

Computer networks - 1DV701

Assignment 3

Author: Michael Johansson & Jakob
Heyder
Semester: VT 2017

Contents

1	Assignment summary	1
2	Problem one	2
3	Problem two	3
3.1	VG.1 wireshark analyze	4
4	Problem three	5

1 Assignment summary

- **Michael** Work percentage 50%
- **Jakob** Work percentage 50%

2 Problem one

In figure 2.1 we show a successful RRQ (Read-Request) to the implemented tftp server retrieving a small test-text file.

We use the original socket as a kind of server socket accepting the requests on port 4970 (Usually 69 in FTP) and then after receiving a request, either write or read, we open a new thread for the specific client connection. In this thread we use the sending socket which acquires a free port (zero port indicates to get a random free port e.g. 5800) and then send the new specified port to the client in the ACK (WRQ) or DATA (RRQ) packet. This is defined in the TFTP-Specification that the initialization will be on a predefined port and then the server communicates the used port to the client. This way we can also handle multiple client requests since the original socket is freed after handling the client in a separate thread. Also the send socket connects to the remote port and address of the client given from the request.

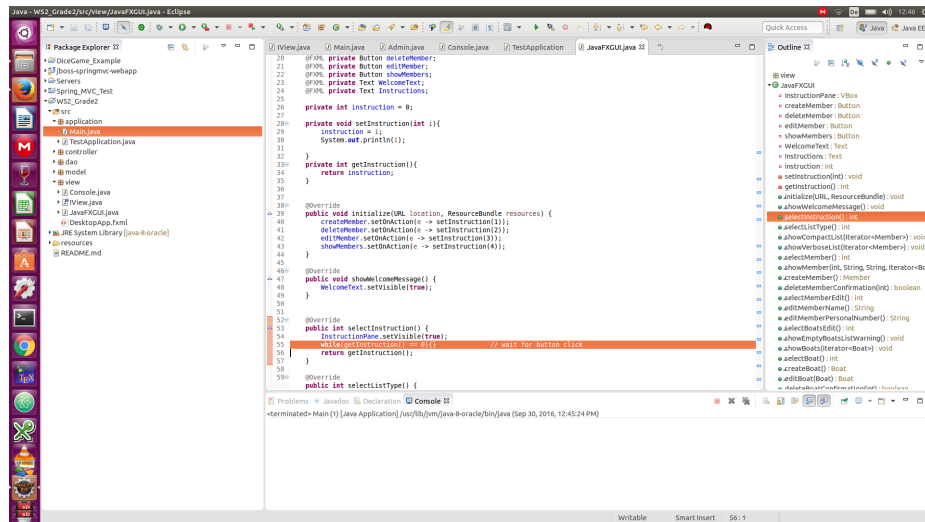


Figure 2.1: Successful READ-Request. We can see the tftp-client in the terminal window, eclipse tftp server and the home directory where the retrieved file is saved to.

3 Problem two

In figure 3.1 we send and receive multiple large files. The task says sending but it is not clear if it means sends from client or server. However both is on the screenshot with files larger then 512 bytes. The case of files which are so large that they exceed the package number of a short is thought of but not mentioned in the specification. Therefore its left out and assumed out of scope in this assignment.

We implemented a timeout mechanism that the sending socket times out if it does not receive the next DATA/ACK packet in 150ms. If it times out it will try to retransmit or simply tries to receive again. We have a re-transmission counter which will be increased and stops the execution after 5 retransmissions/waiting-times so that no infinite loop will occur.

The execution of a write-request can be seen also on figure 3.1.

