1 Task I

The number of client IPs are 522, 939, 510.
The number of Server IPs are 45, 50, 89.

2 Task II

The number of unique TCP flows are 3256, 5422 and 3280.

3 Task III

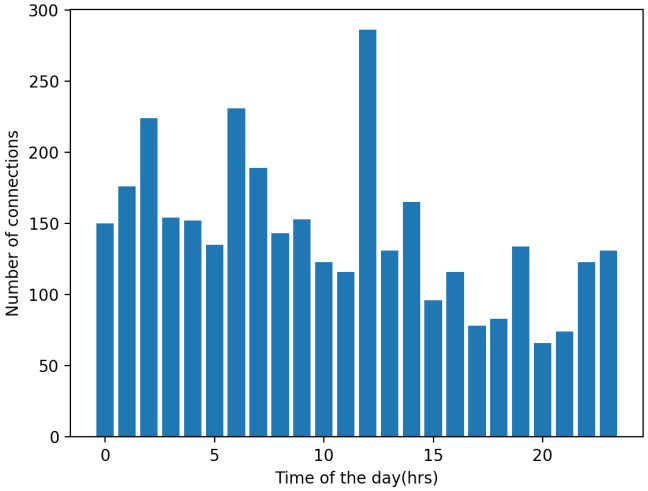

Figure 1: day1

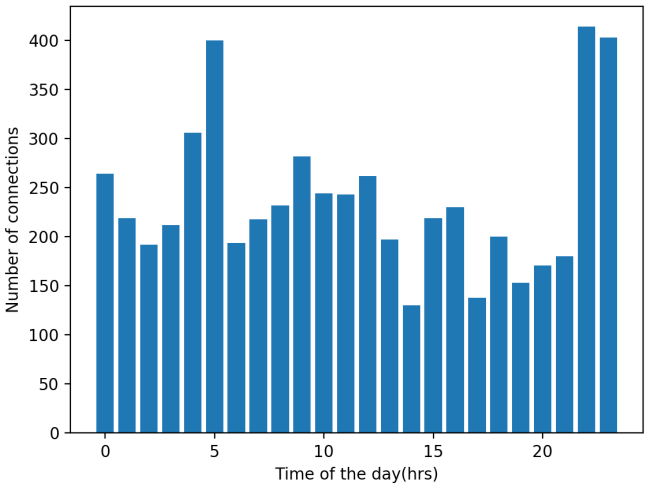

Figure 2: day2

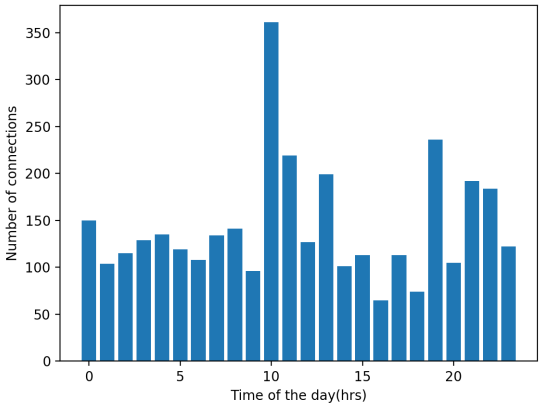

Figure 3: day3

To identify DOS attacks, we can see the usual trend of the number of connections at that particular time of the day. If it is suddenly very high than normal, then there are high chances of the attack.

4 Task IV

Flows starting before the packet capture and continuing beyond the end of packet capture were ignored as in the statement.
If the same flow appears again, then it is considered as a new flow.

Most connections are of very short duration because most TCP requests are for returning flags and acknowledgements and very few only are big like request to download an image. Hence, short duration connections are made for them. Also, this TCP data is underlying the FTP connection on port 21 and not port 20 data and on port 21, many clients try to connect to server and hence small connections are made for that.

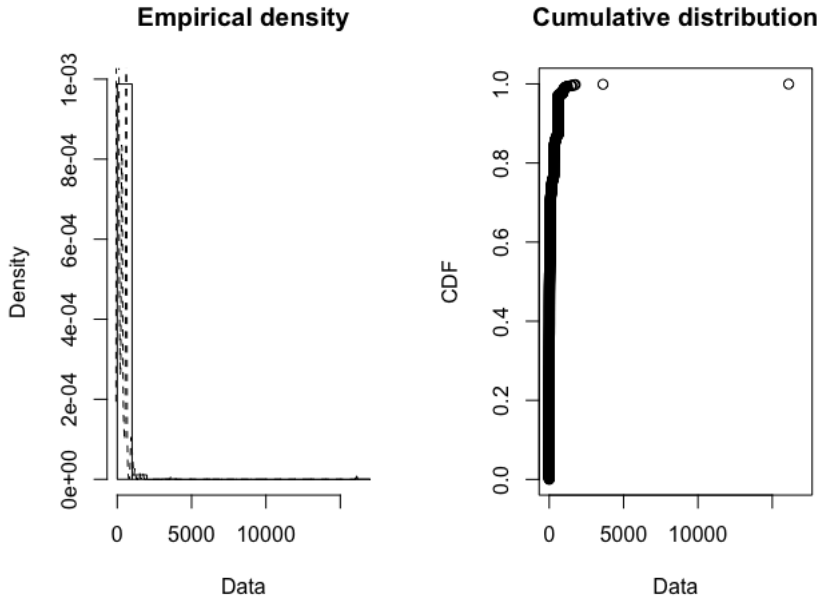

Figure 4: day1

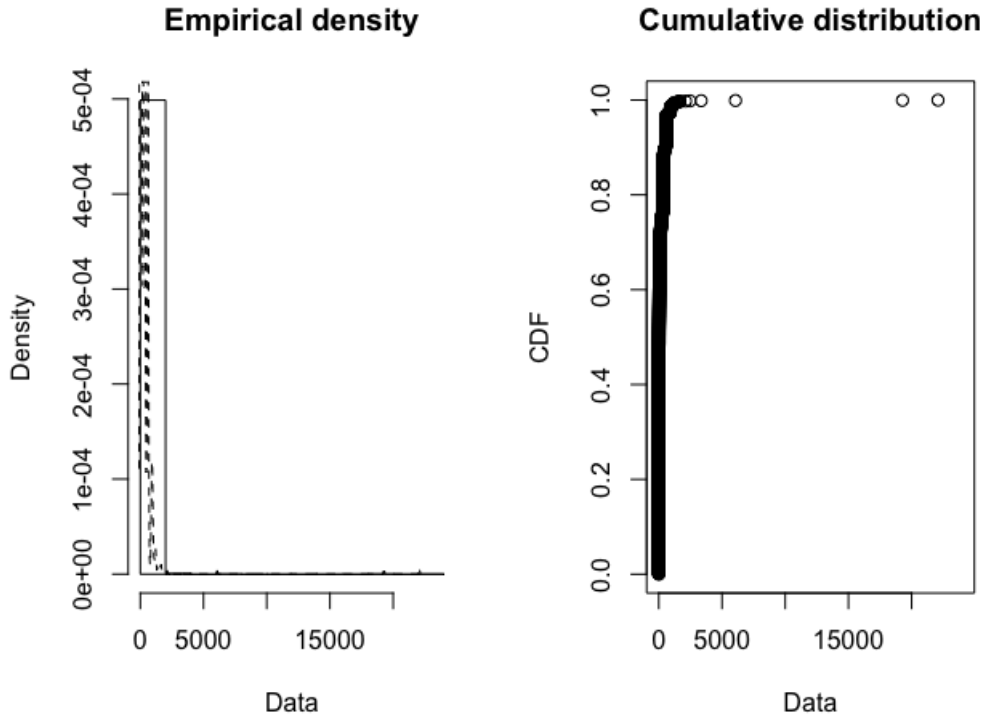

Figure 5: day2

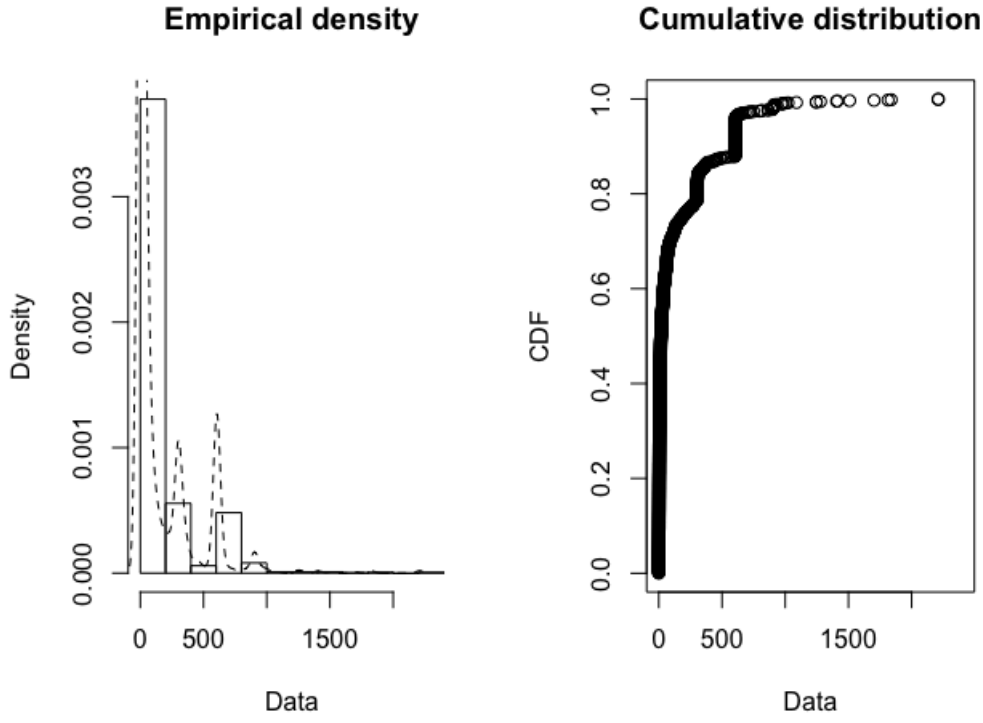

Figure 6: day3

5 Task V

Correlation(sent to the server)=0.8286131, 0.02642153, 0.09926753
Correlation(sent to the client)=0.733241, 0.1633183, 0.4465107

