Design Document 10/30/2023

RDT 2.0

Daniel Maccaline, Nathan Grady

Project Phase 3

**Phase purpose:**

The purpose of this phase is to implement RDT 2.2, with a system that is able to reliably transfer a file over a connection that does not drop packets, but can corrupt packets.

**Code explanation**

**Overview:**

Two Boolean control variables and three integer control variables are used to adjust the functionality of the code. The first three are found in functions.py, and are printFlag, corruptionPercent\_server\_to\_client and corruptionsPercent\_client\_to\_server. These printFlag Boolean controls if the debug output information is printed. The corruptionPertcent variables indicate the percent chance of corruption in each direction. Note that values entered here are in percentages corruptionPercent\_server\_to\_client = 60 is a 60% chance of corruption, or a probability of .6. Note that any time any of these are changed, the server must be restarted for them to take full effect

The remaining two values are found in Client.py, and are used to have the client send multiple files for testing the time taken. The flag runMultipleTests enables the client to re-send the file, and iterations is the number of times the file is sent. Once complete, the average time for each run is printed to the terminal. See the execution example below for example outputs.

**Client.py**

*"""  
TCP Client  
Authors: Daniel Maccaline and Nathan Grady  
 Based on code from phase 1 (Daniel Maccaline)  
"""*import socket  
import tkinter as tk  
from tkinter import filedialog  
from send\_receive import \*  
import datetime  
import time

Imports and Headers

def Get\_Packets\_Raw(file, packetsize):  
  
 currentIndex = 0  
  
 data = file.read()  
  
 #create packet list  
 packet = []  
  
 while(currentIndex < len(data)):  
  
 #extract just the data from the packet  
 bytesdata=data[currentIndex:currentIndex + packetsize]  
  
 packet.append(bytesdata)  
  
 currentIndex += packetsize  
  
 return packet

Get\_Packets\_Raw functions. Splits the file data into a list of equally sized packets, each of a length specified by packetsize. Note that no headers are applied at this point.

def UDPClient(fileName):  
  
 # packet size in bytes  
 packetSize = 1024  
  
 # read file in here  
 try:  
 file = open(fileName, "rb")  
 except:  
 print("File could not be opened...")  
 return  
  
 if file.closed:  
 print("File could not be opened")  
  
 #raw packets means just the packet with no header or anything yet  
 data = Get\_Packets\_Raw(file, packetSize)  
  
 file.close()  
 # endregion

Attempt file read from filename specified in argument. Note that the variable packetSize is also set at this point. Once opened, create packets using Get\_Packets\_Raw, then close the file.

# set server name and port to expect server at  
 serverName = 'localhost'  
 serverPort = 11000  
 # create UDP Socket  
 clientSocket = socket.socket(socket.AF\_INET, socket.SOCK\_DGRAM)

Create UDP Socket for connection to the server

#send packets one at a time  
 try:  
 print("sending ",len(data),"packets")  
 print("corruption rate from the client to the server is: ",corruptPercent\_client\_to\_server,"%")  
 print("corruption rate from the server to the client is: ",corruptPercent\_server\_to\_client,"%")  
 print()  
  
 start\_time = datetime.datetime.now()  
  
 for i in range (0,len(data)):  
 rdt\_send(clientSocket, serverName, serverPort, data[i])  
 if(printflag): print("sending packet number ",i)  
  
 #send stop bit  
 rdt\_send(clientSocket, serverName, serverPort, b'stop')  
  
 end\_time=datetime.datetime.now()  
 print()  
 print("finished sending")  
 print("start: ",start\_time," end:",end\_time)  
 time = end\_time-start\_time  
 print("total time: ",(end\_time-start\_time))  
  
 except:  
 print("ther server is probably down")

Ty to send the data to the server. First prints the messages indicating the loss chance, then records a start time. The function then loops over every packet in the data variable, and calls rdt\_send (function found in send\_recieve.py, discussed later), followed by a packet indicating to the server that the file transfer is complete. Then records an end time, and prints the statistics for the run.

