+		-+
CS 433		
Assignment 1:Problem	1	
DESIGN DOCUMENT		
+		-+

Name : Lipika Rajpal Roll Number : 20110102

Overview of the solution:

As a solution to problem statement 1, a full-fledged socket-client application has been built. This application is written in the python language. It uses socket programming principles and OS APIs to create a network that enables file transfer and command execution between a server and a client.

The application consists of the following components/files:

- 1. A python file 'server.py' works as a server on the network.
- 2. A python file 'client.py' works as a client on the network.
- 3. The TCP protocol is used at the transport layer.

The application allows the following commands:

CMD	Description	Status
CWD	Retrieve the path of the current working directory for the user	
LS	List the files/folders present in the current working directory	
CD <dir></dir>	Change the directory to <dir> as specified by the client</dir>	OK/NOK
DWD <file></file>	Download the <file> specified by the user on server to client</file>	OK/NOK
UPD <file></file>	Upload the <file> on client to the remote server in CWD</file>	OK/NOK

The client can request any of the above services from the server.

MODES OF LAYERING

1. File service Layer:

The file service layer enables the client to request services from the server. The server responds by executing the requested commands like some OS APIs:

• LS: The server procures the list of all the folders in the current working directory of the server and transfers it to the client.

Fig 1: Implementation of the response to the 'LS' command in server.py

• **CWD:** The server responds by sending the current working directory of the server to the client.

```
if (job == "CWD"):
    res = os.getcwd()

send_encryp(res)

print("[SERVER] Service Provided")
```

Fig 2: Implementation of the response to the 'CWD' command in server.py

• **CD <dir>**: The server changes its current directory to the directory mentioned by the client in the request(**<dir>**)

```
if (job[0:2] == "CD"):
    dir = ""
    for i in range(3, len(job)):
        dir += job[i]
        dir_exist = os.path.exists(dir)
        if (dir_exist):
            os.chdir(dir)
            confirmation = "OK"
        else:
            confirmation = "NOK"

send_encryp(confirmation)
        # c.send(confirmation.encode())
        print(os.getcwd())
        print("[SERVER] Service Provided")
```

Fig 3: Implementation of the response to the 'CD <dir>' call in server.py

The file transfer functionality between the server and the client:

UPD <file>:

• This service enables the client to upload any file (.txt, .png, etc.) to the current directory of the server.

• If the file gets uploaded successfully, the server responds by sending 'STATUS: OK' to the client. If, somehow, the file upload fails, 'STATUS: NOK' is sent.

Overview of the service using an example:

For instance, the client wants to upload the file with the name 'abc.txt' to the server.

We will go with the intuitive notion that the file should exist if the client wants to upload some file. Therefore, the client first checks if the file exists using an OS API – os.file.exists. If it returns true, the file exists and sends a positive response to the server to continue the upload process. Else, it sends a message "FAIL" to the server. If the server gets a 'FAIL' message, it responds to the client by a status code 'NOK' and ends this service. However, if the file exists, the client starts reading the file's contents as bytes. It sends this content to the server in several packets of 2048 bytes. A while loop over the condition that the file is not yet fully read ensures that all the file's data is read and sent to the server.

The server receives these packets in succession and writes them in a file with the name: 'name of the original file + from_CLIENT.extension.' In our example, the name of the file received on the server would be 'abc_from_CLIENT.txt.'

After the server successfully receives the file, it sends the client a confirmation message 'STATUS: OK', and the service ends.

Associated challenges while implementing UPD file service:

The sender has to send chunks of 2048 bytes continuously to the server in succession. Due to this, a synchronization problem arose between the sending and receiving packets. Some packets got lost during the transmission. This led to considerable data loss, and the file could not be uploaded successfully.

To ensure a lossless transmission, a feedback mechanism was implemented. After the client sends one packet, it waits for the server to send a confirmation message 'DONE.' Only after this, the client sends the next packet.

```
while rem size>=0:
170
171
                      content h = c.recv(2054)
172
                      mode encryption = content h[0] - 48
173
                       content = content_h[1:]
174
                       if (mode_encryption == 1):
176
                          content = encrypt cipher(content, -1*shift cipher)
                       if (mode_encryption == 2):
178
179
                          content= transpose(content)
                       file.write(content)
                       send_encryp("DONE")
                       rem size -= 2048
```

Fig 4: The while loop that ensures lossless arrival of file data in server.py

DWD <file>:

- This service enables the client to download any file (.txt, .png, etc.) from the server to the current working directory of the client.
- The client can download a particular file by specifying its path.
- The server confirms if the file download is successful by sending a status code 'OK.' Else responds with 'STATUS: NOK.'
- The requested file gets downloaded in the client directory with the name: 'original name + from SERVER.extension'

Overview of DWD service with an example:

The implementation of this service is the same as that of the UPD <file> service. The only change is that now we assume that the server should have access to the file required by the client. Hence, the server checks for the existence of the file. If it exists, the process continues. Otherwise, the server responds by a status code 'NOK' and terminates the process.

The server reads and sends the file's contents in chunks of 2048 bytes. A while loop ensures that the client safely receives all the contents. A feedback mechanism similar to the UPD service is implemented here. The server only sends the next chunk of data if the client confirms that it has received the previous chunk.

The feedback mechanism was implemented to **overcome the challenge** of lossless transmission as, without it, a significant number of chunks were getting lost over the network.

```
if (file exist):
                   send_encryp("file is there")
                  c.recv(1024)
                   file= open(file_name, "rb")
                  filesize = os.path.getsize(file name)
210
                  rem_size = filesize
211
                  send_encryp(str(rem_size))
212
                  c.recv(1024)
213
                  while rem size>=0:
214
                       content = file.read(2048)
215
216
217
                       send encryp(content)
218
                       c.recv(2048)
219
220
221
                       rem size -= 2048
224
                  file.close()
225
                   confirmation = "STATUS : OK, file download successfully"
```

Fig 5: The implementation of the download process if the requested file exists in server.py

2. <u>Encryption Layer:</u>

As required by the problem statement, there are three modes of encryption:

1. Plain text:

The data is transmitted over the network without any encryption. It is represented by 'MODE o' in the application.