After removing outliers, the correlations increased as follows:
Correlation(sent to the server)=0.8881797, 0.1281794, 0.17009924

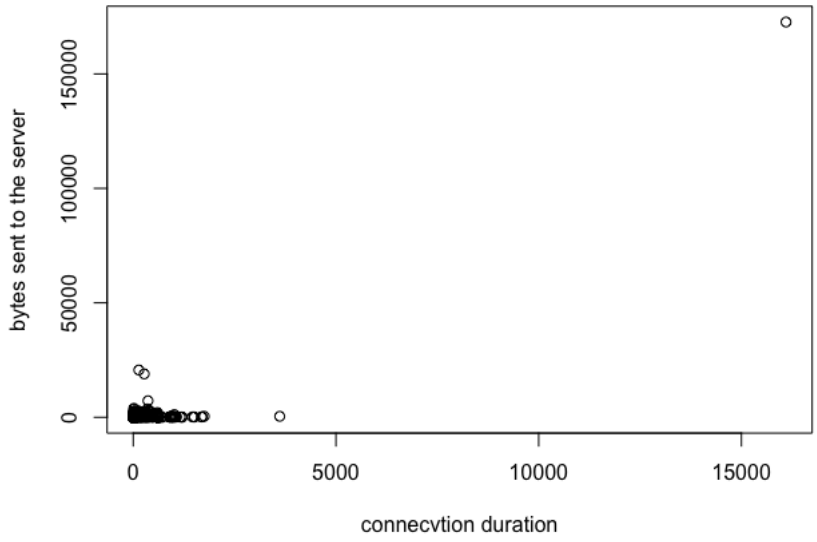

Figure 7: day1-to server

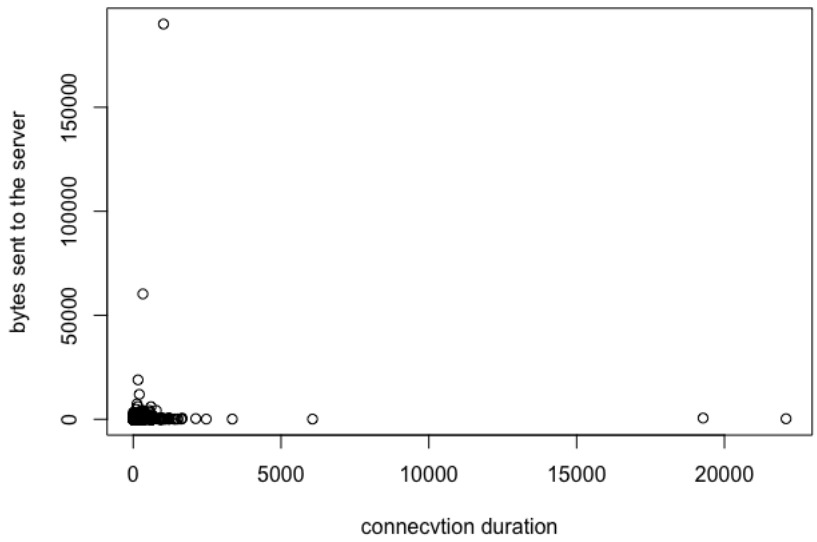

Figure 8: day2-to server

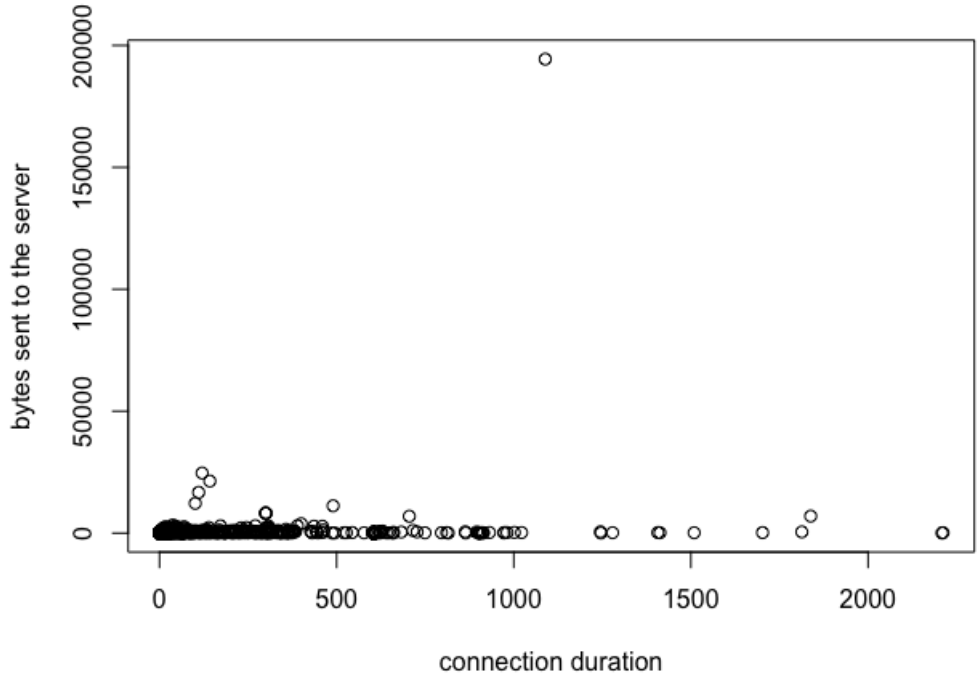

Figure 9: day3-to server

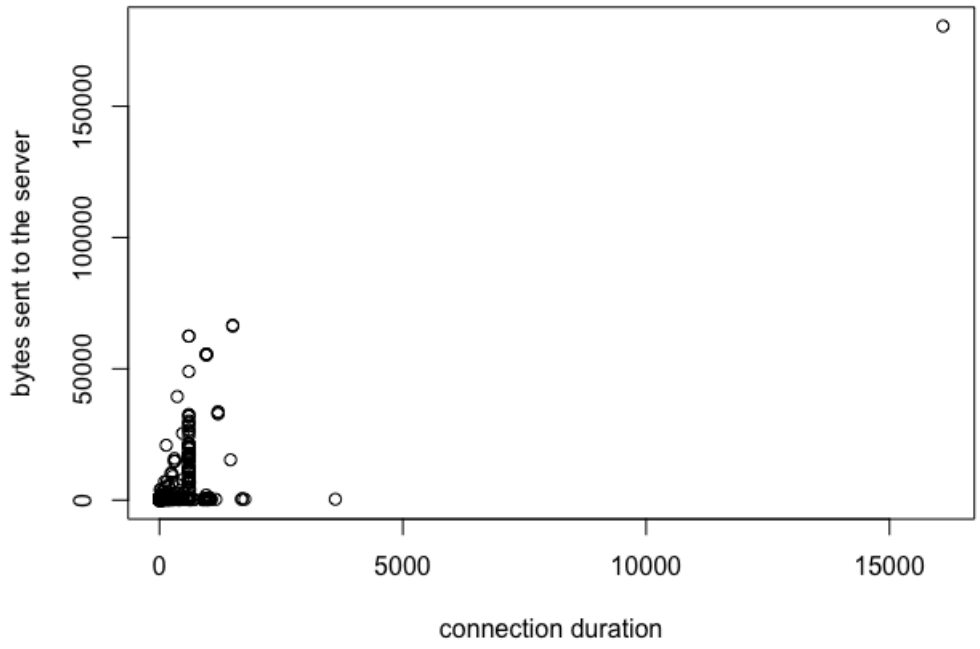

Figure 10: day1-to client

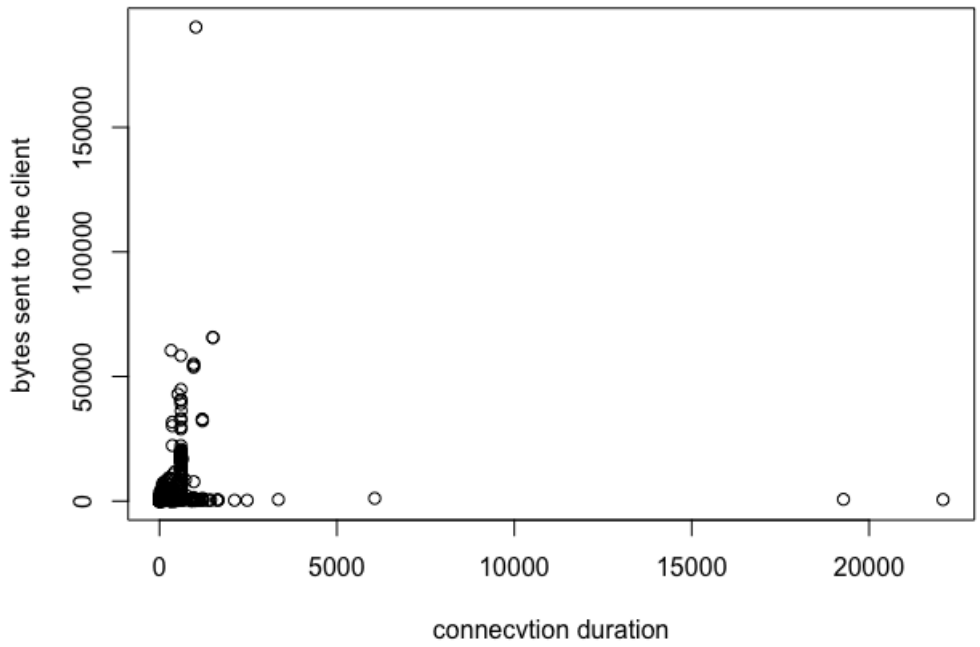

Figure 11: day2-to client

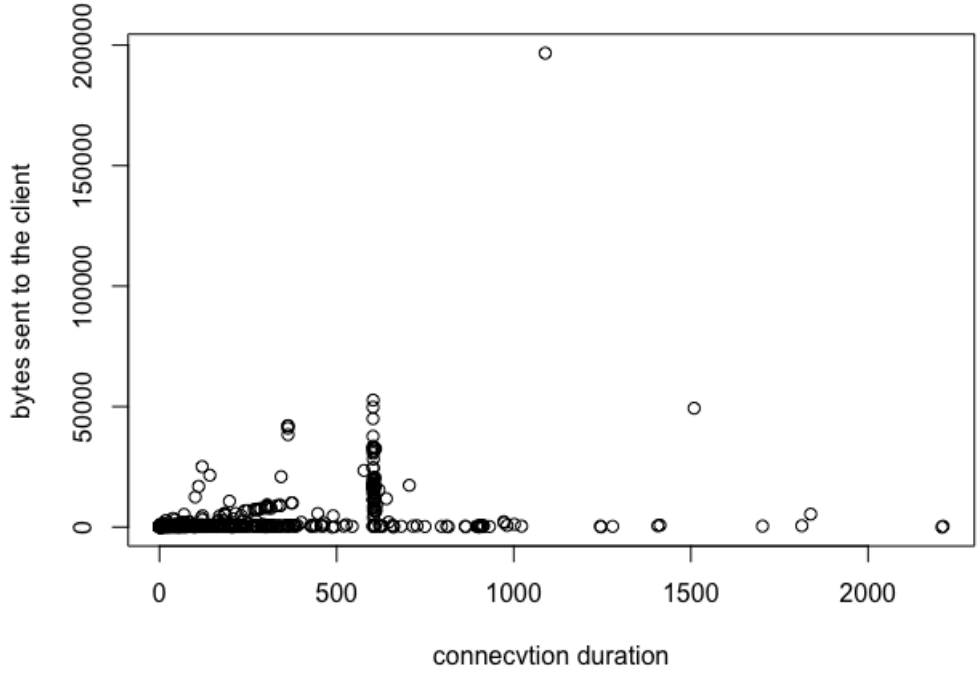

Figure 12: day3-to client

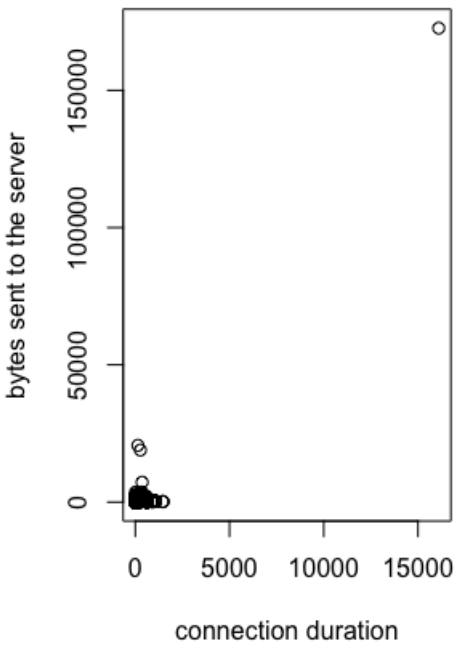

Figure 13: day1-to server(after removing outliers)

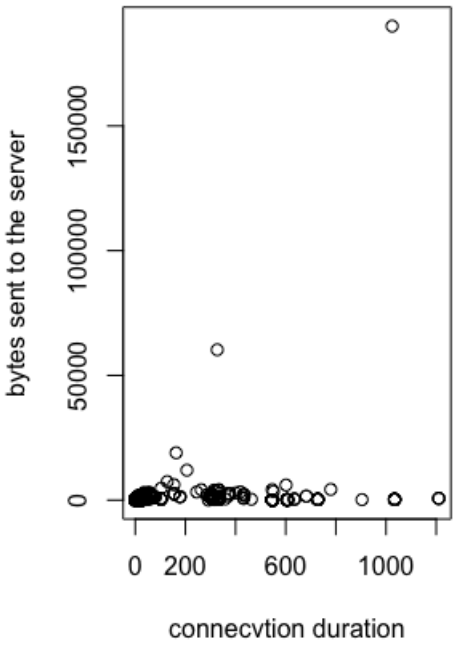

Figure 14: day2-to server(after removing outliers)

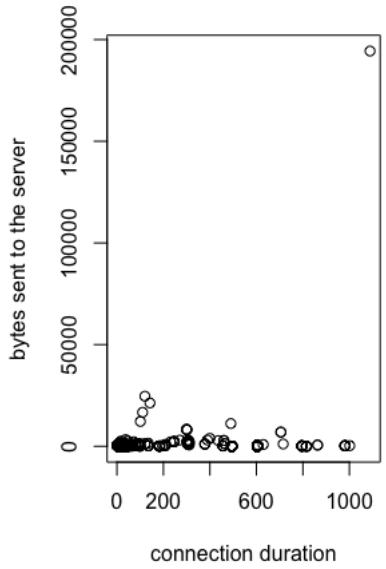

Figure 15: day3-to server(after removing outliers)