If the try fails, then the server did not respond, and an error is printed.

clientSocket.close()  
 #Return time taken in microseconds and seconds  
 return time.microseconds, time.seconds

Close the socket connection, convert time to a microseconds and seconds value, and return the values to main

#Main, used to start TCPClient and send name of passed file  
if \_\_name\_\_ == "\_\_main\_\_":  
  
 #Variables used for automatic tests, Iterations -> Number of tests, runMultipleTests bool used to control if tests are done  
 iterations = 3  
 runMultipleTests = False  
  
 root = tk.Tk()  
 root.withdraw()  
  
 file\_path = filedialog.askopenfilename()  
  
 #check if input argument provided  
 if len(file\_path) <= 1:  
 #output error if no input file provided  
 print("Error: No input file specified")

Main function. Sets values for running multiple tests, and opens dialog box prompting the user for a filepath. Then checks if a filepath was selected.

else:  
  
 #if not running multiple, just call UDP client and disregard returns  
 if not runMultipleTests:  
 #pass input file name to client  
 UDPClient(file\_path)

This else statement is connected to the if statement in the previous set of code. If not running multiple tests, the code simply calls the UPDClient function with the filepath as an argument.

#Test  
 else:  
 #Store number of iterations for denominator of average calc  
 avgDen = iterations  
 #Stores time returned by function  
 timeR = 0  
 #iterate for (iterations) times  
 while(iterations > 0):  
 print("\n\n\nStarting run " + str(avgDen-iterations))  
 iterations = iterations - 1  
 #Function returns time spent in microseconds and seconds  
 micros, sec = UDPClient(file\_path)  
 #add time to timeR, dividing micros to adjust  
 timeR = timeR + micros/1000000 + sec  
 #sleep before next call (avg time goes up without this sleep)  
 time.sleep(1)  
 #print average results  
 print("Average results: ", str(timeR/avgDen))

This if is connected to the if in the previous code block. If running multiple tests, store the number of iterations, and set timeR to 0 to store the returned times. Then iterate in a loop for iterations times, storing the timed result of each run to timeR. Then print the average, by dividing timeR by avgDen.

**Server.py**

*"""  
TCP Server  
Authors: Daniel Maccaline and Nathan Grady  
 Based on code from phase 1 (Daniel Maccaline)  
"""*import socket  
from send\_receive import \*  
import os

Header and import statements.

def UDPServer():  
  
 #string of bytes to hold passed file  
 frame=b''  
  
 #Define server port number  
 serverPort = 11000  
  
 #Create UDP Socket  
 serverSocket = socket.socket(socket.AF\_INET, socket.SOCK\_DGRAM)  
 #Bind socket to port mumber  
 serverSocket.bind(('', serverPort))  
 #output message indicating ready to recieve  
 print('The server is ready to recieve')  
  
 count=0

Setup server and initialize variables to store the received data (frame, stores in bytes) and which packet the server is receiving (count, only used for debug output).

#Loop forever, continually read messages sent to socket  
 while True:  
  
 rcvPacket, addr =rdt\_rcv(serverSocket)  
 if(printflag): print("recieved packet: ", count)  
 if(printflag): print()  
 count+=1

Loop, continually receiving packets indefinetly. Uses the function rdt\_rcv to receive packets (function defined in send\_recieve.py, discussed later).

#Test  
 #if passed sentence = stop code  
 if(rcvPacket==b'stop'):  
 count=0  
 #store created output to bmp file and open the file  
  
 f = open("temp.jpg", "wb")  
 f.write(frame)  
 f.close()  
 os.startfile("temp.jpg")  
  
 #clear the frame  
 frame = b''  
 #Output completion statement  
 print("Finished recieving file\nFile opened in seperate window")  
  
 else:  
 #if not at end of file, concatenate sentence to frame  
 frame+=(rcvPacket)

If the packet sent has the stop code, then stop the server is at the end of the file. Reset count for the next file, write the data to a file (temp) and clear the frame. Finally, output message indicating completion. Otherwise, append the received packet to the frame.

#Main method used to start server  
if \_\_name\_\_ == "\_\_main\_\_":  
 UDPServer()

Main function. Used to simply start the server function.

**send\_and\_recieve.py**

from functions import \*

Import functions. Functions is defined in functions.py, discussed later in this document.

#using this to track what sequnce number the rdt\_send function attaches to its packet  
sequenceNum=0  
def rdt\_send(clientSocket,serverName,serverPort,data):  
 global sequenceNum  
 flag=True  
  
 #make the packet  
 sendpkt = make\_pkt(sequenceNum,data)

Beginning of rdt\_send, used by client. sequenceNum is initially 0, and tracks which sequence is sent and expected (0 or 1). Flag is initialized to true, to be used in a loop in the next code block. Sendpkt is initialized to the packet that is to be sent. This packet contains the sequence number and checksum in the header, and is made by make\_pkt, defined in functions.py.