2. Caesar cipher:

Represented by 'MODE 1'

The data is encrypted before transmitting over the network. There is a shift factor set as an integer (ex. 2). Each alphanumeric character in the data is converted to the ASCII character, with the ASCII value having an offset equal to the shift factor. The sender encrypts the message, i.e., shifts the alphanumeric characters with an offset of shift factor, say N.

The receiver decrypts the data by shifting the characters with an offset of -1*shift factor or -N.

Hence, because of the above logic, a single function can be used for both encryption and decryption of the data.

```
23 v def encrypt_cipher(text, shift):
        if (type(text) is bytes):
            text = list(text)
            for i in range(0, len(text)):
            text[i] = (text[i] + shift)%256
          return bytes(text)
        result = ""
        for i in text:
            if (i.isdigit()):
                result += chr((ord(i) + shift - 48)%10 + 48)
            elif (i.isupper()):
                result += chr((ord(i) + shift-65) % 26 + 65)
            elif (i.islower()):
                result += chr((ord(i) + shift - 97) % 26 + 97)
                result += i
        return result
```

Fig 6: The function responsible for the encryption and decryption in MODE 1. This is present in both server.py and client.py

3. Transpose:

Represented by 'MODE 2'

The function reverses the content of the message in a word-by-word manner. The same function can do both encryption and decryption.

For instance, consider the encryption and decryption of the string:

```
'the dog' -> 'eht god' -> 'the dog'
```

```
def transpose(text):

if (type(text) is bytes):
    text = list(text)

text.reverse()
    return bytes(text)

lines = text.splitlines()
    encrypted_lines = []

for line in lines:
    result = ""

words = line.split()

for word in words:
    result += ""

result += ""

encrypted_lines.append(result[1:])

return '\n'.join(encrypted_lines)
```

Fig 7: The transpose function present in both server.py and client.py

Incorporation of the encryption layer:

We have to make an encryption layer for the application. This means that each message sent over the network has to be encrypted. Along with this, a header should be attached to the data containing the information about the mode of encryption. The program/host at the receiving end will read this header, remove it and decrypt the message according to the information in the header.

This is ensured by a custom function to send the data over the network:

```
def send_encryp(text):

if (mode_encryption == 1):
    text= encrypt_cipher(text, shift_cipher)

if (mode_encryption == 2):
    text= transpose(text)

if (type(text) is not bytes):
    msg = str(mode_encryption) + text
    c.send(msg.encode())

else:
    c.send(str(mode_encryption).encode() + text)
```

Fig 8: This function encrypts the data and attaches the suitable header, then sends the data

3. TCP:

The Transmission Control Protocol is at the heart of our application. It is the fourth layer in the OSI model of networking. The TCP ensures reliable end-to-end communication between the client and the server.

It is the second layer of the TCP/IP model. It acts as an intermediary between the application layer and the network layer.

The TCP uses a handshake protocol to establish a connection between two hosts. We have used TCP as the transport layer protocol to ensure a safe/lossless transmission between the hosts.

Snapshots of the commands:

1. LS

```
BYE
\Documents\CN_SEM5_ASS1\server.py"ASS1>

[SERVER]: Socket successfully created
[SERVER]: socket binded to 50345

[SERVER]: got connected to ('127.0.0.1', 56755)

[CLIENT] LS
[SERVER] Service Provided

[SERVER] Service Provided Service
```

Fig 9

2. CWD

Fig 10

3. CD <dir>

Here, CD C:\Users\hii\Documents\Oj

```
[SERVER] Service Provided Enter the command :CD C:\Users\hii\Documents\OJ

[CLIENT] CD C:\Users\hii\Documents\OJ [SERVER] :

C:\Users\hii\Documents\OJ OK

[SERVER] Service Provided Enter the command :LS

[CLIENT] LS [SERVER] :

[SERVER] Service Provided actual_out_from_CLIENT.txt input.txt out.txt
```

Fig 11

4. UPD <file>

Here we upload a file with the name: 'ex1.png'



Fig 12: ex1.png

```
[CLIENT] UPD ex1.png Enter the command :MODE 1
ex1_from_CLIENT.png Enter the command :UPD ex1.png
[SERVER] Service Provided [SERVER] :

STATUS : OK, file upload successful
Enter the command :
```

Fig 13: We have also changed the mode to MODE 1. And uploaded the file 'ex1.png'



Fig 14: ex1_from_CLIENT.png

The file received by the server

5. DWD <file>

Here, the client wants to download a text file 'download_file.txt'

Fig 16: Original file

Fig 17: File received by the client

WIRESHARK analysis indicating the correct encryption by the encryption layer-

1. The command LS in plain text/MODE o indicates no encryption:

```
[CLIENT] LS

[SERVER] Service Provided

[CLIENT] LS

[CLIENT] LS

[SERVER] Service Provided

[SERVER] Service Provided

[CLIENT] LS

[SERVER] Service Provided
```

Fig: 18

Wireshark information:

