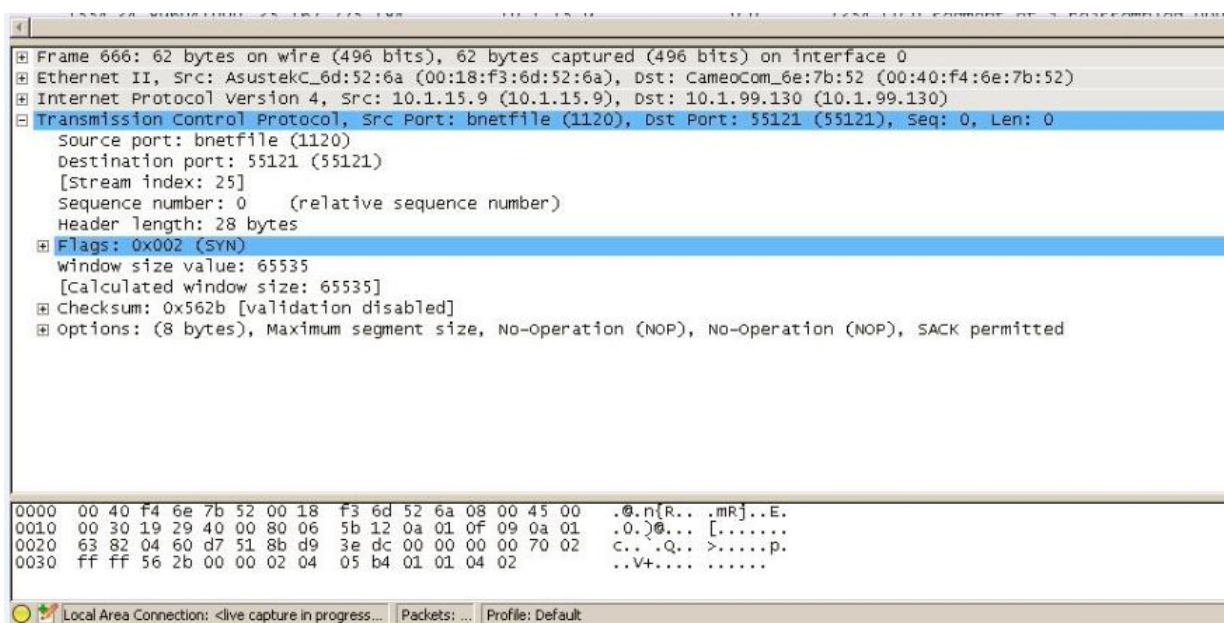


Рис. 5: Запрос на установку TCP-соединения

Рассмотрим пример передачи файла в пассивном режиме. Для этого существует команда RETR файл. Команды RETR, STOR и LIST можно прервать в процессе выполнения с помощью команды ABOR, в ответ на которую сервер должен ответить 426 «передача прервана», а затем — 226 «отмена операции произошла успешно».