#basically we keep sending the same packet until we get the response wanted  
 while(flag):  
 #udt send packet  
 udt\_send(clientSocket,(serverName,serverPort),sendpkt,corruptPercent\_client\_to\_server)  
 # wait to recieve a packet  
 rcvpkt, addr = udt\_rcv(clientSocket)  
  
 #extract the data from the packet  
 data, recieved\_sequence\_num, chksum = extract(rcvpkt)  
 if(printflag): print(" sent sequnce num: ", sequenceNum)  
 if(printflag): print(" recivied seq: ", recieved\_sequence\_num)  
  
 flag=False  
 #if the recieved packet is corrupt or the wrong sequnce number do the loop again  
 if(corrupt(rcvpkt)or (not (recieved\_sequence\_num==sequenceNum))):  
 if(printflag): print("corrupt")  
 flag=True

Loop to send the packet. Each loop, the packet is sent, and a function waits for a response from the server. If the response is an Nack (ack with the wrong sequence number) or corrupted, the flag stays true and the loop repeats, resending the packet. If the response is correct and not corrupt, the flag is set to false and the loop is exited. Note each packet is sent using udt\_send, which is defined later in this file.

#if we get here that means we like the repsonse we got and we can iterate the  
 #sequence number and then move on  
 if(printflag): print()  
  
 sequenceNum = (sequenceNum + 1) % 2

Outside of the loop, change sequence number to next value. This is the end of this function. The next packet is sent by re-calling this function.

#send the packets corrupting some of them  
def udt\_send(sendingSocket,destination\_addr,packet,corruptPercent):  
  
 randomNum = random.randint(1, 100)  
  
 # if the random number is less than corrupt percent corrupt the packet  
 if (randomNum <= corruptPercent):  
 packet=coruptPacket(packet)  
  
 sendingSocket.sendto(packet, destination\_addr)

Entirety of udt\_send. Used by the client and server to send packets, this function is responsible for corrupting files that are sent, using the passed corruptPercent, using a random value from random.ranint to determine what to corrupt. The packet is corrupted using the corruptPacket function, defined in functions.py. The function ends by sending the packet.

def udt\_rcv(recievingSocket):  
 while True:  
 #recieve the data as a byte array  
 data, addr = recievingSocket.recvfrom(2048) # buffer size is 2048 bytes  
  
 return data, addr

Entirety of udt\_rcv. Simple receives the data and returns it to the calling function.

expected\_sequence\_Num=0  
sndpkt = make\_pkt(1, b'generic response')  
def rdt\_rcv(recievingSocket):  
 global expected\_sequence\_Num  
 global sndpkt  
 flag=True

Beginning of the rdt\_rcv function, which is used by the server to receive packets. Note that the sequence number is initialized here, and separate from the clients initial sequence number. Additionally, a default packet is also created using make\_pkt. This will be explained later in the function.

#true  
 while(flag):  
  
 flag = False  
  
 #get the data  
 rcvPacket, addr=udt\_rcv(recievingSocket)  
  
 # extract the data  
 data,recieved\_sequence\_num,chksum = extract(rcvPacket)  
  
 if(printflag): print(" expecting sequnce num: ",expected\_sequence\_Num)  
 if(printflag): print(" recivied seq: ",recieved\_sequence\_num)

Beginning of loop used to receive packet. Loops until the flag is false. Note that the flag is set to false at the start of the loop, but swapped back to true if the packet received is corrupt or the incorrect sequence number. This part of the loop receives a packet using udt\_rcv (defined later in this file) and extracts the data using the extract function (defined in functions.py).

#Test  
 #for now just read as 'if bad packet' bad=corrupt or wrong sequnce number  
 if(corrupt(rcvPacket) or (not (recieved\_sequence\_num==expected\_sequence\_Num))):  
 #keep previous response do the loop again  
 if(printflag): print(" corrupt")  
 flag=True  
 else:  
 #make good response, exit loop  
 sndpkt=make\_pkt(expected\_sequence\_Num,b'')

If the package is corrupt, as determined by the corrupt function (defined in functions.py, returns true if corrupt or false if not corrupt) or the sequence number does not matches the expected sequence number, set the flag to true to stay in the loop. If not corrupt and the sequence number matches, override sndpkt with a positive acknowledgement, created with make\_pkt.