6 Task VI

Mean=51.811252, 31.497259, 51.346367
Median=22.295093, 14.375269, 19.582489

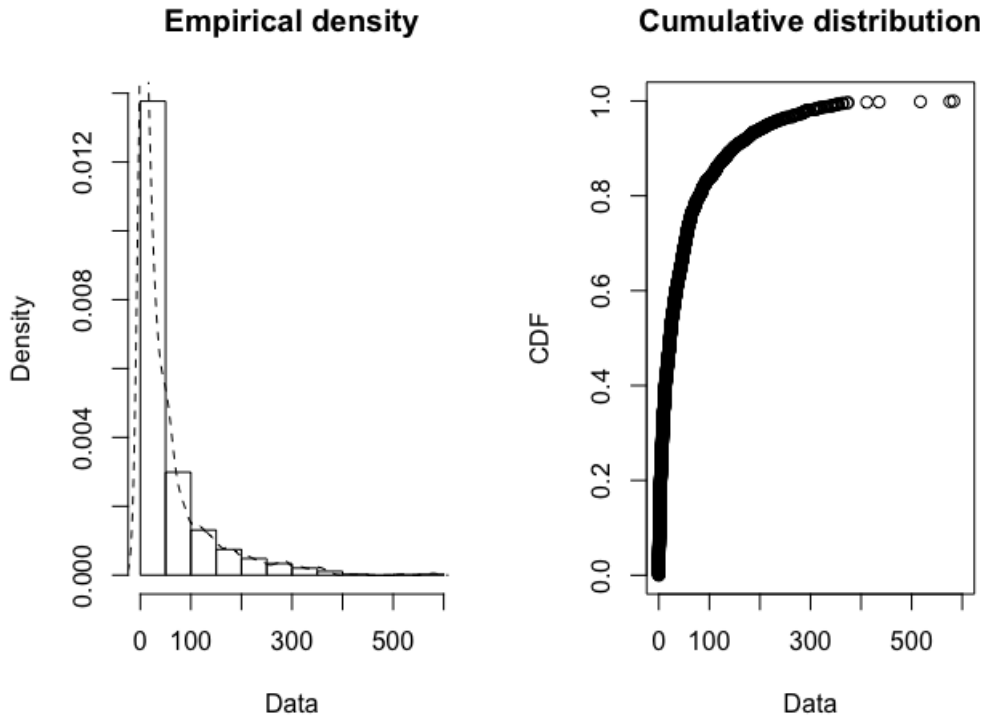

Figure 16: day1

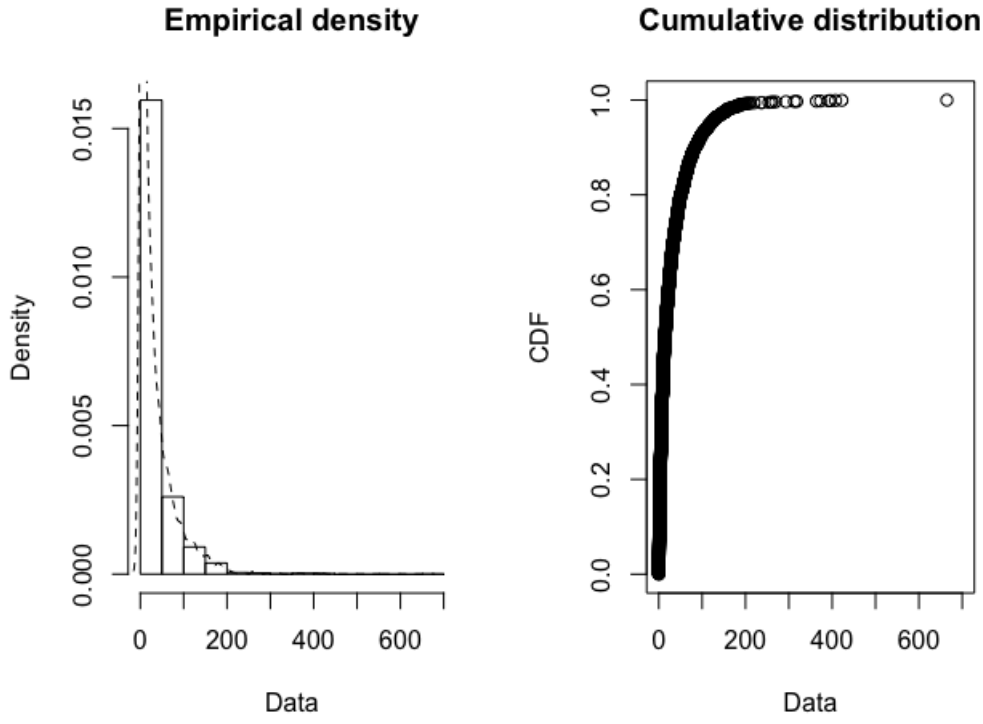

Figure 17: day2

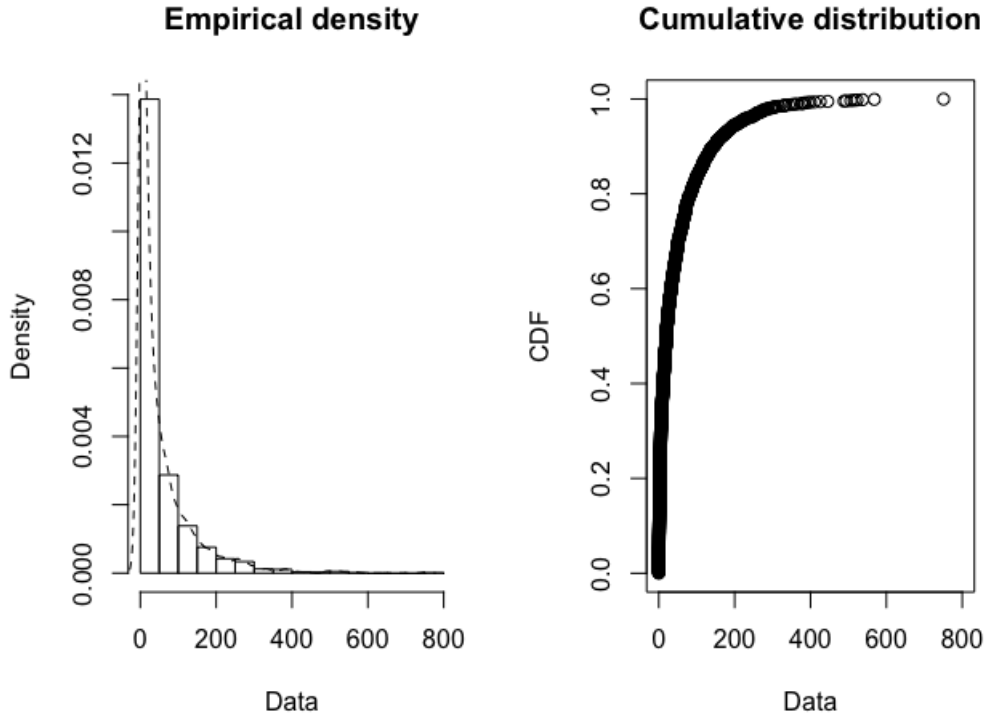

Figure 18: day3

7 Task VII

Due to congestion, some packets may be dropped and they may take a very large time. Mean=1.170584, 0.990487, 1.217088
Median=0.592348, 0.499414, 0.589962