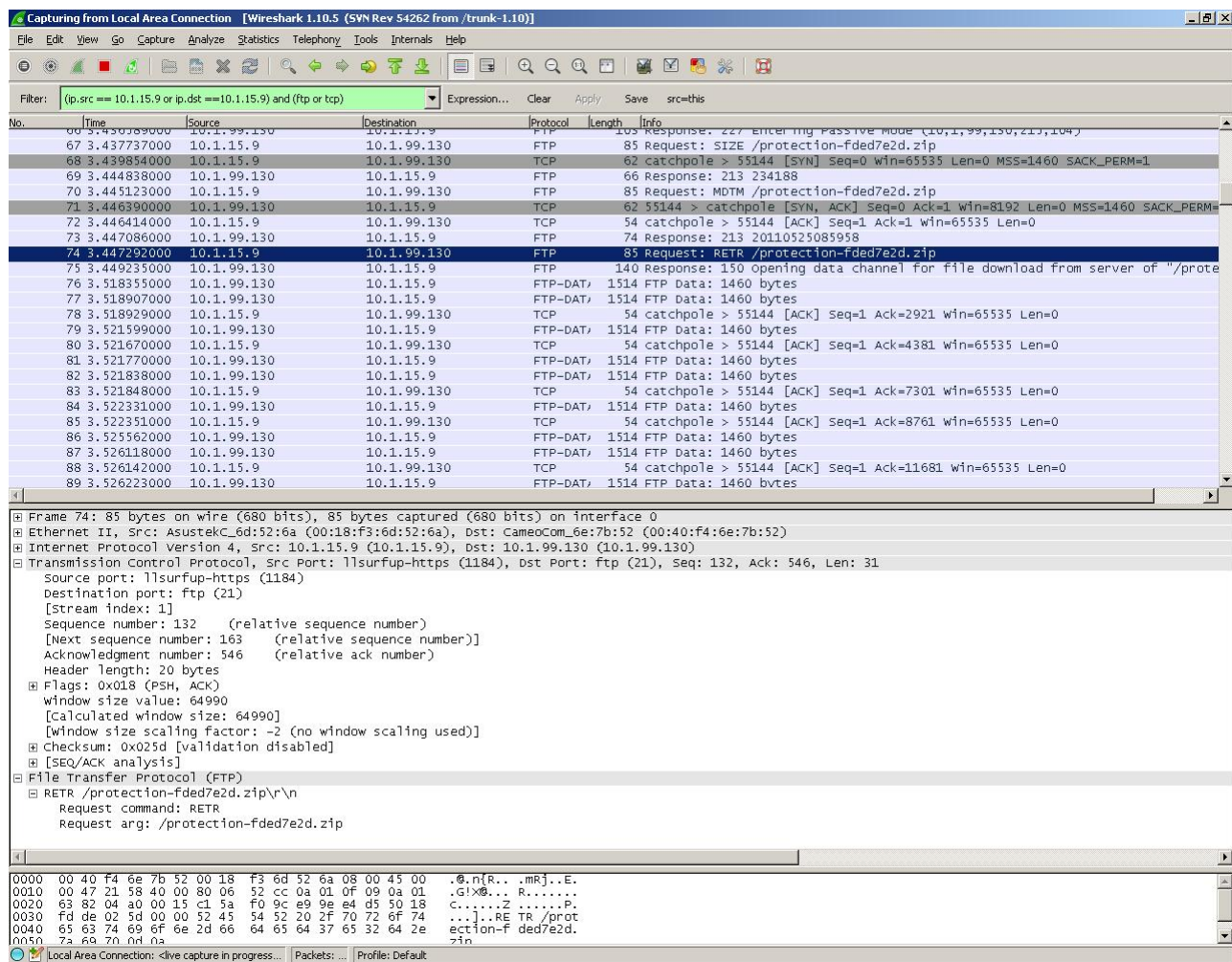


Рис. 6: Запрос на скачивание файла

Capturing from Local Area Connection [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: (ip.src == 10.1.15.9 or ip.dst == 10.1.15.9) and (ftp or tcp) Expression... Clear Apply Save src=this