# reply to the data with either "good" repsonse or the previous response  
 udt\_send(recievingSocket, addr, sndpkt,corruptPercent\_server\_to\_client)

Send acknowledgement. Always sends what is stored in sndpkt. If the received packet was good, the previous code block set sndpkt to acknowledge with the current sequence number. If the received packet was bad, then it sends what was stored in sndpkt previously, which is an acknowledgement with the previous sequence number.

#deliver the data  
return data, addr

Deliver data back to server function.

**functions.py**

import random  
printflag=True  
corruptPercent\_client\_to\_server = 60  
corruptPercent\_server\_to\_client= 60

Imports and control flags. Printflag controls debug output, corruptPercent controls the chance of corruption, as explained in the overview

def make\_pkt(seq,data):  
 #packet format = seq,chksum,data  
 #Note: Sequence number 0 is encoded as 00000000 and Sequence number 1 is encoded as 11111111 (255)  
 if(seq == 1):  
 seq = int.to\_bytes(255, 1, "big")  
 else:  
 seq = int.to\_bytes(seq, 1, "big")  
  
 #seq=int.to\_bytes(seq, 1, "big")  
 packet=seq+data  
 chksum = GetCheckSum(packet)  
 packet=chksum+packet  
  
 return packet

Entirety of make\_pkt. First overrides the sequence number “1” to 255. This is so the 1 is sent as 11111111 instead of 00000001 (adds redundancy, as need 8 simultaneous bitflips to swap from 1 to 0 or 0 to 1 with this system). Then concatenates the data to the sequence number. Then calculates checksum, and concatenates the checksum and packet. Finally returns packet. Note that header format is checksum as 1st and 2nd byte, sequence as 3rd byte, and data as 4th byte and up.

def extract(rcvpkt):  
  
 chksum = rcvpkt[0:2] #chksum is 1st and 2nd Byte  
  
 seq = rcvpkt[2:3] # sequence num should be 3rd Byte  
  
 seqinteger = int.from\_bytes(seq, "big")  
  
 if(seqinteger == 255):  
 seqinteger = 1  
  
 pckt=rcvpkt[3:] #packet starts at the 4th Byte  
  
 return pckt, seqinteger, chksum

Entirety of extract packet. Extracts the checksum, data, and sequence number and returns them as separate values. Note it also changes 255 back to 1 for the sequence number.

def GetCheckSum(packet):  
 chksum=0  
 currentIndex = 0  
 #go though packet grouping bytes in groups of 2  
 while(currentIndex < len(packet)):  
 byteslice=packet[currentIndex:currentIndex + 2]  
  
 #convert the byte slice to int  
 intslice=int.from\_bytes(byteslice, "big")  
  
 #add the integer to the pre existing checksum  
 chksum+=intslice  
  
 #if the chksum is greater than 65536 than subtrack 65535 (this is the decimal equivlent of  
 #getting rid of the 17th 1 in binary and the adding 1 on the lsb  
 if(chksum>=65536):  
 chksum-=65535  
 currentIndex += 2  
 # convert integer back to byte slice  
 chksum\_byte = int.to\_bytes(chksum, 2, "big")  
  
 return chksum\_byte

Entirety of GetCheckSum, which calculates checksum of a packet. Does this by slicing packets into 2-byte pieces, and adding them together. Returns checksum.

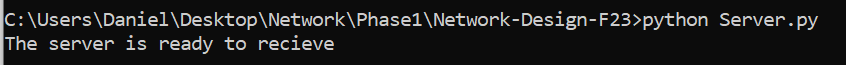
def coruptPacket(packet):  
 corruptpacket =packet+b'corrupt'  
 return corruptpacket

Packet corrupter. Corrupts packets by adding bytes to the packet.

#tells you if a packet is corrupt or not  
def corrupt(rcvPacket):  
 recieved\_chksum=rcvPacket[0:2] #checksum is the first two bits  
  
 packet=rcvPacket[2:] #take the chksum off of the front of the packet  
  
 calculated\_chksum=GetCheckSum(packet)#calculate the actual chksum of the packet so you can compare it  
 #to the recieved one  
  
 if(printflag): print(" recieved chksum: ",recieved\_chksum)  
 if(printflag): print(" calculated chksum: ", calculated\_chksum)  
  
 return (not(recieved\_chksum==calculated\_chksum))

Entirety of corrupt function, used to determine if a packet is corrupt. Done by extracting the checksum, then calculating the checksum for the packet, and comparing the results. Returns true if corrupt, false if not corrupt.