No.	Time	Source	Destination	Protocol	Length Info
	175 329.933739	127.0.0.1	127.0.0.1	TCP	126 25001 → 52626 [PSH, ACK] Seq=16 Ack=174 Win=2161152 Len=82
	176 329.933768	127.0.0.1	127.0.0.1	TCP	44 52626 → 25001 [ACK] Seq=174 Ack=98 Win=2161152 Len=0
	177 329.933805	127.0.0.1	127.0.0.1	TCP	44 25001 → 52626 [FIN, ACK] Seq=98 Ack=174 Win=2161152 Len=0
	178 329.933822	127.0.0.1	127.0.0.1	TCP	44 52626 → 25001 [ACK] Seq=174 Ack=99 Win=2161152 Len=0
	179 329.934679	127.0.0.1	127.0.0.1	TCP	44 52626 → 25001 [FIN, ACK] Seq=174 Ack=99 Win=2161152 Len=0
	180 329.934708	127.0.0.1	127.0.0.1	TCP	44 25001 → 52626 [ACK] Seq=99 Ack=175 Win=2161152 Len=0
	181 379.140297	127.0.0.1	127.0.0.1	TCP	47 52587 → 50345 [PSH, ACK] Seq=7 Ack=525 Win=8439 Len=3
	182 379.140354	127.0.0.1	127.0.0.1	TCP	44 50345 → 52587 [ACK] Seq=525 Ack=10 Win=8442 Len=0
	183 379.143113	127.0.0.1	127.0.0.1	TCP	306 50345 → 52587 [PSH, ACK] Seq=525 Ack=10 Win=8442 Len=262
L	184 379.143163	127.0.0.1	127.0.0.1	TCP	44 52587 → 50345 [ACK] Seq=10 Ack=787 Win=8438 Len=0
> N	ull/Loopback	on wire (376 bits), Gersion 4, Src: 127.0.		5 bits)	on interface \Device\NPF_Loopback, id 0
000	02 00 00 00 45	00 00 2b 1c 52 40 00	80 06 00 00 ····E··	+ · R@ · · ·	
001		00 00 01 cd 6b c4 a9		· · k · · b/	
0020	66 a8 fe 34 50	18 20 f7 3d 52 00 00	30 4c 53 f ⋅ ⋅ 4P ⋅	· =R··01	LS

Fig 19: We can see that the command LS is sent as it is, without any encryption.

No.	Time	Source	Destination	Protocol	Length Info		
	175 329.933739	127.0.0.1	127.0.0.1	TCP	126 25001 → 52626	[PSH, ACK] Seq=16 Ack=174 Win	=2161152 Len=82
	176 329.933768	127.0.0.1	127.0.0.1	TCP	44 52626 → 25001	[ACK] Seq=174 Ack=98 Win=2161	152 Len=0
	177 329.933805	127.0.0.1	127.0.0.1	TCP	44 25001 → 52626	[FIN, ACK] Seq=98 Ack=174 Win	=2161152 Len=0
	178 329.933822	127.0.0.1	127.0.0.1	TCP	44 52626 → 25001	[ACK] Seq=174 Ack=99 Win=2161	152 Len=0
	179 329.934679	127.0.0.1	127.0.0.1	TCP	44 52626 → 25001	[FIN, ACK] Seq=174 Ack=99 Win	=2161152 Len=0
	180 329.934708	127.0.0.1	127.0.0.1	TCP	44 25001 → 52626	[ACK] Seq=99 Ack=175 Win=2161:	152 Len=0
İ	181 379.140297	127.0.0.1	127.0.0.1	TCP	47 52587 → 50345	[PSH, ACK] Seq=7 Ack=525 Win=	8439 Len=3
	182 379.140354	127.0.0.1	127.0.0.1	TCP	44 50345 → 52587	ACK] Seq=525 Ack=10 Win=8442	Len=0
	183 379.143113	127.0.0.1	127.0.0.1	TCP	306 50345 → 52587	[PSH, ACK] Seq=525 Ack=10 Win	=8442 Len=262
L	184 379.143163	127.0.0.1	127.0.0.1	TCP	44 52587 → 50345	[ACK] Seq=10 Ack=787 Win=8438	Len=0
		s on wire (2448 bits)	, 306 bytes captured	(2448 bits	s) on interface \Dev:	ce\NPF_Loopback, id 0	
	Null/Loopback						
>	Internet Protocol V	ersion 4, Src: 127.0.	0.1, Dst: 127.0.0.1				
000	00 02 00 00 00 45	00 01 2e 1c 54 40 00	80 06 00 00 ····E··	. •т@••••			
00:	10 7f 00 00 01 7f	00 00 01 c4 a9 cd 6b	66 a8 fe 34 ·····	· · · · · kf · ·	4		
002	20 62 41 77 00 50	18 20 fa c1 ae 00 00		· · · · · · 0ac			
		75 74 5f 66 72 6f 6d		_ from_CL			
		78 74 20 61 63 74 75		t actual_			
		6f 6d 5f 53 45 52 56		n_ SERVER.			
		69 65 6e 74 2e 70 79		en t.py do			
		5f 66 69 6c 65 2e 74		fi le.txt	d		
	80 6f 77 6e 6c 6f (
				file_fr	ro		