No.	Time	Source	Destination	Protocol	Length	Info
331	3.608911000	10.1.99.130	10.1.15.9	FTP-DAT	1514	FTP Data: 1460 bytes
332	3.608977000	10.1.99.130	10.1.15.9	FTP-DAT	1514	FTP Data: 1460 bytes
333	3.608987000	10.1.15.9	10.1.99.130	TCP	54	catchpole > 55144 [ACK] Seq=1 Ack=225809 win=65535 Len=0
334	3.609150000	10.1.99.130	10.1.15.9	FTP-DAT	1514	FTP Data: 1460 bytes
335	3.609167000	10.1.15.9	10.1.99.130	TCP	54	catchpole > 55144 [ACK] Seq=1 Ack=227269 win=65535 Len=0
336	3.609632000	10.1.99.130	10.1.15.9	FTP-DAT	1514	FTP Data: 1460 bytes
337	3.609694000	10.1.99.130	10.1.15.9	FTP-DAT	702	FTP Data: 648 bytes
338	3.609715000	10.1.15.9	10.1.99.130	TCP	54	catchpole > 55144 [ACK] Seq=1 Ack=229377 win=65535 Len=0
339	3.613667000	10.1.99.130	10.1.15.9	FTP-DAT	1514	FTP Data: 1460 bytes
340	3.613773000	10.1.99.130	10.1.15.9	FTP-DAT	1514	FTP Data: 1460 bytes
341	3.613797000	10.1.15.9	10.1.99.130	TCP	54	catchpole > 55144 [ACK] Seq=1 Ack=232297 win=65535 Len=0
342	3.614392000	10.1.99.130	10.1.15.9	FTP-DAT	1514	FTP Data: 1460 bytes
343	3.614447000	10.1.15.9	10.1.99.130	TCP	54	catchpole > 55144 [ACK] Seq=1 Ack=233757 win=65535 Len=0
344	3.614516000	10.1.99.130	10.1.15.9	FTP-DAT	486	FTP data: 432 bytes
345	3.614551000	10.1.99.130	10.1.15.9	TCP	60	55144 > catchpole [FIN, ACK] Seq=234189 Ack=1 win=17520 Len=0
346	3.614564000	10.1.15.9	10.1.99.130	TCP	54	catchpole > 55144 [ACK] Seq=1 Ack=234190 win=65103 Len=0
347	3.614613000	10.1.99.130	10.1.15.9	FTP	111	Response: 226 Successfully transferred "/protection-fded7e2d.zip"
348	3.614624000	10.1.15.9	10.1.99.130	TCP	54	llsurfup-https > ftp [ACK] Seq=163 Ack=689 win=64847 Len=0
349	3.615068000	10.1.15.9	10.1.99.130	TCP	54	catchpole > 55144 [FIN, ACK] Seq=1 Ack=234190 win=65103 Len=0
350	3.617387000	10.1.99.130	10.1.15.9	TCP	60	55144 > catchpole [ACK] Seq=234190 Ack=2 win=17520 Len=0
1189	123.751488000	10.1.99.130	10.1.15.9	FTP	81	Response: 421 Connection timed out.
1190	123.752003000	10.1.99.130	10.1.15.9	TCP	60	ftp > llsurfup-https [FIN, ACK] Seq=716 Ack=163 win=17358 Len=0
1193	123.752448000	10.1.15.9	10.1.99.130	TCP	54	llsurfup-https > ftp [ACK] Seq=163 Ack=717 win=64820 Len=0

Frame 347: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface 0
 Ethernet II, Src: CameoCom_6e:f4:6e:7b:52 (00:40:f4:6e:7b:52), Dst: AsustekC_6d:52:6a (00:18:f3:6d:52:6a)
 Internet Protocol Version 4, Src: 10.1.99.130 (10.1.99.130), Dst: 10.1.15.9 (10.1.15.9)
 Transmission Control Protocol, Src Port: ftp (21), Dst Port: llsurfup-https (1184), Seq: 632, Ack: 163, Len: 57
 Source port: ftp (21)
 Destination port: llsurfup-https (1184)
 [Stream index: 1]
 Sequence number: 632 (relative sequence number)
 [Next sequence number: 689 (relative sequence number)]
 Acknowledgment number: 163 (relative ack number)
 Header length: 20 bytes
 Flags: 0x018 (PSH, ACK)
 Window size value: 17358
 [Calculated window size: 17358]
 Window size scaling factor: -2 (no window scaling used)
 Checksum: 0xdb2f (validation disabled)
 [SEQ/ACK analysis]
 File Transfer Protocol (FTP)
 226 Successfully transferred "/protection-fded7e2d.zip"\r\n
 Response code: Closing data connection (226)
 Response arg: Successfully transferred "/protection-fded7e2d.zip"