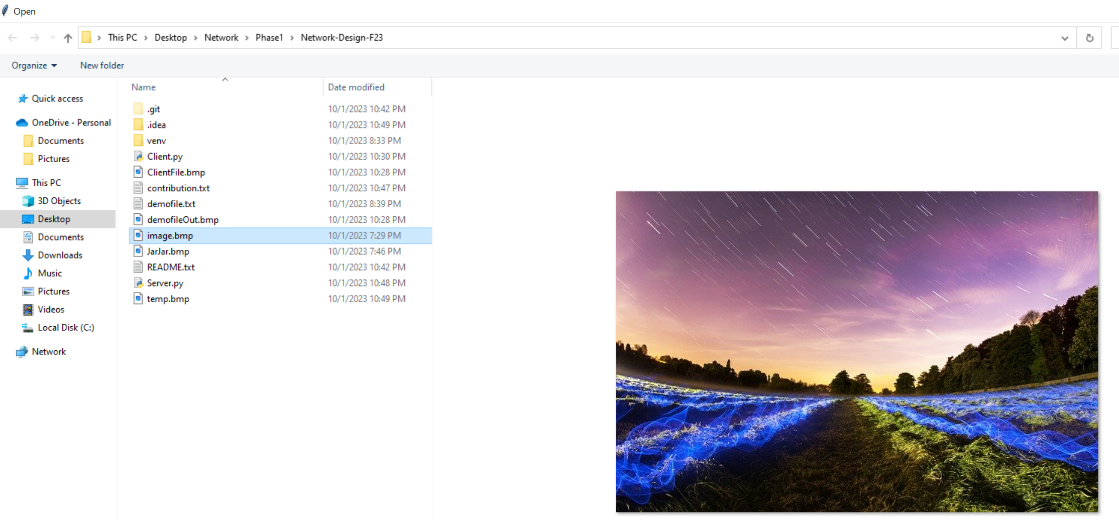
**Execution Example**



Command line command used to start the server code. In this case, the Server.py file is in the folder Network-Design-F23. In the above, you can also see the output provided by the server before the client is run.



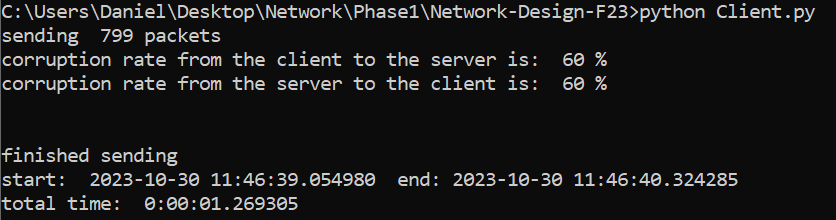
Command line command used to start the client code. In this case, the Client.py file is in the folder Network-Design-F23. Note after the above is run, a standard file select window will open



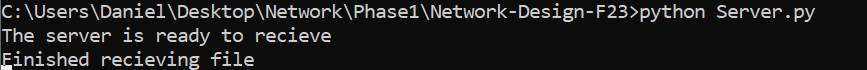
File Select window opened when client.py is run

As noted in the code explanation section, the output produced depends on two separate Boolean flags, printflag (found in functions.py) and runMultipleTests (found on line 98 of Client.py). As such, the different outputs for each combination of these Booleans are shown in this section. Note the information in this section above are not affected by these Boolean values.

Below is the output produced by the client and server with both flags set to False (no output, only one run)