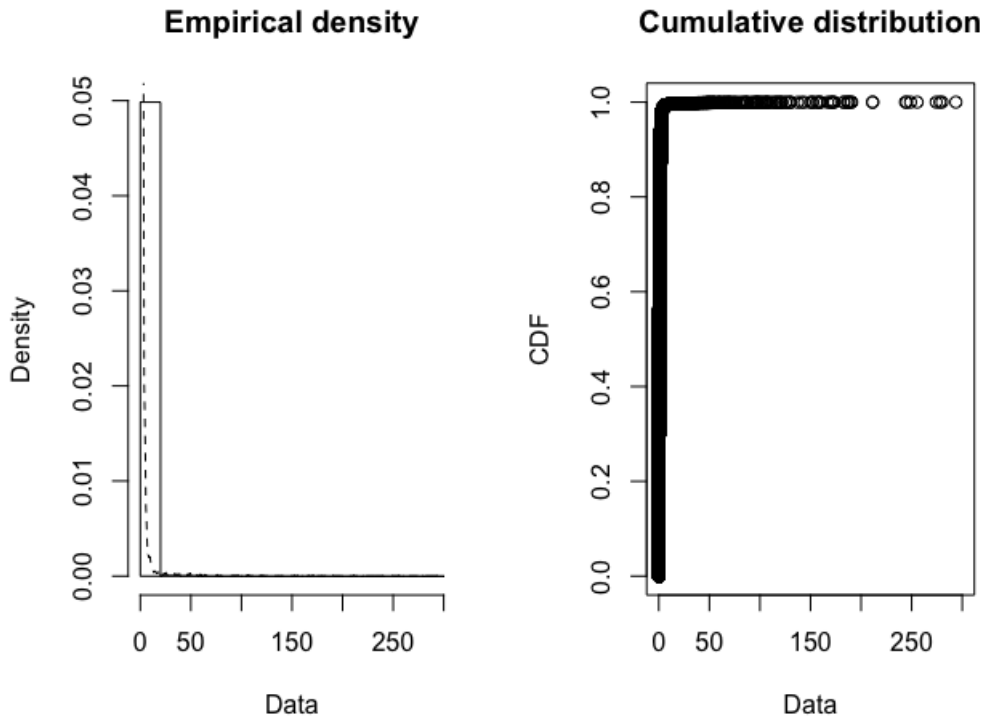

Figure 19: day1

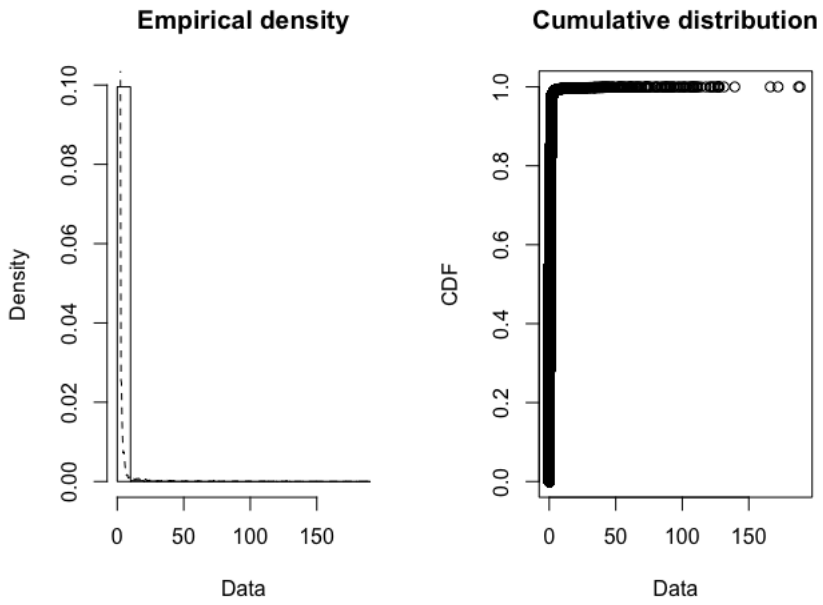

Figure 20: day2

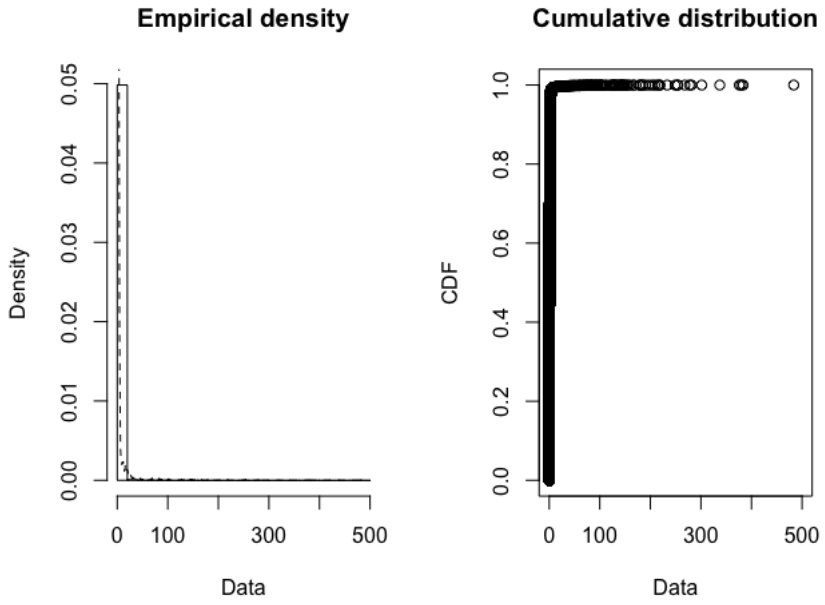

Figure 21: day3

8 Task VIII

Yes, it is clustered around some specific values as most of the packets are just acks and has only header and no other data. Hence it is clustered there.

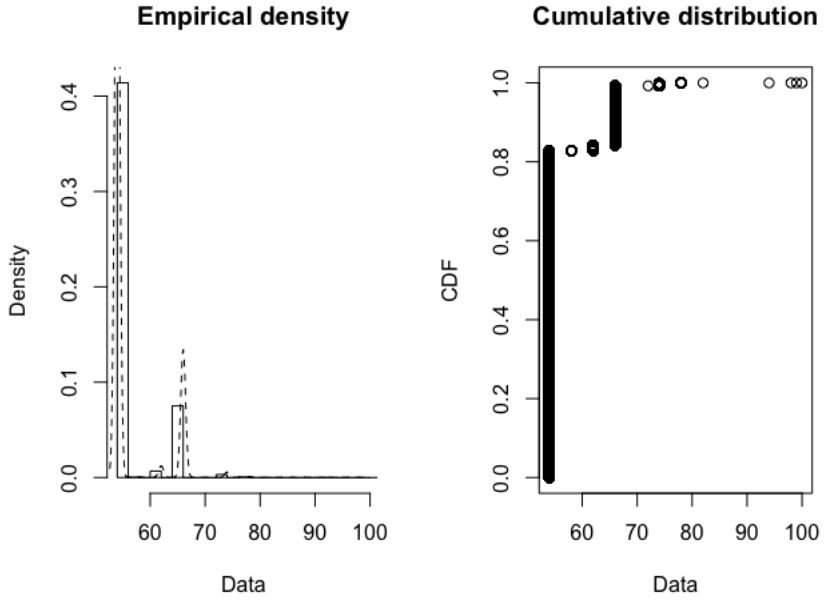

Figure 22: day1(outgoing packets)