0000 00 18 f3 6d 52 6a 00 40 f4 6e 7b 52 08 00 45 00 ...mR].@.n{R..E.
 0010 00 61 4f 62 40 00 7f 06 25 a8 0a 01 63 82 0a 01 .aob@...%.c...
 0020 0f 09 00 15 04 a0 e9 9e e5 2b c1 5a f0 bb 50 18+.Z..P.
 0030 43 ce db 2f 00 00 32 32 36 20 53 75 63 63 65 73 C./..22 6 Succes
 0040 73 66 75 6c 6c 79 20 74 72 61 6e 73 66 65 72 72 sfully t ransferr
 0050 65 a4 20 72 2f 70 72 6f 74 65 63 74 69 6f 6e 2d ed "/protection-

Local Area Connection: -live capture in progress... Packets: ... Profile: Default

Рис. 7: Подтверждение получения файла

4.3 Активный режим



Рис. 8: Схема работы протокола ftp в активном режиме

Запрос на соединение от клиента. Содержит IP-адрес для подключения и два числа, из которых

находится номер порта.

```
⊕ Frame 1879: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
⊕ Ethernet II, Src: IntelCor_9d:6b:3d (4c:eb:42:9d:6b:3d), Dst: D-LinkIn_7c:58:30 (c8:be:19:7c:58:30)
⊕ Internet Protocol Version 4, Src: 192.168.1.3 (192.168.1.3), Dst: 195.208.113.245 (195.208.113.245)
⊖ Transmission Control Protocol, Src Port: 61828 (61828), Dst Port: 21 (21), Seq: 63, Ack: 230, Len: 25
  Source Port: 61828 (61828)
  Destination Port: 21 (21)
  [Stream index: 3]
  [TCP Segment Len: 25]
  Sequence number: 63 (relative sequence number)
  [Next sequence number: 88 (relative sequence number)]
  Acknowledgment number: 230 (relative ack number)
  Header Length: 20 bytes
  ⊕ .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
  window size value: 8134
  [Calculated window size: 32536]
  [window size scaling factor: 4]
  ⊕ Checksum: 0x2b21 [validation disabled]
  Urgent pointer: 0
  ⊕ [SEQ/ACK analysis]
⊖ File Transfer Protocol (FTP)
  ⊖ PORT 192,168,1,3,242,72\r\n
    Request command: PORT
    Request arg: 192,168,1,3,242,72
    Active IP address: 192.168.1.3 (192.168.1.3)
    Active port: 62024
```

Рис. 9: Пакет, содержащий команду PORT

```
⊕ Frame 1881: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
⊕ Ethernet II, Src: D-LinkIn_7c:58:30 (c8:be:19:7c:58:30), Dst: IntelCor_9d:6b:3d (4c:eb:42:9d:6b:3d)
⊕ Internet Protocol Version 4, Src: 195.208.113.245 (195.208.113.245), Dst: 192.168.1.3 (192.168.1.3)
⊖ Transmission Control Protocol, Src Port: 21 (21), Dst Port: 61828 (61828), Seq: 230, Ack: 88, Len: 29
  Source Port: 21 (21)
  Destination Port: 61828 (61828)
  [Stream index: 3]
  [TCP Segment Len: 29]
  Sequence number: 230 (relative sequence number)
  [Next sequence number: 259 (relative sequence number)]
  Acknowledgment number: 88 (relative ack number)
  Header Length: 20 bytes
  ⊕ .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
  window size value: 29
  [Calculated window size: 14848]
  [window size scaling factor: 512]
  ⊕ Checksum: 0x106e [validation disabled]
  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. 10: Ответ об успешном выполнении команды