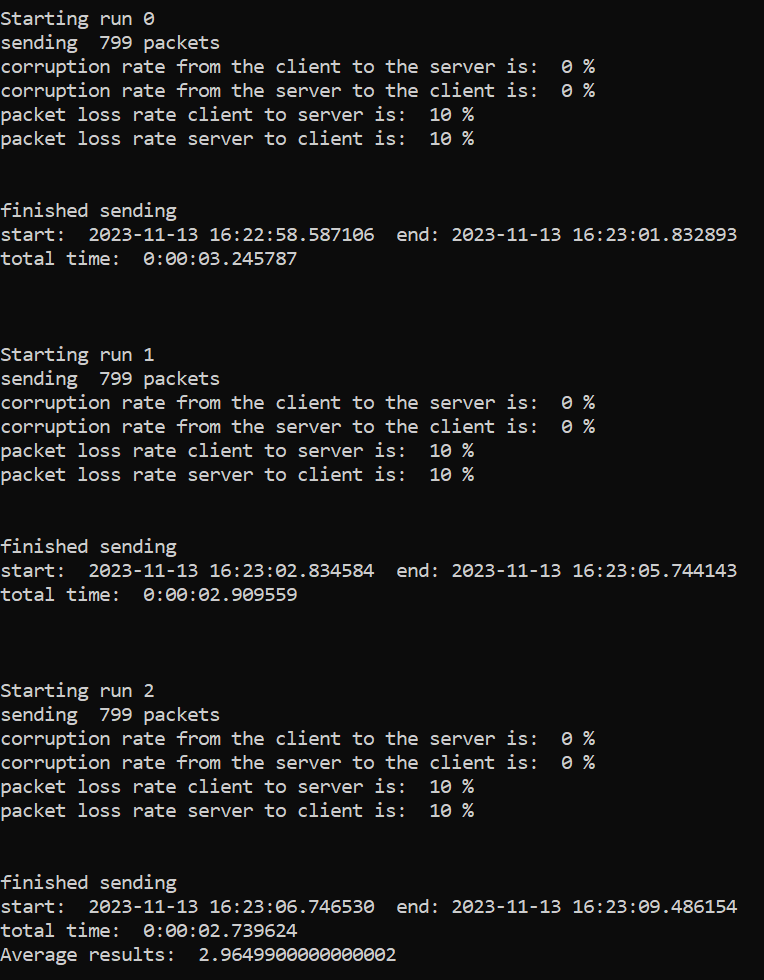


Output produced by the client with both flags set to false. Note the client to server and server to client corruption rate is shown. Additionally, the start and end time, as well as the total time are printed at the end.



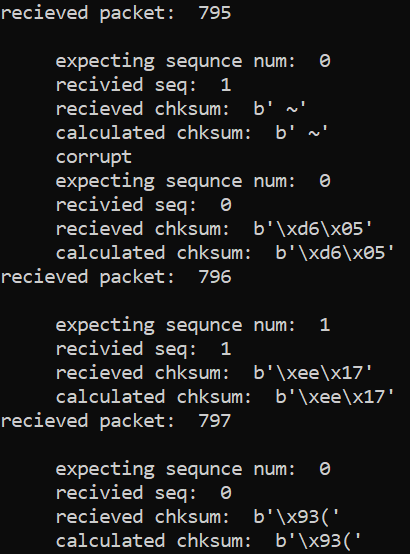
Output produced by the server

Below is the output produced by the client with the runMultipleTests flag set to true, with iterations set to 3 (3 runs are performed then averaged). Note that the output of the server is unchanged between each runs, and as such the server produces the same output as if the client were run multiple times, and as such is not shown below.

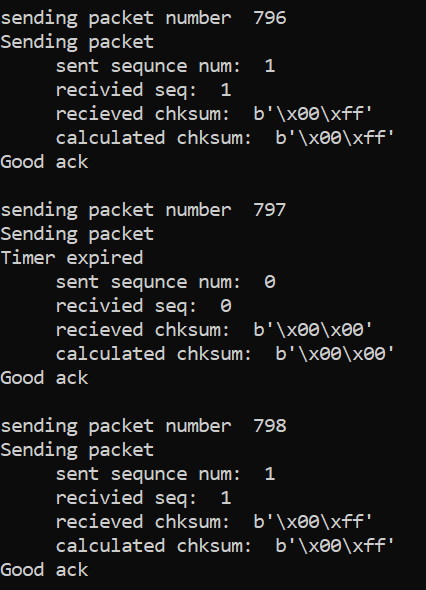


Output produced by the client when running multiple runs. Note the only changes are the run # being printed out before the run, and the average across all the runs printed at the end of all the runs.

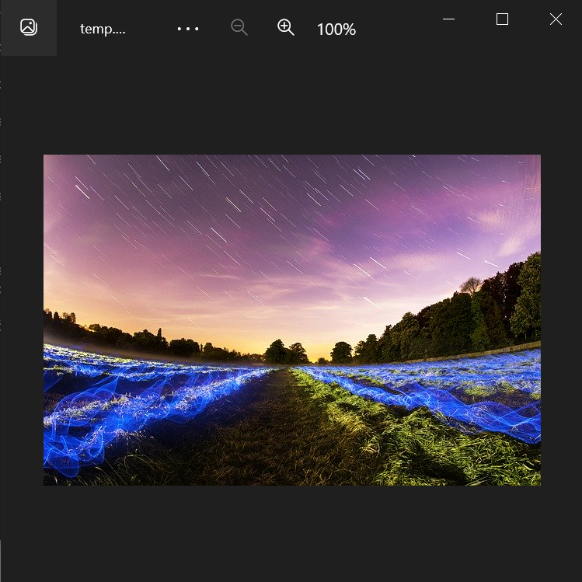
Below is the output produced by the client and server when the print flag is true. For the below output the runMultipleTests flag is false.