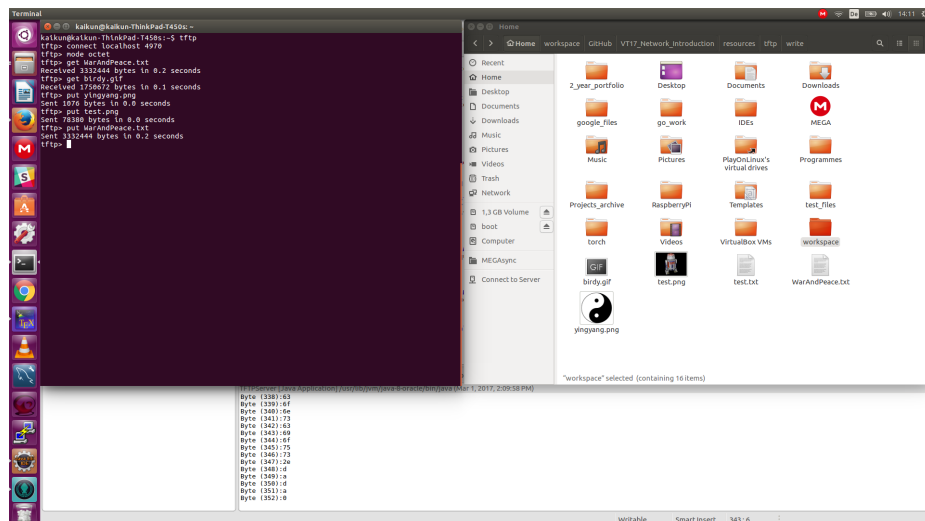


Figure 3.1: Read and write multiple large files. On the left hand side we see the tftp client transferring files from the home directory or reading files from the server. We can see the bytes transferred.

3.1 VG.1 wireshark analyze

In figure 3.2 we can see the line marked where the client, in this case with the localhost - 127.0.0.1 - src-address from the randomly choosen free port 53874 is sending a UDP Packet to the server. The server address is also localhost - 127.0.0.1 - dest-address and the port is the chosen 4970, which is usually 69 for the FTP protocols. In the bottom rows we can see the content of the package and beside all the headers of the lower layers the data of the UDP packet is marked. In the data we can see it start with the 2Bytes 00 01 which is defined in the TFTP-Specification as the operational code for a read request. The next bytes, in this case 8, until a zero byte are defined as the filename string. After the zero byte the mode will be defined by the following bytes closed with a zero byte again. In this case we can see that the OP-Code is RRQ, the filename of the requested file is test.txt and the mode is octet.

In figure 3.3 we can see the line marked where the server answers to the clients read request. We see that the destination and source address are again localhost, but would have switched. The switch we can identify on the ports, while the client port 53874 is now the receiving port the sending port from the server changed to 53964. This tells the client that this will be the port on the server side used for the rest of the file transmission. The initial port 4970 is only used to handle new requests. In the bottom rows we can see the data send back from the server. It starts with the 2Bytes 00 03 which is the OP-Code for DATA packages recording to the TFTP-Specification. The next two bytes 00 01 indicate the package number. In this case it is the first data package sent. It follows the actual file-data. In this case it is a text file and simply transfers the ASCII-Characters saved in it, "This is a test.".

In figure 3.4 we can see the line marked where the client sends an acknowledgement back to the server that it received the data package. We can see that the source and destination port flipped again and that the client now sends to the server port it received the data package from. The client sends only 4 Bytes data back. The first two indicating the OP-Code again in this case 00 04, meaning it is an acknowledgment packet and 2 more bytes 00 01 referencing the package number of the received packet which gets acknowledged. Due to the fact that the received data package was less than 516 bytes (512 inc. 4bytes header data) the client knows that the file is complete and with sending the ACK-Packet back the connection is terminated normally.

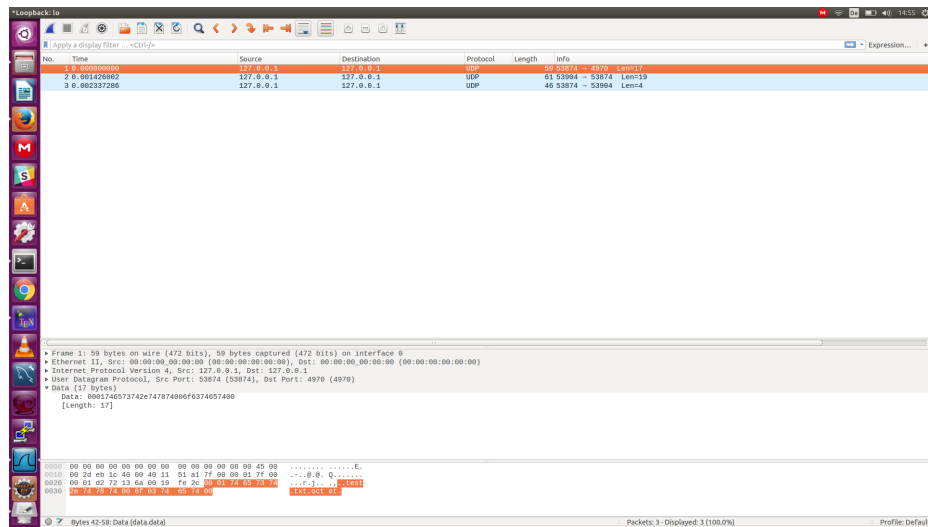


Figure 3.2: We see a screen of a read request in wireshark. The send data, which is a TFTP-RRQ is marked in the bottom rows.