```

+ Frame 1882: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
+ Ethernet II, Src: IntelCor_9d:6b:3d (4c:eb:42:9d:6b:3d), Dst: D-LinkIn_7c:58:30 (c8:be:19:7c:58:30)
+ Internet Protocol Version 4, Src: 192.168.1.3 (192.168.1.3), Dst: 195.208.113.245 (195.208.113.245)
- Transmission Control Protocol, Src Port: 61828 (61828), Dst Port: 21 (21), Seq: 88, Ack: 259, Len: 6
  Source Port: 61828 (61828)
  Destination Port: 21 (21)
  [Stream index: 3]
  [TCP Segment Len: 6]
  Sequence number: 88 (relative sequence number)
  [Next sequence number: 94 (relative sequence number)]
  Acknowledgment number: 259 (relative ack number)
  Header Length: 20 bytes
  .... 0000 0001 1000 = Flags: 0x018 (PSH, ACK)
  window size value: 8127
  [calculated window size: 32508]
  [window size scaling factor: 4]
+ Checksum: 0xfbd7 [validation disabled]
  urgent pointer: 0
+ [SEQ/ACK analysis]
- File Transfer Protocol (FTP)
  NLST\r\n
  Request command: NLST

```

Рис. 11: Запрос списка файлов

Далее осуществляется соединение по заданным IP и номеру порта. Запрос на соединения отправляет сервер.

```

+ Frame 1884: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
+ Ethernet II, Src: D-LinkIn_7c:58:30 (c8:be:19:7c:58:30), Dst: IntelCor_9d:6b:3d (4c:eb:42:9d:6b:3d)
+ Internet Protocol Version 4, Src: 195.208.113.245 (195.208.113.245), Dst: 192.168.1.3 (192.168.1.3)
- Transmission Control Protocol, Src Port: 20 (20), Dst Port: 62024 (62024), Seq: 0, Len: 0
  Source Port: 20 (20)
  Destination Port: 62024 (62024)
  [Stream index: 42]
  [TCP Segment Len: 0]
  Sequence number: 0 (relative sequence number)
  Acknowledgment number: 0
  Header Length: 40 bytes
+ .... 0000 0000 0010 = Flags: 0x002 (SYN)
  window size value: 14600
  [calculated window size: 14600]
+ Checksum: 0x98da [validation disabled]
  urgent pointer: 0
+ Options: (20 bytes), Maximum segment size, SACK permitted, Timestamps, No-Operation (NOP), window scale

```

Рис. 12: Запрос на соединение от сервера

```

+ Frame 1887: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
+ Ethernet II, Src: D-LinkIn_7c:58:30 (c8:be:19:7c:58:30), Dst: IntelCor_9d:6b:3d (4c:eb:42:9d:6b:3d)
+ Internet Protocol Version 4, Src: 195.208.113.245 (195.208.113.245), Dst: 192.168.1.3 (192.168.1.3)
- Transmission Control Protocol, Src Port: 20 (20), Dst Port: 62024 (62024), Seq: 1, Ack: 1, Len: 0
  Source Port: 20 (20)
  Destination Port: 62024 (62024)
  [Stream index: 42]
  [TCP Segment Len: 0]
  Sequence number: 1 (relative sequence number)
  Acknowledgment number: 1 (relative ack number)
  Header Length: 32 bytes
+ .... 0000 0001 0000 = Flags: 0x010 (ACK)
  window size value: 29
  [calculated window size: 14848]
  [window size scaling factor: 512]
+ Checksum: 0x90a7 [validation disabled]
  urgent pointer: 0
+ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
+ [SEQ/ACK analysis]

```

Рис. 13: Подтверждение установки соединения

4.4 Безопасность протокола

FTP-аутентификация, как правило, применяет обычную схему имя пользователя/пароль для предоставления доступа. Имя пользователя посылается серверу в виде команды USER, а пароль - в виде команды PASS. Если предоставленная клиентом информация принята сервером, то сервер отправит клиенту приглашение и начнется сессия. Также, пользователи могут, если сервер позволяет, войти в систему без предоставления учетных данных, но сервером предоставляется лишь ограниченный доступ для таких сессий.

Но также хост FTP-сервиса может предоставить анонимный доступ к FTP. Пользователи обычно входят в систему анонимно, в качестве имени пользователя используется «anonymous». Как правило, пользователей просят прислать адрес электронной почты вместо пароля, никакой тщательной проверки не производится. Многие FTP-хосты, предоставляющие обновления программного обеспечения, поддерживают анонимный доступ.

