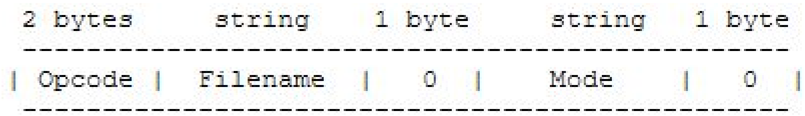
Jericho Perdon
Prof Scrivnor
Comp 429
4 Feb 2021

Lab 2

Tftp qanda

1) What is the syntax for a RRQ or WRQ packet in TFTP?

The syntax for a RRQ or WRQ packet in TFTP is that the file name is in a sequence of bytes terminating in a zerobyte.



```
 2 bytes     string    1 byte     string   1 byte
 ------------------------------------------------
| Opcode |  Filename  |   0  |    Mode    |   0  |
 ------------------------------------------------
```

2) Which bytes contain the opcode for the RRQ in frame number 1 in the L02-tftp.pcapng file?

The bytes that contain the opcode for the RRQ in frame number 1 in the L02-tftp.pcapng file are bytes 42 and 43.

3) What is the name of the file for the RRQ in frame number 1?

The name of the file for the RRQ in frame number 1 is Source File: rfc1350.txt.

4) What are the three supported modes for RRQ/WRQ in TFTP?

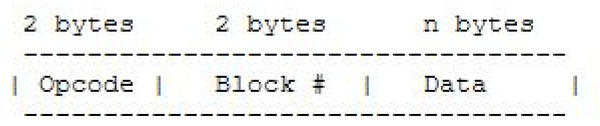
The three supported modes for RRQ/WRQ in TFTP are “netascii:, “octet”, or “mail”.

5) Which mode was used in the RRQ in frame number 1?

The mode used in the RRQ in frame number 1 is netascii.

6) What is the syntax for a DATA packet in TFTP?

The syntax for a DATA packet in TFTP is



```
 2 bytes     2 bytes      n bytes
 ----------------------------------
| Opcode |   Block #  |   Data     |
 ----------------------------------
```

7) Explain the purpose of `block` numbers according to the RFC.

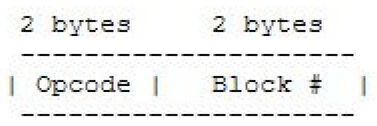
The purpose of block numbers is to allow the program to use a single number in order to discriminate between new packers and duplicates.

8) What would happen if a data block contained < 512 bytes?

If a data block contained less than 512 bytes, then it will signal the end of the transfer.

9) What is the syntax of an ACK packet in TFTP?

The syntax of an ACK packet in TFTP is



```
 2 bytes     2 bytes
 ---------------------
| Opcode |   Block #  |
 ---------------------
```

ACK packets are acknowledged packets that have the opcode 4 and contain the block number the block number that corresponds to the acknowledged DATA packet.

10) Write down the frame number of one DATA packet and its coinciding ACK packet from the file transfer.

The frame number of one DATA packet and its coinciding ACK packet from the file transfers are: Frame 6 DATA packet (3) and Frame 7 Acknowledgment (4).

11) There are two IP addresses in this transaction, which one is the server and which one is the client?

The client IP address is 192.168.19.1 and the server IP address is 192.168.19.99.

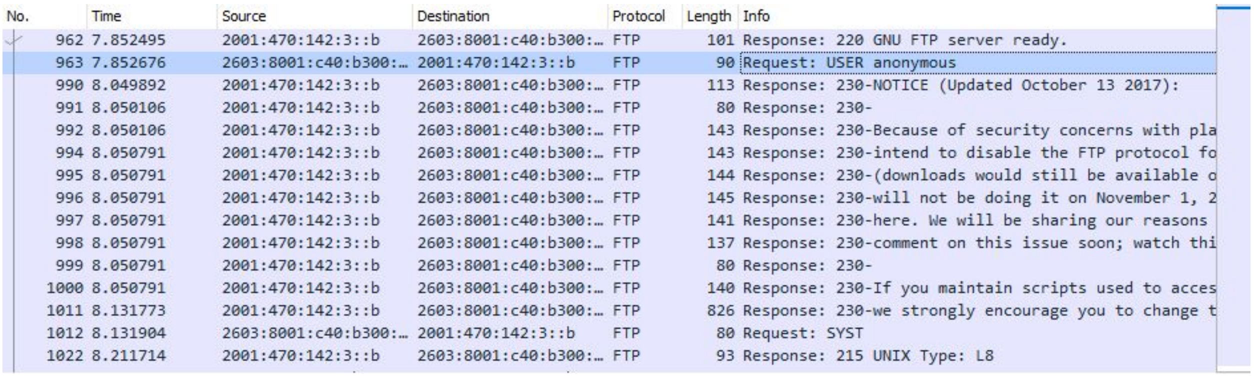
12) What port number is the server listening for a RRQ or WRQ on?