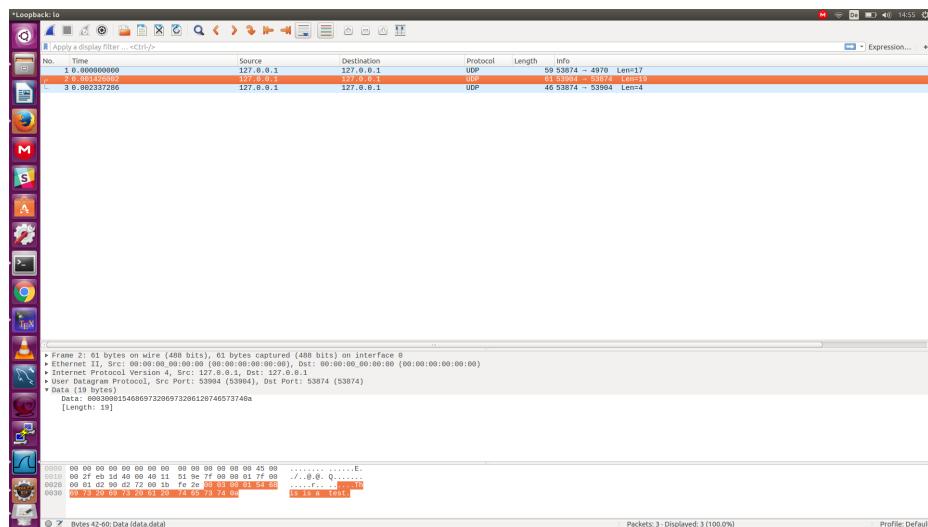


Figure 3.3: We see a screen of the answer from the TFTP-server to TFTP-RRQ in wireshark. The send data, which includes the file-data inc. TFTP-Header (DATA-OPCODE and packet number) is marked in the bottom rows.

4 Problem three

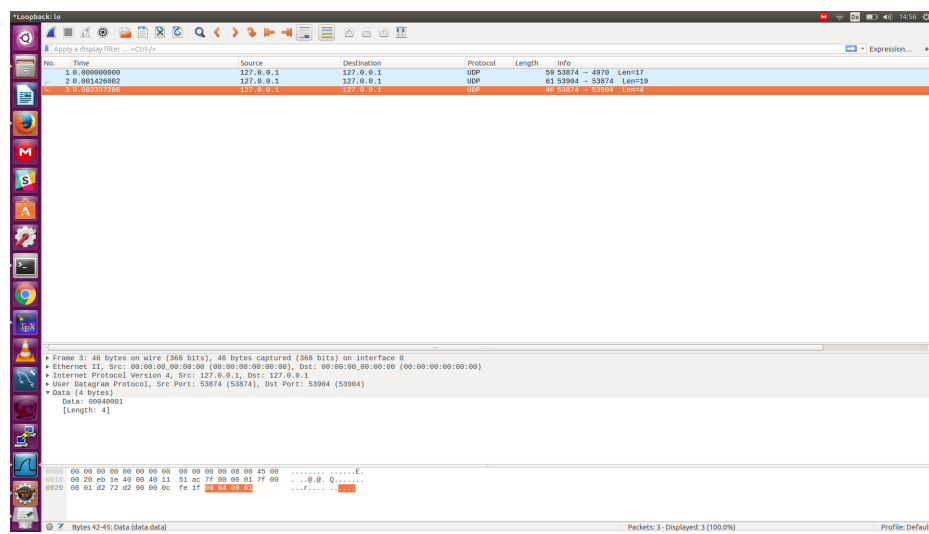


Figure 3.4: We see a screen of the acknowledgement of the TFTP-client to the received data file of the TFTP-Server. The data is again marked in the bottom rows.