		56 45 52 2e 74 78 74	20 65 78 2e m_SERVE	R .txt ex	c.		
008	90 70 6e 67 20 65	56 45 52 2e 74 78 74 78 31 2e 70 6e 67 20	20 65 78 2e m_SERVE 65 78 31 5f png ex1	R .txt ex L. png ex1	ro «. L_		
90k	70 6e 67 20 65 3 00 66 72 6f 6d 5f	56 45 52 2e 74 78 74 78 31 2e 70 6e 67 20 43 4c 49 45 4e 54 2e	20 65 78 2e m_SERV8 65 78 31 5f png exi 70 6e 67 20 from_Cl	ER .txt ex L. png ex1 .I ENT.png	ro <. L_ 3		
00a 00l	a0 70 6e 67 20 65 3 00 66 72 6f 6d 5f 4 00 65 78 31 5f 66 3	56 45 52 2e 74 78 74 78 31 2e 70 6e 67 20 43 4c 49 45 4e 54 2e 72 6f 6d 5f 53 45 52	20 65 78 2e m_SERV6 65 78 31 5f png ext 70 6e 67 20 from_Cl 56 45 52 2e ex1_fro	ER .txt ex L. png ex1 .I ENT.png om _SERVER	c. L_ 3		
000 000 000	a0 70 6e 67 20 65 2 b0 66 72 6f 6d 5f 4 c0 65 78 31 5f 66 2 d0 70 6e 67 20 65 2	56 45 52 2e 74 78 74 78 31 2e 70 6e 67 20 43 4c 49 45 4e 54 2e 72 6f 6d 5f 53 45 52 78 5f 66 72 6f 6d 5f	20 65 78 2e m_SERV6 65 78 31 5f png ext 70 6e 67 20 from_Cl 56 45 52 2e ex1_fro 43 4c 49 45 png ex	ER .txt ex L. png ex1 LI ENT.png Dm _SERVER _f rom_CLI	TO C. L_ S S C.		
998 998 996 996	a0 70 6e 67 20 65 70 66 72 6f 6d 5f 76 65 78 31 5f 66 70 6e 67 20 65 70 6e 67 20 65 70 6e 67 20 66 70	56 45 52 2e 74 78 74 78 31 2e 70 6e 67 20 43 4c 49 45 4e 54 52 78 5f 66 72 6f 6d 5f 6d 5f 67 20 73 65 72 76 65	20 65 78 2e m_SERVE 65 78 31 5f png exi 70 6e 67 20 from_Cl 56 45 52 2e ex1_fro 43 4c 49 45 png ex 72 2e 70 79 NT.png	ER .txt ex L. png ex1 LI ENT.png DM _SERVER _f rom_CLI s erver.p	ro c. L_ 3 R. EE		
00: 00: 00: 00: 00:	a0 70 6e 67 20 65 60 66 72 6f 6d 5f 6d 65 78 31 5f 66 70 6e 67 20 65 70 6e 67 20 65 70 6e 67 20 74 65 6d 70 6	56 45 52 2e 74 78 74 78 31 2e 70 6e 67 20 43 4c 49 45 4e 54 2e 72 6f 6d 5f 53 45 52 78 5f 66 72 6f 6d 5f 67 20 73 65 72 76 65 43 6f 64 65 52 75 6e	20 65 78 2e m_SERVE 65 78 31 5f png ext 70 6e 67 20 from_Cl 56 45 52 2e ex1_fros 72 2e 70 79 NT.png 6e 65 72 46 tempCo	ER .txt ex L. png ex1 LI ENT.png Dm _SERVER _f rom_CLI s erver.p Dd eRunner			
00; 00; 00; 00; 00; 00;	a0 70 6e 67 20 65 1 a0 66 72 6f 6d 5f 6 a0 65 78 31 5f 66 1 a0 70 6e 67 20 65 1 a0 4e 54 2e 70 6e 6 a0 69 6c 65 2e 70 1	56 45 52 2e 74 78 74 78 31 2e 70 6e 67 20 43 4c 49 45 4e 54 2e 72 6f 6d 5f 53 45 52 78 5f 66 72 6f 6d 5f 72 07 3 65 72 76 65 43 6f 64 65 52 75 6e 79 20 75 70 6c 6f 61	20 65 78 2e m_SERVE 65 78 31 5f png ext 70 6e 67 20 from_Cll 56 45 52 2e ex1_frc 43 4c 49 45 png ex 72 2e 70 79 NT.png 6e 65 72 46 tempCc 64 5f 66 69 ile.py	ER .txt ex L. png ex1 LI ENT.png Dm _SERVER f rom_CLI s erver.p Dd eRunner u pload_f	co 		
000 000 000 000 000 010	a0 70 6e 67 20 65 20 66 72 6f 6d 5f 4 6d 5f 4 6d 5f 4 6d 6f 72 6f 66 72 6f 66 72 6f 6d 70 6e 6f 72 70 70 70 70 70 70 70 70 70 70 70 70 70	56 45 52 2e 74 78 74 78 31 2e 70 6e 67 20 43 4c 49 45 4e 54 2e 72 6f 6d 5f 53 45 52 78 5f 66 72 6f 6d 5f 67 20 73 65 72 76 65 43 6f 64 65 52 75 6e	20 65 78 2e m_SERVE 65 78 31 5f png exi 70 6e 67 20 from CI 56 45 52 2e ex1_frc 43 4c 49 45 png ex_ 72 2e 70 79 NT.png 6e 65 72 46 tempCc 64 5f 66 69 le.txt	ER .txt ex L. png ex1 LI ENT.png Dm _SERVER _f rom_CLI s erver.p Dd eRunner			