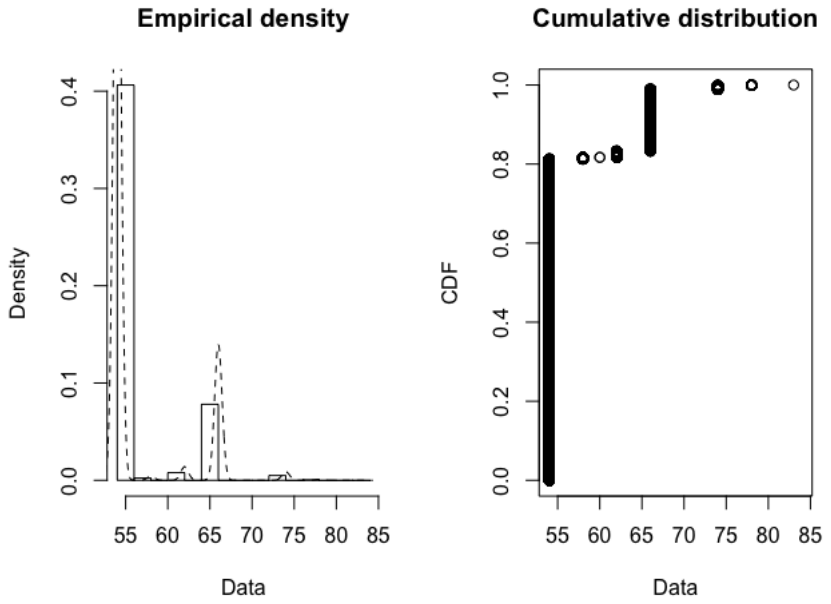

Figure 23: day2(outgoing packets)

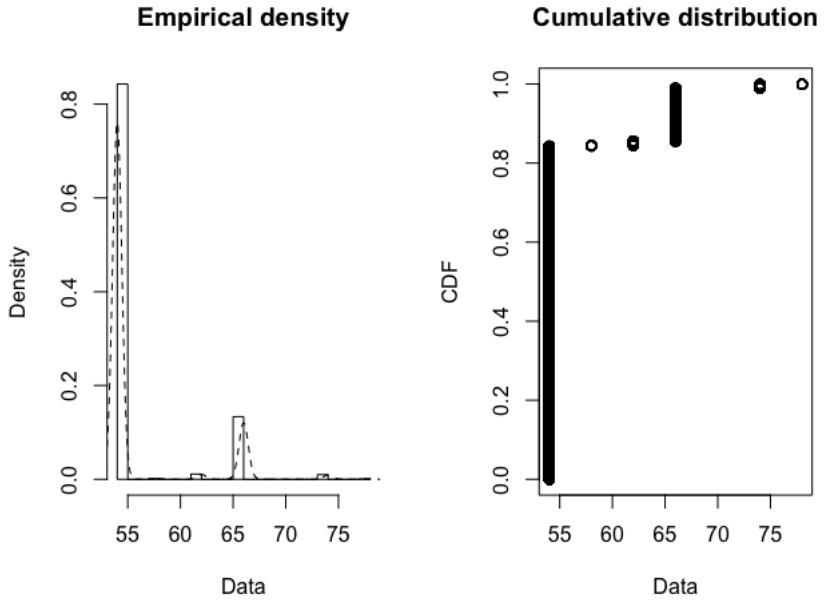

Figure 24: day3(outgoing packets)

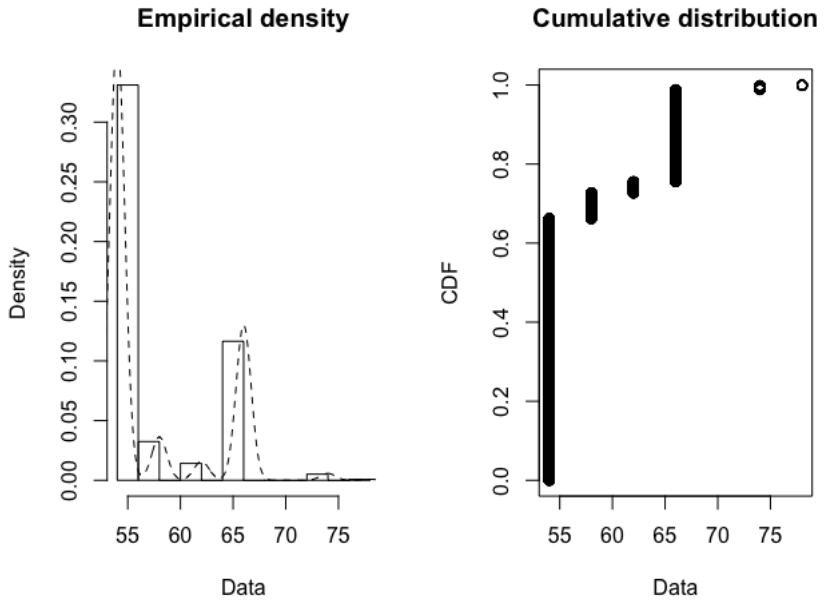

Figure 25: day1(incoming packets)

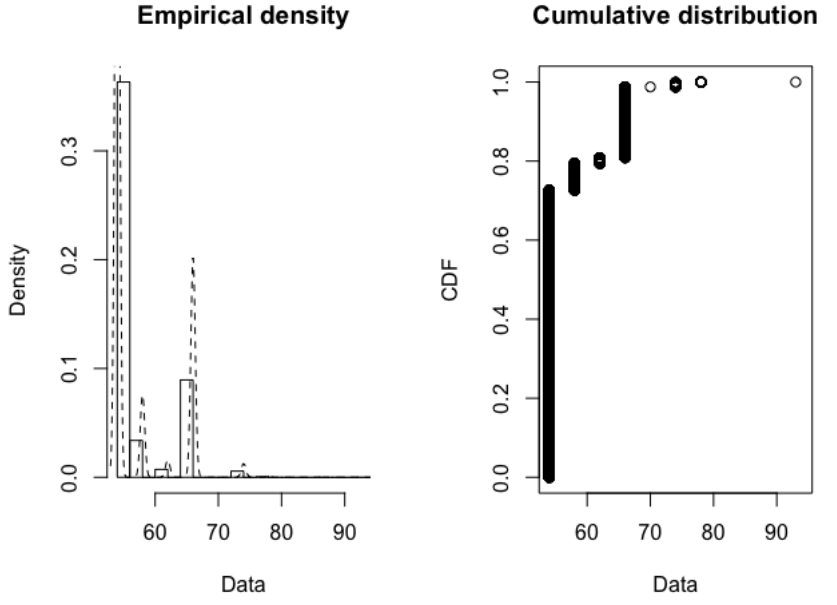

Figure 26: day2(incoming packets)

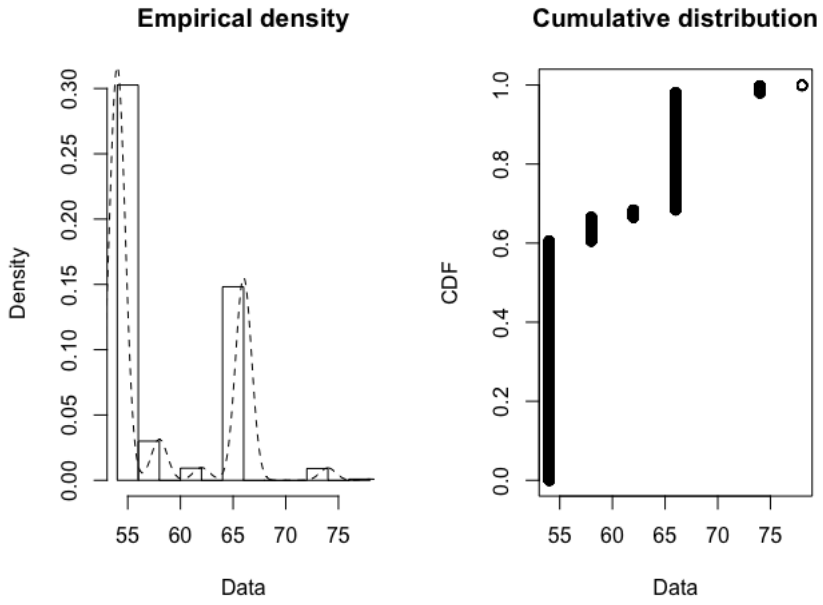

Figure 27: day3(incoming packets)

9 Task IX

Duplicate acks were seen at the very ends of the TCP connections.
I wasn't able to identify where spurious retransmissions happened and where packet re-transmission happened.
Out-of-order delivery didn't occur anywhere.