```
> Frame 34: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: CameoCom_6e:7b:52 (00:40:f4:6e:7b:52), Dst: AsustekC_6d:52:6a (00:18:f3:6d:52:6a)
> Internet Protocol Version 4, Src: 195.208.113.245 (195.208.113.245), Dst: 10.1.15.9 (10.1.15.9)
▼ 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. 14: Пакет с логином для подключения

В ответ, сервер прислал пакет с кодом 331.

```

> Frame 34: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
> Ethernet II, Src: CameoCom_6e:7b:52 (00:40:f4:6e:7b:52), Dst: AsustekC_6d:52:6a (00:18:f3:6d:52:6a)
> Internet Protocol Version 4, Src: 195.208.113.245 (195.208.113.245), Dst: 10.1.15.9 (10.1.15.9)
v 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: 1820591233]
    Acknowledgment number: 1226796794
    Header Length: 20 bytes
> Flags: 0x018 (PSH, ACK)
    Window size value: 25
    [Calculated window size: 16384]
    [Window size scaling factor: 256]
    Checksum: 0x365e [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
> [SEQ/ACK analysis]
v File Transfer Protocol (FTP)
    v 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. 15: Ответ сервера на пакет с логином

Вводится пароль и клиент получает пакет с кодом 230, сообщающий об успешной идентификации и возможности работать дальше.

```

Ethernet II, Src: CameoCom_6e:7b:52 (00:40:f4:6e:7b:52), Dst: AsustekC_6d:52:6a (00:18:f3:6d:52:6a)
Internet Protocol Version 4, Src: 195.208.113.245 (195.208.113.245), Dst: 10.1.15.9 (10.1.15.9)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 90
    Identification: 0xb827 (47143)
    Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 59
    Protocol: TCP (6)
    Header checksum: 0x38a7 [correct]
    Source: 195.208.113.245 (195.208.113.245)
    Destination: 10.1.15.9 (10.1.15.9)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: ftp (21), Dst Port: remote-as (1053), Seq: 150, Ack: 24, Len: 50
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. 16: Ответ сервера на пакет с паролем

5 Выводы

В ходе работы были исследованы пакеты протокола FTP. FTP отличается от других приложений тем, что он использует два TCP соединения для передачи файла.

1. Управляющее соединение устанавливается как обычное соединение клиент-сервер. Сервер осуществляет пассивное открытие на заранее известный порт FTP (21) и ожидает запроса на соединение от клиента. Клиент осуществляет активное открытие на TCP порт 21, чтобы установить управляющее соединение. Управляющее соединение существует все время, пока клиент общается с сервером. Это соединение используется для передачи команд от клиента к серверу и для передачи откликов от сервера. Тип IP сервиса для управляющего соединения устанавливается для получения "минимальной задержки так как команды обычно вводятся пользователем.

2. Соединение данных открывается каждый раз, когда осуществляется передача файла между клиентом и сервером. (Оно также открывается и в другие моменты, как мы увидим позже.) Тип сервиса IP для соединения данных должен быть "максимальная пропускная способность так как это соединение используется для передачи файлов.

FTP не разрабатывался как защищённый (особенно по нынешним меркам) протокол и имеет многочисленные уязвимости в защите. FTP не может зашифровать свой трафик, все передачи — открытый текст, поэтому имена пользователей, пароли, команды и данные могут быть прочитаны кем угодно, способным перехватить пакет по сети.

Поэтому часто применяется SFTP — отдельный протокол, основанный на SSH. Его преимуществом является способность использовать защищенное соединение для передачи файлов и навигации по файловой системе на обеих системах — локальной и удаленной.