Fig 20: The response by the server is also not encrypted

Now, MODE is changed to 1 from 0. It ensures that the data will be encrypted according to the Caesar cipher with a shift factor of 2.

NOTE: the shift factor is hard-coded as 2 in server.py and client.py.

The same request 'LS' is made by the client (refer to Fig 21)

```
[CLIENT] LS

[SERVER] Service Provided

[CLIENT] LS

[SERVER] Service Provided

[SERVER] Service Provided

[CLIENT] LS

[SERVER] Service Provided

``

Fig 21

## Its Wireshark analysis-

| No.                                                                                                                                                                                                                                                                                                                |     | Time       | Source              | Destination | Protocol                                | Length Info                                                  |  |  |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|------------|---------------------|-------------|-----------------------------------------|--------------------------------------------------------------|--|--|
|                                                                                                                                                                                                                                                                                                                    | 219 | 660.129035 | 127.0.0.1           | 127.0.0.1   | TCP                                     | 77 14517 → 49671 [PSH, ACK] Seq=647 Ack=287 Win=8239 Len=33  |  |  |
|                                                                                                                                                                                                                                                                                                                    | 220 | 660.129066 | 127.0.0.1           | 127.0.0.1   | TCP                                     | 44 49671 → 14517 [ACK] Seq=287 Ack=680 Win=1269 Len=0        |  |  |
|                                                                                                                                                                                                                                                                                                                    | 221 | 660.129166 | 127.0.0.1           | 127.0.0.1   | TCP                                     | 48 49671 → 14517 [PSH, ACK] Seq=287 Ack=680 Win=1269 Len=4   |  |  |
|                                                                                                                                                                                                                                                                                                                    | 222 | 660.129187 | 127.0.0.1           | 127.0.0.1   | TCP                                     | 44 14517 → 49671 [ACK] Seq=680 Ack=291 Win=8239 Len=0        |  |  |
|                                                                                                                                                                                                                                                                                                                    | 223 | 660.129347 | 127.0.0.1           | 127.0.0.1   | TCP                                     | 77 29844 → 49672 [PSH, ACK] Seq=439 Ack=764 Win=8375 Len=33  |  |  |
|                                                                                                                                                                                                                                                                                                                    | 224 | 660.129392 | 127.0.0.1           | 127.0.0.1   | TCP                                     | 44 49672 → 29844 [ACK] Seq=764 Ack=472 Win=8406 Len=0        |  |  |
|                                                                                                                                                                                                                                                                                                                    | 241 | 673.302889 | 127.0.0.1           | 127.0.0.1   | TCP                                     | 47 52587 → 50345 [PSH, ACK] Seq=10 Ack=787 Win=8438 Len=3    |  |  |
|                                                                                                                                                                                                                                                                                                                    | 242 | 673.302935 | 127.0.0.1           | 127.0.0.1   | TCP                                     | 44 50345 → 52587 [ACK] Seq=787 Ack=13 Win=8442 Len=0         |  |  |
|                                                                                                                                                                                                                                                                                                                    | 243 | 673.304450 | 127.0.0.1           | 127.0.0.1   | TCP                                     | 306 50345 → 52587 [PSH, ACK] Seq=787 Ack=13 Win=8442 Len=262 |  |  |
| -                                                                                                                                                                                                                                                                                                                  | 244 | 673.304481 | 127.0.0.1           | 127.0.0.1   | TCP                                     | 44 52587 → 50345 [ACK] Seq=13 Ack=1049 Win=8437 Len=0        |  |  |
| > Frame 241: 47 bytes on wire (376 bits), 47 bytes captured (376 bits) on interface \Device\NPF_Loopback, id 0 > Null/Loopback > Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  0000 02 00 00 00 45 00 00 2b 1c 5e 40 00 80 06 00 00E.+ ^@ 0010 7f 00 00 01 7f 00 00 01 cd 6b cd a9 62 41 77 00k.bAw |     |            |                     |             |                                         |                                                              |  |  |
| 0010<br>0020                                                                                                                                                                                                                                                                                                       |     |            | 18 20 f6 39 48 00 6 |             | ················bAw<br>··:P····9H···1NU |                                                              |  |  |

In Fig 22, we can see that the command 'LS' is encrypted to 'NU' over the network. This is because the shift factor is 2. Therefore, L was changed to N, and S was changed to U. Hence, our data is correctly encrypted.