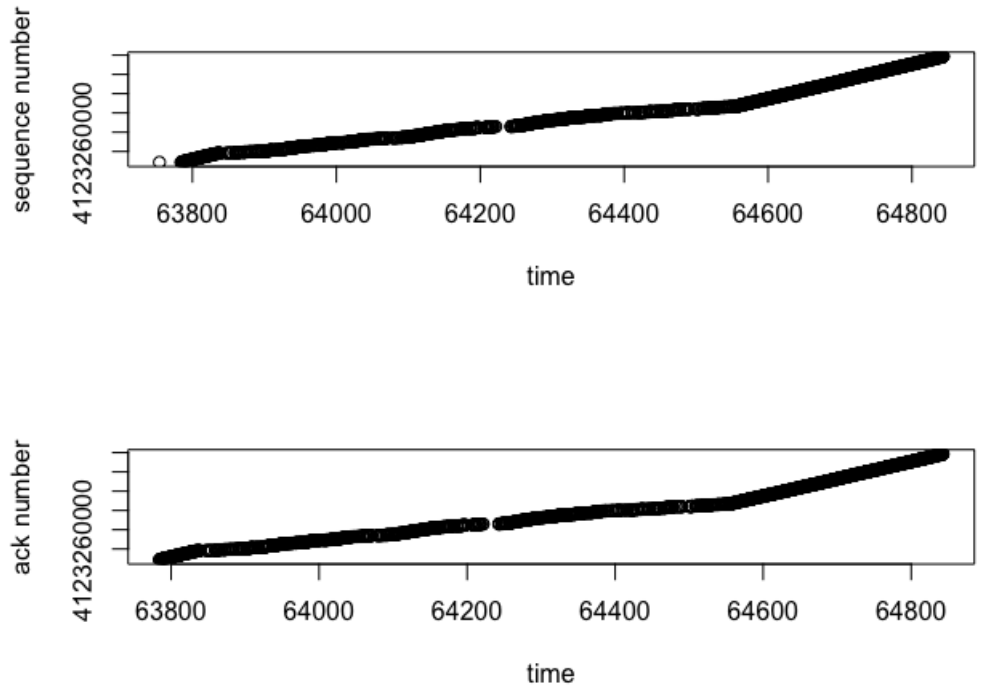

Figure 28:

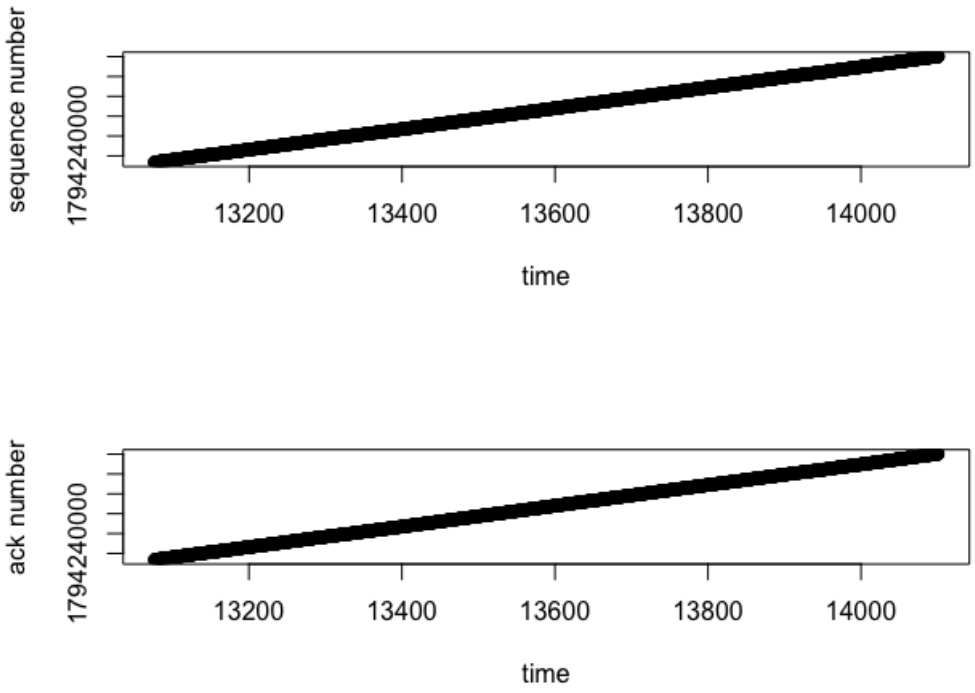

Figure 29:

10 Task X

For question 6:
Exponential Estimate Std. Error
rate(day1) 0.01928925 0.0004713086
rate(day2) 0.03173719 0.0006061479
rate(day3) 0.01946388 0.0004758842

Normal dist Estimate Std. Error
mean(day1) 51.84235 1.824753
sd (day 1) 74.48032 1.290295
mean(day2) 31.50877 0.8608108
sd (day 2) 45.02624 0.6086851
mean(day3) 51.37722 1.908193
sd (day 3) 77.83938 1.349297

For question 7:
Exponential Estimate Std. Error
rate(day1) 0.8542628 0.003144666
rate(day2) 1.009593 0.0034216
rate(day3) 0.8216219 0.003096314

Normal dist Estimate Std. Error
mean(day1) 1.170600 0.02193428
sd (day 1) 5.958539 0.01550988
mean(day2) 0.9904979 0.013791447
sd (day 2) 4.0693650 0.009752023
mean(day3) 1.217105 0.02643482
sd (day 3) 7.014597 0.01869224

From the plots, we can see that exponential distribuiton gives the best fitting.

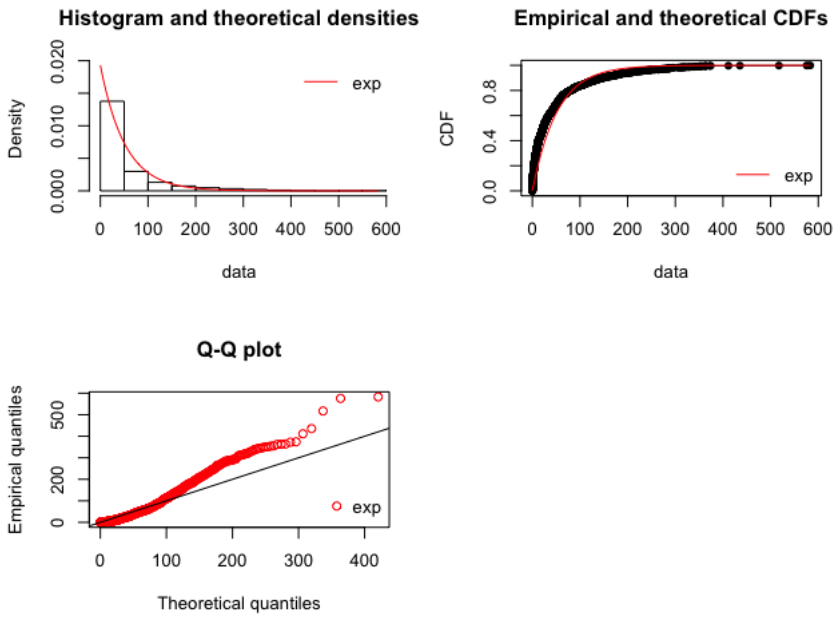

Figure 30: day1(exponential-q6)

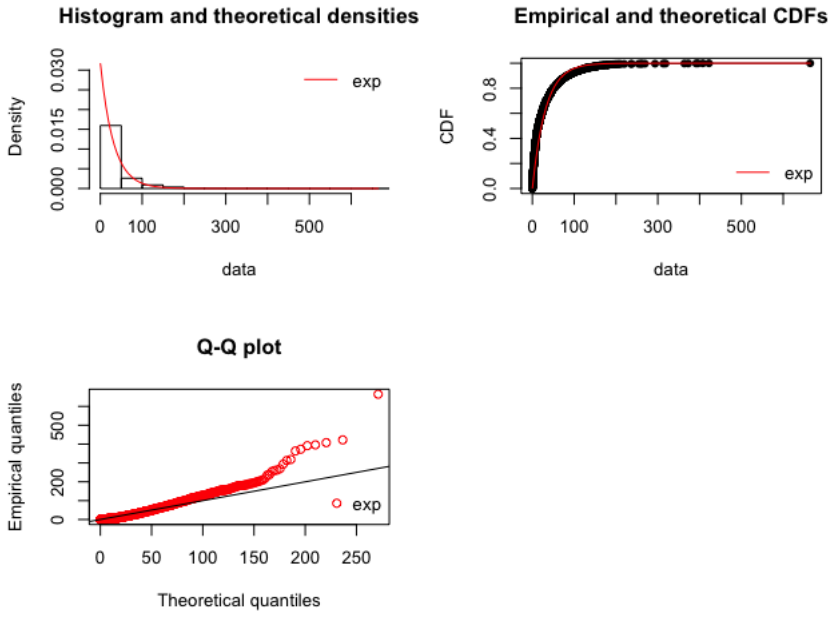

Figure 31: day2(exponential-q6)

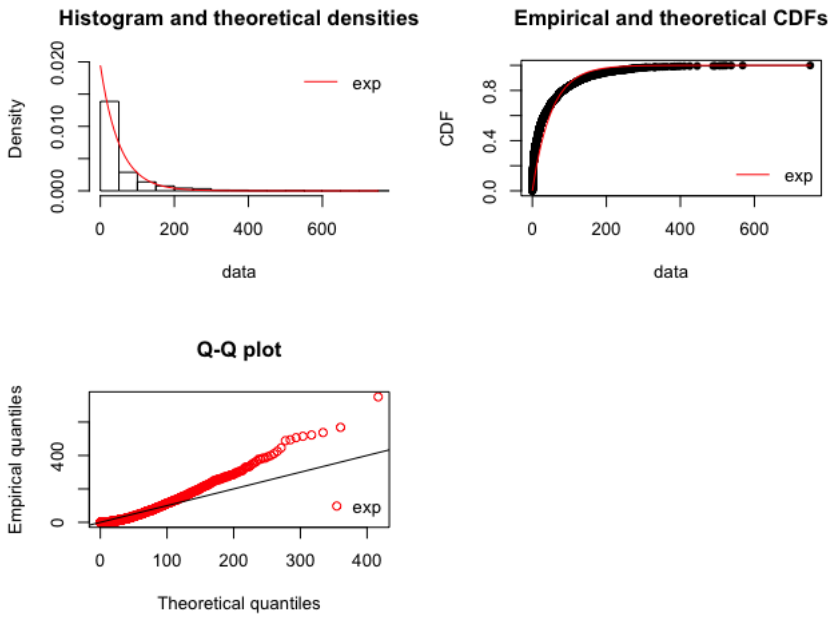

Figure 32: day3(exponential-q6)