Excerpt of output produced by the Server with print True. Note that after receiving packet 795, the server receives a packet with an incorrect sequence number. This indicates the Acknowledgement for packet 795 was dropped, causing the client to re-send the packet, resulting in the server receiving a packet with the incorrect sequence number. This packet is listed as “corrupt,” due to the sequence number being incorrect. After this the next packet is the correct sequence number, indicating the client received the new ack 1, allowing the process to continue.



Output produced by the Client with print True. Notice the “Timer expired” line under packet 797. This indicates that either no ack was received, or a negative acknowledgement was received. As the corrupt chance in this run was 0%, either the packet or ack can be assumed to have been dropped. The timer expired line indicates that a duplicate packet 979 was sent. As can be seen by the results below this, the packet was correctly sent, and the proper acknowledgement was received for the re-sent packet.



Window opened by the server containing the received image.

**Performance Plots:**

Basic considerations:

* File size was 799kB
* All measurements taken on the same pc (Daniel Maccaline’s Desktop)
* All Times taken as an average over 10 runs
* All print commands that occur between the timer being started and stopped were disabled
  + The only print commands were the print statement indicating the program was starting and the time display at the end

**Option 1 - No Loss/bit-errors**

With Loss and corruption rates at 0% both ways, the time to transmit the file was: .33 s

From this result, an interesting observation can be made. First, the time taken for a 0% loss is the same as the time taken with a 0% corruption rate in phase 3. This is expected, as the only change is when and how retransmissions occur, and at this setting, no retransmission occurs.

**Option 2 – ACK packet bit-error:**

ACK corrupted from server to client

Numeric Results (Packet Corruption, Server):

|  |  |
| --- | --- |
| Corruption chance (Server to Client) | Average time |
| 0% | .34 |
| 5% | .84 |
| 10% | 1.48 |
| 15% | 2.22 |
| 20% | 3.21 |
| 25% | 4.12 |
| 30% | 5.37 |
| 35% | 6.70 |
| 40% | 8.46 |
| 45% | 9.99 |
| 50% | 12.53 |
| 55% | 15.23 |
| 60% | 18.58 |

**Option 3 – Data packet bit-error:**

Packet corrupted from client to server

Numeric Results (Packet Corruption, Client):

|  |  |
| --- | --- |
| Corruption chance (Client to Server) | Average time |
| 0% | .34 |
| 5% | .77 |
| 10% | 1.50 |
| 15% | 2.15 |
| 20% | 3.21 |
| 25% | 4.29 |
| 30% | 5.34 |
| 35% | 6.85 |
| 40% | 8.51 |
| 45% | 10.28 |
| 50% | 12.51 |
| 55% | 15.85 |
| 60% | 19.32 |

**Option 4 – ACK packet loss:**

ACK dropped from server to client

Numeric Results (Packet Loss, Server):

|  |  |
| --- | --- |
| Loss chance (Server to Client) | Average time |
| 0% | .34 |
| 5% | .91 |
| 10% | 1.42 |
| 15% | 2.15 |
| 20% | 3.14 |
| 25% | 4.01 |
| 30% | 5.22 |
| 35% | 6.93 |
| 40% | 8.45 |
| 45% | 10.13 |
| 50% | 12.63 |
| 55% | 15.91 |
| 60% | 19.38 |

**Option 5 – Data packet loss:**

Packet dropped from client to server

Numeric Results (Packet Loss, Client):

|  |  |
| --- | --- |
| Loss chance (Client to Server) | Average time |
| 0% | .34 |
| 5% | .84 |
| 10% | 1.40 |
| 15% | 2.27 |
| 20% | 3.11 |
| 25% | 4.13 |
| 30% | 5.37 |
| 35% | 6.81 |
| 40% | 8.44 |
| 45% | 10.24 |
| 50% | 12.48 |
| 55% | 15.87 |
| 60% | 18.94 |