| 368 874.197285 127.0.0.1 127.0.0.1 TCP 126 25001 + 52555 [PSH, ACK] Seq-16 Ack-174 Min-2161152 Len-02 368 874.197286 127.0.0.1 127.0.0.1 TCP 44 52555 - 25001 [ACK] Seq-16 Ack-174 Min-2161152 Len-0 368 874.197304 127.0.0.1 127.0.0.1 TCP 44 52555 - 25001 [ACK] Seq-174 Ack-09 Min-2161152 Len-0 368 874.197302 127.0.0.1 127.0.0.1 TCP 44 52555 - 25001 [ACK] Seq-174 Ack-09 Min-2161152 Len-0 368 874.201544 127.0.0.1 127.0.0.1 TCP 44 52555 - 25001 [ACK] Seq-174 Ack-09 Min-2161152 Len-0 368 874.201578 127.0.0.1 127.0.0.1 TCP 44 52555 - 25001 [ACK] Seq-174 Ack-09 Min-2161152 Len-0 388 947.204552 127.0.0.1 127.0.0.1 TCP 44 52555 - 25001 [ACK] Seq-194 Ack-199 Min-2161152 Len-0 389 947.204550 127.0.0.1 127.0.0.1 TCP 44 52557 - 25041 [ACK] Seq-194 Ack-199 Min-2161152 Len-0 389 947.204506 127.0.0.1 127.0.0.1 TCP 44 52557 - 25045 [ACK] Seq-194 Ack-10 Min-3442 Len-0 389 947.204506 127.0.0.1 127.0.0.1 TCP 44 52587 + 59345 [PSH, ACK] Seq-194 Ack-10 Min-3442 Len-0 389 947.204506 127.0.0.1 127.0.0.1 TCP 44 52587 + 59345 [ACK] Seq-1949 Ack-10 Min-3442 Len-0 389 947.204506 127.0.0.1 127.0.0.1 TCP 44 52587 + 59345 [ACK] Seq-1949 Ack-10 Min-3442 Len-0 389 947.204506 127.0.0.1 127.0.0.1 TCP 44 52587 + 59345 [ACK] Seq-1949 Ack-10 Min-3442 Len-0 389 947.204506 127.0.0.1 127.0.0.1 TCP 44 52587 + 59345 [ACK] Seq-1949 Ack-10 Min-3442 Len-0 380 947.204506 127.0.0.1 127.0.0.1 TCP 44 52587 + 59345 [ACK] Seq-1949 Ack-10 Min-3442 Len-0 380 947.204506 127.0.0.1 127.0.0.1 127.0.0.1 TCP 44 52587 + 59345 [ACK] Seq-1949 Ack-10 Min-3442 Len-0 380 947.204506 127.0.0.1 127.0.0.1 127.0.0.1 TCP 44 52587 + 59345 [ACK] Seq-1949 Ack-10 Min-3442 Len-0 380 947.204506 127.0.0.1 127.0.0.1 127.0.0.1 TCP 44 52587 + 59345 [ACK] Seq-1949 Ack-10 Min-3442 Len-0 380 947.204506 127.0.0.1 127.0.0.1 127.0.0.1 TCP 44 52587 + 59345 [ACK] Seq-1949 Ack-10 Min-3442 Len-0 380 947.204506 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.0.1 127.0.       |                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                   | _                                                                                                                         |                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| 364 874.197288 127.0.0.1 127.0.0.1 TCP 44 52655 + 25901 [ACK] Seq-127 Ack-98 kin-2161152 Lene9 366 874.197394 127.0.0.1 127.0.0.1 TCP 44 52655 + 25901 [ACK] Seq-127 Ack-99 kin-2161152 Lene9 367 874.281544 127.0.0.1 127.0.0.1 TCP 44 52655 + 25901 [RIN, ACK] Seq-127 Ack-99 kin-2161152 Lene9 368 874.281548 127.0.0.1 127.0.0.1 TCP 44 52655 + 25901 [RIN, ACK] Seq-127 Ack-99 kin-2161152 Lene9 369 947.284552 127.0.0.1 127.0.0.1 TCP 44 52655 + 25901 [RIN, ACK] Seq-127 Ack-99 kin-2161152 Lene9 369 947.284552 127.0.0.1 127.0.0.1 TCP 47 52567 + 59045 [PSH, ACK] Seq-13 Ack-199 kin-2161152 Lene9 369 947.284552 127.0.0.1 127.0.0.1 TCP 47 52567 + 59045 [PSH, ACK] Seq-13 Ack-199 kin-2487 Lene3 389 947.286255 127.0.0.1 127.0.0.1 TCP 47 52567 + 59045 [PSH, ACK] Seq-19 Ack-19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 306 [9845 + 52567] [ACK] Seq-19 Ack-19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 44 52587 + 59045 [PSH, ACK] Seq-19 Ack-19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 44 52587 + 59045 [ACK] Seq-1949 Ack-19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 44 52587 + 59045 [ACK] Seq-1949 Ack-19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 44 52587 + 59045 [ACK] Seq-1949 Ack-19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 44 52587 + 59045 [ACK] Seq-1949 Ack-19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 44 52587 + 59045 [ACK] Seq-1949 Ack-19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 44 52587 + 59045 [ACK] Seq-1949 Ack-19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 44 52587 + 59045 [ACK] Seq-1949 Ack-19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 44 52587 + 59045 [ACK] Seq-1949 Ack-19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 44 52587 + 59045 [ACK] Seq-1949 Ack-19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 44 52587 PCH 5287 ACK 19 kin-2487 Lene3 389 947.286264 127.0.0.1 127.0.0.1 TCP 44 52587 PCH 5287 ACK 19 kin-2487 Lene3 389 947.286264 127.0.0.1 TCP 44 52687 ACK 19 kin-2487 Lene3 389 947.286264 127.       | No.                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                   |                                                                                                                           |                                                               |
| 365 874.197304 127.8.0.1 127.8.0.1 TCP 44 52655 + 22601 [ACK] Seq-98 Ack=174 Min=2101152 Lene0 366 874.297304 127.0.0.1 127.0.0.1 TCP 44 52655 + 22601 [ACK] Seq-174 Acke99 Min-21011552 Lene0 367 874.201548 127.0.0.1 127.0.0.1 TCP 44 52655 + 22601 [ACK] Seq-174 Acke99 Min-2101152 Lene0 368 874.201578 127.0.0.1 127.0.0.1 TCP 44 52655 + 22601 [ACK] Seq-174 Acke99 Min-2101152 Lene0 369 874.204512 127.0.0.1 127.0.0.1 TCP 47 52657 [ACK] Seq-174 Acke99 Min-2101152 Lene0 369 474.204512 127.0.0.1 127.0.0.1 TCP 47 5267 + 52655 [ACK] Seq-174 Acke90 Min-2401152 Lene0 387 947.206295 127.0.0.1 127.0.0.1 TCP 47 5267 + 5267 [ACK] Seq-184 Ack-1849 Min-2437 Lena0 387 947.206295 127.0.0.1 127.0.0.1 TCP 306 [59345 * 52557 [ACK] Seq-1849 Ack-184 Min-2404 Lene0 387 947.206295 127.0.0.1 127.0.0.1 TCP 306 [59345 * 52557 [ACK] Seq-1849 Ack-184 Min-8442 Lene0 387 947.206295 127.0.0.1 127.0.0.1 TCP 306 [59345 * 52557 [ACK] Seq-1849 Ack-184 Min-8442 Lene0  Frame 387: 366 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface \Device\WP_Loopback, id 0  Mull/Loopback Internet Protocol Version 4, 5rc: 127.0.0.1, Dst: 127.0.0.1  Thermal 387: 366 bytes on wire (2488 bits), 306 bytes captured (2448 bits) on interface \Device\WP_Loopback, id 0  100 7 60 00 01 77 60 00 01 77 60 00 01 77 60 07 60 13 05 75 60 00 00 00 00 00 00 00 00 00 00 00 00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                   |                                                                                                                           |                                                               |
| 366 874.197320 127.0.0.1 127.0.0.1 TCP 44 \$2655 + 25001 [FIN, Seq=1274 Ackee99 kin=2161152 Lenee 368 874.201578 127.0.0.1 127.0.0.1 TCP 44 \$2655 + 25001 [FIN, Seq=1274 Ackee99 kin=2161152 Lenee 368 874.201578 127.0.0.1 127.0.0.1 TCP 44 \$2655 + 25001 [FIN, Seq=1274 Ackee99 kin=2161152 Lenee 368 874.201578 127.0.0.1 127.0.0.1 TCP 44 \$2655 + 25001 [FIN, ACK] Seq=134 Ackee99 kin=2161152 Lenee 368 947.204586 127.0.0.1 127.0.0.1 TCP 44 \$2601 + 52657 [ACK] Seq=09 Acke-175 kin=2161152 Lenee 368 947.204586 127.0.0.1 127.0.0.1 TCP 44 \$2601 + 52657 [ACK] Seq=134 Acke1049 kin=8437 Lene3 369 947.204269 127.0.0.1 127.0.0.1 TCP 306 [98345 + 52567 [ACK] Seq=1494 Acke16 kin=8442 Lene262 388 947.204264 127.0.0.1 127.0.0.1 TCP 306 [98345 + 52567 [ACK] Seq=1494 Acke16 kin=8442 Lene262 388 947.204264 127.0.0.1 127.0.0.1 TCP 306 [98345 + 52567 [ACK] Seq=1494 Acke16 kin=8442 Lene262 388 947.204264 127.0.0.1 127.0.0.1 TCP 306 [98345 + 52567 [ACK] Seq=1494 Acke16 kin=8442 Lene262 388 947.204264 127.0.0.1 127.0.0.1 Dst: 127.0.0.1 Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1 Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1  Therener Protocol Version 4, Src: 127.0.0.1  Therener Protocol Vers |                                                                                                              | 364 874.197268                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 127.0.0.1                                                                                                                                                                                                                                                         | TCP                                                                                                                       |                                                               |