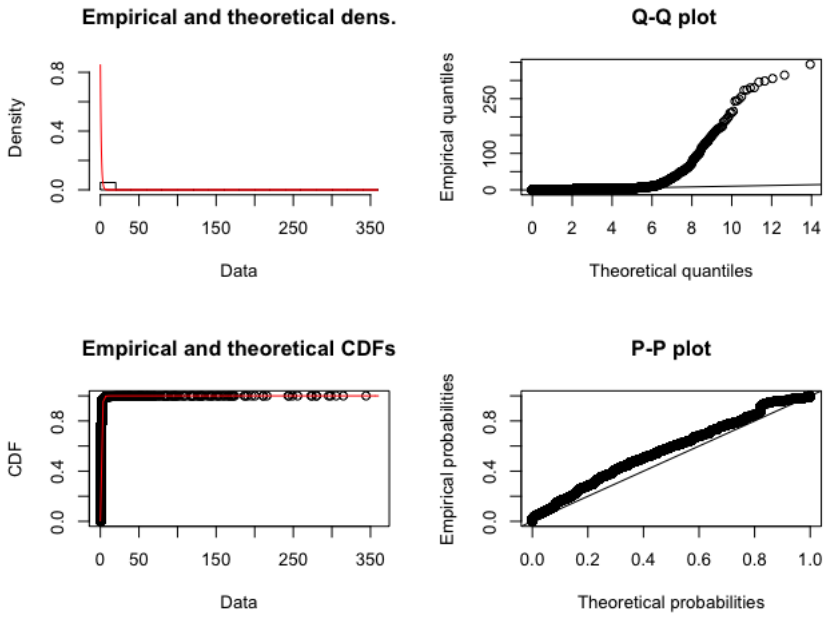

Figure 33: day1(exponential-q7)

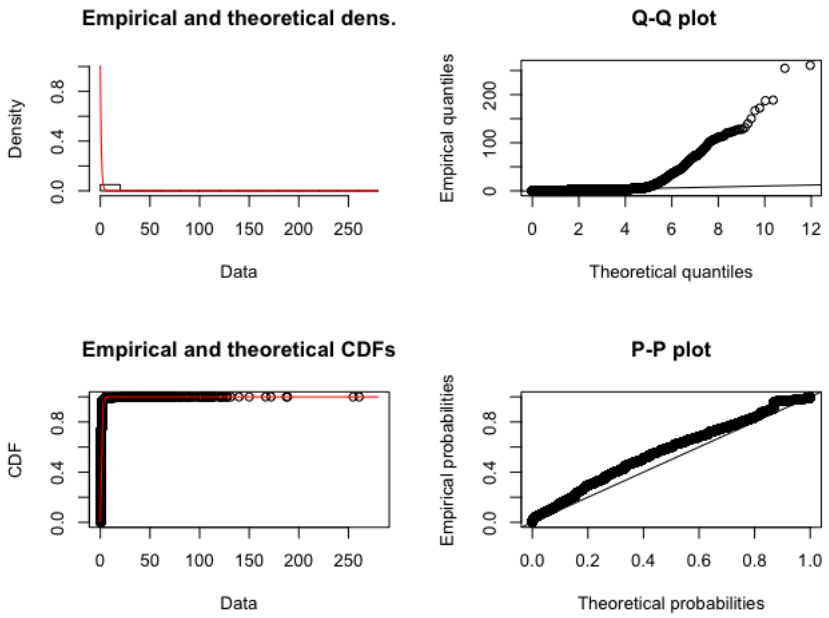

Figure 34: day2(exponential-q7)

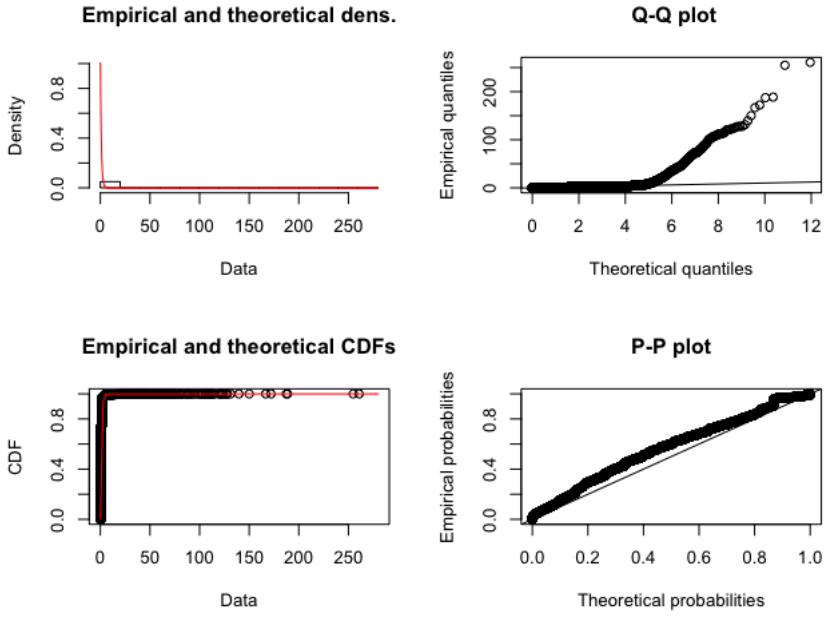

Figure 35: day3(exponential-q7)

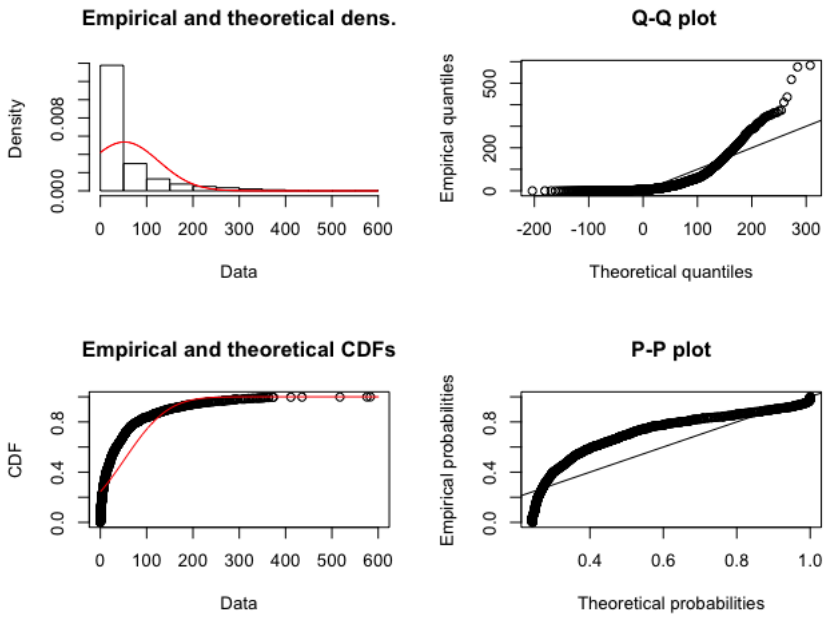

Figure 36: day1(normal-q6)

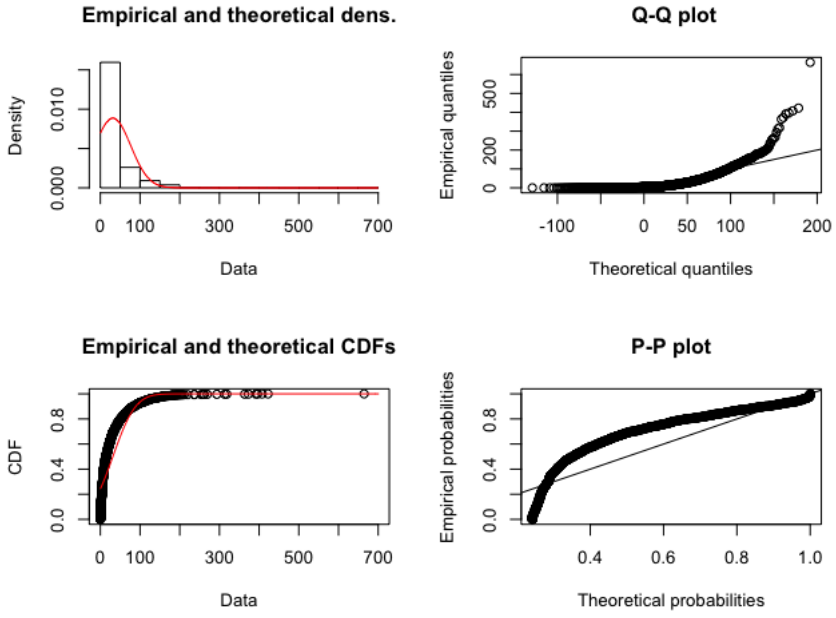

Figure 37: day2(normal-q6)

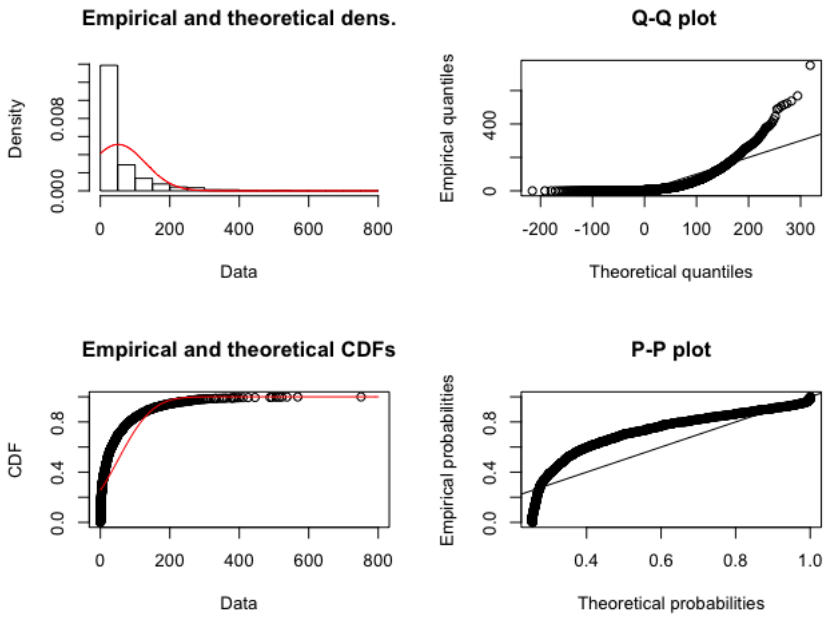

Figure 38: day3(normal-q6)