The port number that the server os listening for a RRQ or WRQ on is port 69.

Ftp qanda

2) What is the name of the user who logged into the FTP Server? Identify the request and responses using the frame number in your answer.

The name of the user who logged into the FTP server was “anonymous”. The frame number is 963.



No.	Time	Source	Destination	Protocol	Length	Info
962	7.852495	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	101	Response: 220 GNU FTP server ready.
963	7.852676	2603:8001:c40:b300:…	2001:470:142:3::b	FTP	90	Request: USER anonymous
990	8.049892	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	113	Response: 230-NOTICE (Updated October 13 2017):
991	8.050106	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	80	Response: 230-
992	8.050106	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	143	Response: 230-Because of security concerns with pla
994	8.050791	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	143	Response: 230-intend to disable the FTP protocol fo
995	8.050791	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	144	Response: 230-(downloads would still be available o
996	8.050791	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	145	Response: 230-will not be doing it on November 1, 2
997	8.050791	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	141	Response: 230-here. We will be sharing our reasons
998	8.050791	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	137	Response: 230-comment on this issue soon; watch thi
999	8.050791	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	80	Response: 230-
1000	8.050791	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	140	Response: 230-If you maintain scripts used to acces
1011	8.131773	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	826	Response: 230-we strongly encourage you to change t
1012	8.131904	2603:8001:c40:b300:…	2001:470:142:3::b	FTP	80	Request: SYST
1022	8.211714	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	93	Response: 215 UNIX Type: L8

3) What is the IP address of you (client) and the IP address of the server?

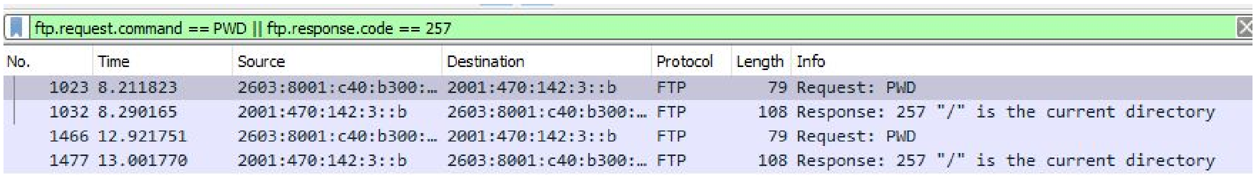
Since my wireshark client displayed the IP addresses in IPv6 form and not IPv4, I used the command “ipconfig” in command prompt to determine the IPv4 form of the client which was 192.168.0.35. The server IPv4 address is 209.51.188.20.

4) Find a "PWD" request command sent by the client. Use a Wireshark filter to isolate the packet.

- What is the Wireshark filter you used?
- What frame numbers contain PWD requests?
- What is the filter to display PWD requests OR (hint: `||`) ftp responses that contain code `257`.

Note: this filter should display the requests from the client and responses by the server.

The wireshark filter I used was “ftp.request.command == PWD || ftp.response.code == 257”. The frame numbers that contained the PWD requests are 1023 and 1466.



ftp.request.command == PWD || ftp.response.code == 257

No.	Time	Source	Destination	Protocol	Length	Info
1023	8.211823	2603:8001:c40:b300:…	2001:470:142:3::b	FTP	79	Request: PWD
1032	8.290165	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	108	Response: 257 "/" is the current directory
1466	12.921751	2603:8001:c40:b300:…	2001:470:142:3::b	FTP	79	Request: PWD
1477	13.001770	2001:470:142:3::b	2603:8001:c40:b300:…	FTP	108	Response: 257 "/" is the current directory

5) What is the purpose of requesting PASV mode? (Mentioned in the lecture).

The purpose of requesting PASV mode is to help the FTP client’s firewall in blocking incoming connections.

6) Filter to display only the "PASV" requests and responses.

- What filter did you use?
- Find the response for the CWD / command, what port number is opened for the data to flow? (Wireshark tells you which response is for which command)
- Find the response for the SIZE tree.json.gz file, what port number is opened for the data to flow?
- Use the filter `ftp-data` to view the data being transferred. This will confirm your answers from above.

a) ftp.request.command == PWD || ftp.response.code == 257
b) the response for CWD command is on port number 65108
c) the response for SIZE tree.json.gz file is on port number 26302