| 367 874.201544 127.0.0.1 127.0.0.1 TCP 44 52051 x 25055 [CR] ACK Seq-174 Ack-09 Min-zi01152 Lene0 368 874.201578 127.0.0.1 127.0.0.1 TCP 47 52057 [CR] Seq-174 Ack-09 Min-zi01152 Lene0 369 347.204532 127.0.0.1 127.0.0.1 TCP 47 52587 x 5255 [ACK] Seq-13 Ack-1049 Min-a847 Lene0 369 347.204505 127.0.0.1 127.0.0.1 TCP 47 52587 x 52587 [ACK] Seq-13 Ack-1049 Min-a847 Lene0 387 947.206205 127.0.0.1 127.0.0.1 TCP 306 [50345 x 52587 [ACK] Seq-1049 Ack-10 Min-a642 Lene0 388 947.206205 127.0.0.1 127.0.0.1 TCP 306 [50345 x 52587 [ACK] Seq-1049 Ack-10 Min-a642 Lene0  Frame 387: 366 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface \Device\WP_Loopback, id 0  Mull/Loopback Internet Protocol Version 4, 5rc: 127.0.0.1, Dst: 127.0.0.1  Top 306 [50345 x 52587 [ACK] Seq-1049 Ack-10 Min-a642 Lene0  800 20 00 00 00 45 00 01 2 tc cf 40 00 20 06 00 00 Er g  100 07 00 00 17 f0 00 01 1                     |                                                                                                              | 365 874.197304                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 127.0.0.1                                                                                                                                                                                                                                                         | TCP                                                                                                                       |                                                               |
| 388 874.201578 127.0.0.1 127.0.0.1 TCP 44 25081 + 52655 [ACK] Seq-90 Ack-175 kin-2161152 Lene 386 947.204586 127.0.0.1 127.0.0.1 TCP 44 55857 + 59435 [Pst, Pst, Pst, Pst, Pst, Pst, Pst, Pst,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                              | 366 874.197320                                                                                                                                                                                                                                                                                                                                                                                                 | 127.0.0.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 127.0.0.1                                                                                                                                                                                                                                                         | TCP                                                                                                                       |                                                               |
| 385 947.206352 127.0.0.1 127.0.0.1 TCP 47 52587 + 50345 [PSI, ACK] Seq-13 Ack-1349 Min-8437 Len-3 386 947.206295 127.0.0.1 127.0.0.1 TCP 48 59345 + 52587 [ACK] Seq-130409 Ack-13 Min-8424 Len-0 387 947.206295 127.0.0.1 127.0.0.1 TCP 306[59345 + 52587 [PSI, ACK] Seq-13049 Ack-13 Min-8424 Len-0 388 947.206205 127.0.0.1 127.0.0.1 TCP 44 59245 + 52587 [PSI, ACK] Seq-13049 Ack-13 Min-8424 Len-0 388 947.206205 127.0.0.1 127.0.0.1 TCP 44 52587 + 50345 [ACK] Seq-13049 Ack-13 Min-8436 Len-0  Frame 387: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface \Device\NP_Loopback, id 0  Null/Loopback  Thermet Protocol Version 4, 5rc: 127.0.0.1, Dst: 127.0.0.1  100 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                              | 367 874.201544                                                                                                                                                                                                                                                                                                                                                                                                 | 127.0.0.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 127.0.0.1                                                                                                                                                                                                                                                         | TCP                                                                                                                       | 44 52655 → 25001 [FIN, ACK] Seq=174 Ack=99 Win=2161152 Len=0  |
| 386 947.204586 127.0.0.1 127.0.0.1 TCP 44 9945 + 52587 [PAK, Seq-1849 Ack-15 Min-8442 Len-02 388 947.206246 127.0.0.1 127.0.0.1 TCP 44 52587 PSH, Ack Seq-1849 Ack-15 Min-8442 Len-26 388 947.206246 127.0.0.1 127.0.0.1 TCP 44 52587 + 50345 [Ack] Seq-1849 Ack-15 Min-8436 Len-0  Frame 387: 306 bytes on wire (2488 bits), 306 bytes captured (2448 bits) on interface \Device\NPF_Loopback, id 0  Mull/Loopback Internet Protocol Version 4, 5rc: 127.0.0.1, Dst: 127.0.0.1  1000 02 00 00 00 45 00 01 2 Lc cf 40 00 30 06 00 00 00  1000 00 00 01 77 00 00 01 2 00 00 01 77 00 00 01 2 00 00 01 00 00 00 00 00 00 00 00 00 00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                              | 368 874.201578                                                                                                                                                                                                                                                                                                                                                                                                 | 127.0.0.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 127.0.0.1                                                                                                                                                                                                                                                         | TCP                                                                                                                       | 44 25001 → 52655 [ACK] Seq=99 Ack=175 Win=2161152 Len=0       |
| 387 947.206205 127.0.0.1 127.0.0.1 TCP 306[9345 + 52587 [PSH, ACK] Seq-1809 Ack-15 Winn-6442 Len+262 388 947.206246 127.0.0.1 127.0.0.1 TCP 44 52587 + 98345 [ACK] Seq-16 Ack-1311 Win-8436 Len+0  Frame 387: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits) on interface \Device\NPF_Loopback, id 0  Null/Loopback Tinternet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  200 02 00 00 00 45 00 01 2c 1c cf 40 00 80 05 00 00 E                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                              | 385 947.204532                                                                                                                                                                                                                                                                                                                                                                                                 | 127.0.0.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 127.0.0.1                                                                                                                                                                                                                                                         | TCP                                                                                                                       | 47 52587 → 50345 [PSH, ACK] Seq=13 Ack=1049 Win=8437 Len=3    |
| 388 947.206246 127.0.0.1 127.0.0.1 TCP 44 52587 + 50345 [ACK] Seq-16 Ack-1311 Win-8436 Len+0  Frame 387: 366 bytes on wire (2448 bits), 366 bytes captured (2448 bits) on interface \Device\NPF_Loopback, id 0  Null/Loopback  Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  270 000 00 00 04 50 00 12 2 1c cf 40 00 00 06 00 00 00 00 00 00 00 00 00 00                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                              | 386 947.204586                                                                                                                                                                                                                                                                                                                                                                                                 | 127.0.0.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 127.0.0.1                                                                                                                                                                                                                                                         | TCP                                                                                                                       | 44 50345 → 52587 [ACK] Seq=1049 Ack=16 Win=8442 Len=0         |