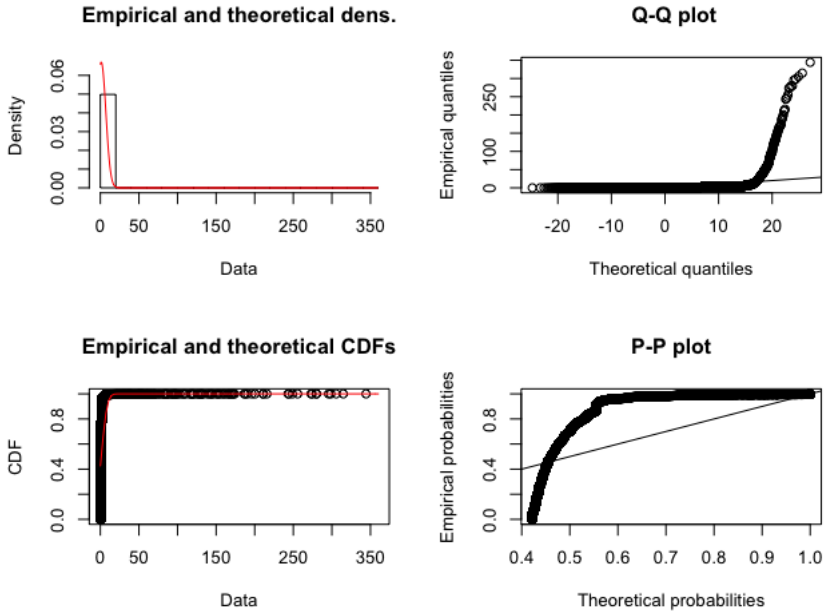

Figure 39: day1(normal-q7)

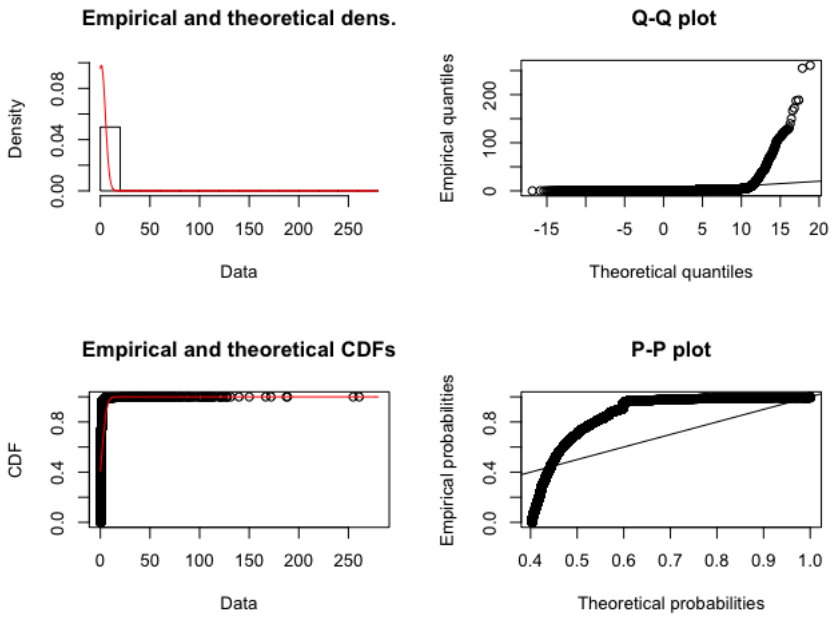

Figure 40: day2(normal-q7)

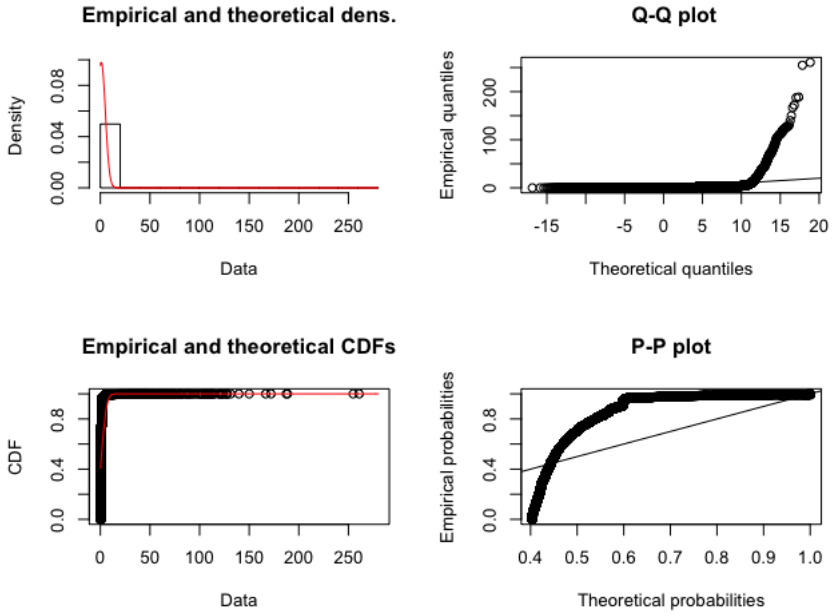

Figure 41: day3(normal-q7)

11 Task XI

λ=0.01928925, 0.03173719, 0.01946388.
μ=128Kb/packetSize
=16KB/56.073160, 16KB/56.241351, 16KB/55.919845
=285.9, 284.5, 286.1
ρ=λ / μ
=66, 111, 68(x$10^{-}6$)
The average queue size = λ / μ - λ
=6.74731e-05, 0.000111567, 6.80364e-05
The average waiting time W =λ/(μ - λ)(μ)
=2.36002e-07, 3.9215e-07, 2.37806e-07.

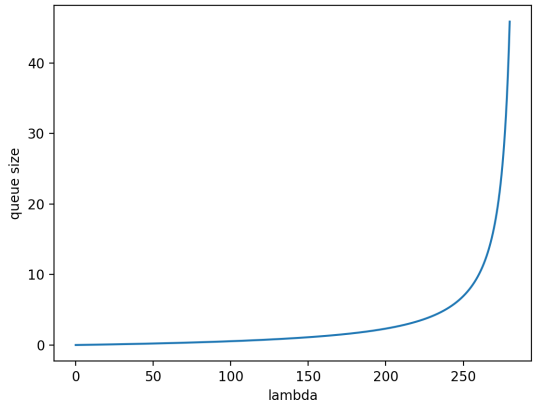

Figure 42:

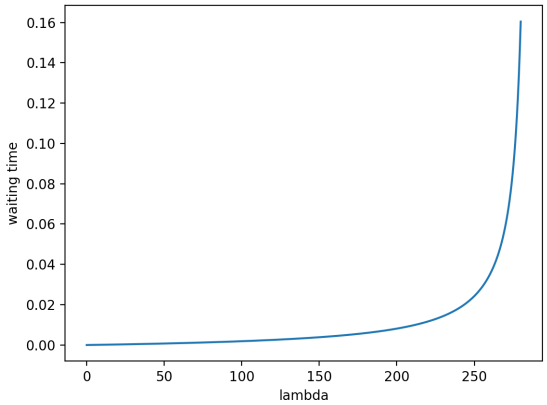

Figure 43:

FTP Commands:
USER: User Name - The argument field is a Telnet string identifying the user.
PASS: Password - The argument field is a Telnet string specifying the user's password.
TYPE: Representation Type - The argument specifies the representation type as described in the Section on Data Representation and Storage.
PORT: Data Port - The argument is a HOST-PORT specification for the data port to be used in data connection.
REST: Restart - The argument field represents the server marker at which file transfer is to be restarted.
OPTS: Options - Select options for a feature
STRU: File Structure - The argument is a single Telnet character code specifying file structure described in the Section on Data Representation and Storage.

MODE: Transfer Mode - The argument is a single Telnet character code specifying the data transfer modes described in the Section on Transmission Modes.
SIZE: Return the size of a file.
RETR: Retrieve - This command causes the server-DTP to transfer a copy of thefile, specified in the pathname, to the server- or user-DTP at the other end of the data connection.
CWD: Change Working Directory - This command allows the user to work with a different directory or dataset for file storage or retrieval without altering his login or accounting information.
HELP: Help - This command shall cause the server to send helpful information regarding its implementation status over the control connection to the user.
NLST: Name List - This command causes a directory listing to be sent from server to user site.
SITE: Site Parameters - This command is used by the server to provide services specific to his system that are essential to file transfer but not sufficiently universal to be included as commands in the protocol.
LIST: List - This command causes a list to be sent from the server to the passive DTP.
STOR: Store - This command causes the server-DTP to accept the data transferred via the data connection and to store the data as a file at the server site.
STAT: Status - This command shall cause a status response to be sent over the control connection in the form of a reply.

FTP Response Codes:
150 About to open data connection. file status is ok
200 The requested action has been successfully completed.
212 Directory status.
213 File status.
214 Explains how to use the server or the meaning of a particular non-standard command.
220 Service ready for new user.
221 Closing control connection.
225 Data connection open but no transfer in progress.
226 Closing data connection. Requested file action successful.
230 User logged in, proceed. Logged out if appropriate.
231 User logged out.
232 Logout command noted and it will complete when transfer done.
234 Specifies that the server accepts the authentication mechanism specified by the client, and the exchange of security data is complete.
250 Requested file action okay, completed.
257 ”PATHNAME” created.
300 Series The command has been accepted, but the requested action is on hold, pending receipt of further information.
331 valid username, need password.
332 Need account for login.
350 Requested file action pending further information
400 Command was not accepted but can be done next attempet since it is temporary error.
421 Service not available.
425 Can’t open data connection.
426 Connection closed without transfer
430 Invalid Authentication
450 Requested action can not be done.
451 Requested action aborted. Local error in processing.
452 Requested action can not be done. Insufficient memory in system
500 Syntax error, incorrect command
530 Not logged in.
532 Login to store files.
550 Requested action can not be done. No file
553 Requested action can not be done. File name format is not acceptable.