| Frame 387: 366 bytes on wire (2448 bits), 366 bytes captured (2448 bits) on interface \Device\NPF_Loopback, id 0 Null/Loopback Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  2000 80: 80 80 80 50 80 12 22 12 12 40 80 80 80 80 80 80 80 80 80 80 80 80 80                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                              | 387 947.206205                                                                                                                                                                                                                                                                                                                                                                                                 | 127.0.0.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 127.0.0.1                                                                                                                                                                                                                                                         | TCP                                                                                                                       | 306 50345 → 52587 [PSH, ACK] Seq=1049 Ack=16 Win=8442 Len=262 |
| Nullivoplack   Tutcomback   T         | L :                                                                                                          | 388 947.206246                                                                                                                                                                                                                                                                                                                                                                                                 | 127.0.0.1                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 127.0.0.1                                                                                                                                                                                                                                                         | TCP                                                                                                                       | 44 52587 → 50345 [ACK] Seq=16 Ack=1311 Win=8436 Len=0         |
| 100 6b 6e 57 2e 72 61 20 77 72 6e 71 63 66 5f 68 6b kng,ra w rnqcf_hk<br>110 6e 67 2e 76 7a 76 20 77 72 6e 71 63 66 5f 68 6b ng,vzv w rnqcf_hk<br>120 6e 67 5f 68 74 71 6f 5f 45 4e 4b 47 50 56 2e 76 ng_htqo_ENKGPV.v                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 0000<br>0010<br>0020<br>0030<br>0040<br>0050<br>0060<br>0070<br>0080<br>0090<br>00a0<br>00b0<br>00c0<br>00d0 | 02 00 00 00 45 6<br>7f 00 00 01 7f 6<br>62 41 77 06 50 1<br>77 63 6e 5f 71.<br>47 50 56 2e 76.<br>7a 76 20 65 6e 74.<br>7a 76 20 65 6e 77.<br>70 6e 71 63 66 5<br>71 79 70 6e 71 66 56 5<br>67 5f 55 47 54 5<br>72 70 69 20 67 7<br>76 74 33 5f 88 7<br>72 70 69 20 67 7<br>70 69 20 67 7<br>70 69 20 67 7<br>70 70 69 20 67 7 | 10 01 2e 1c cf 40 00 10 00 01 c4 a9 cd 6b 10 00 00 1 c4 a9 cd 6b 10 00 00 1 c4 a9 cd 6b 10 00 10 17 76 5f 68 74 71 16 71 a76 20 6 36 57 6 77 11 6f 5f 55 47 54 58 16 67 07 76 60 72 c7 6 18 47 54 2e 76 70 76 76 18 47 54 2e 76 70 76 15 42 41 16 15 65 47 34 17 16 5f 55 47 54 18 16 56 87 47 16 5f 56 47 34 18 16 56 87 47 16 5f 55 47 54 18 16 56 87 47 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 16 17 17 16 17 16 17 17 17 17 17 17 17 17 17 17 17 17 17 | 80 06 00 00E. 66 a9 00 40 31 63 65 76 bAw-P. 57 45 44 4b 63 65 77 17 47 54 26 76 47 78 26 67 77 78 26 67 77 78 26 67 77 78 26 67 77 78 26 67 78 79 79 20 10 20 67 78 32 57 27 79 69 20 10 20 57 78 32 58 45 46 4b 47 791 87 45 46 4b 47 791 87 47 26 72 61 PV.rpl | v_htqo_E v_cevwcr v_htqo_E v_cevwcr gp_v.ra_f hk ng.vzv f_hkng_b GT .vzv g 3. rpi g NK GPV.rp qo_UGTXG _h tqo_Eh u gtxgt. | if-6 if-6 ··le ··le ··le ··le ··le ··le ··le ··l              |
| 120 6e 67 5f 68 74 71 6f 5f 45 4e 4b 47 50 56 2e 76 ng_htqo_ ENKGPV.v                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 66 5f 68 6b kng.ra                                                                                                                                                                                                                                                | w rnqcf                                                                                                                   | nqcf_hk                                                       |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                   |                                                                                                                           |                                                               |
| 7a 76 zv                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                | 1 6f 5f 45 4e 4b 47                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                   | o_ ENKGP\                                                                                                                 | IKGPV. v                                                      |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 0130                                                                                                         | 7a 76                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | ZV                                                                                                                                                                                                                                                                |                                                                                                                           |                                                               |

Fig 23: Encrypted response by the server.

Now, the mode is changed to 2, i.e., the data will be reversed in a word-by-word manner(refer to Fig 24).

```
[SERVER] Service Provided

[CLIENT] LS

[SERVER] Service Provided

[SERVER] Service Provided

[CLIENT] DWD download_file.txt

[CLIENT] DWD download_file.txt

[SERVER] STATUS OK, Service Provided

Enter the command :MODE 2

Enter the comm
```

Fig 24: The mode is changed, and the client wants to download the file 'download\_file.txt'

| No. |       | Time           | Source                | Destination         | Protocol    | Length Info                                                                                        |
|-----|-------|----------------|-----------------------|---------------------|-------------|----------------------------------------------------------------------------------------------------|
|     | 157   | 1423.074879    | 127.0.0.1             | 127.0.0.1           | TCP         | 44 52587 → 50345 [ACK] Seq=1332 Ack=498054 Win=8296 Len=0                                          |
|     | 157   | 7 1465.179034  | 127.0.0.1             | 127.0.0.1           | TCP         | 66 52587 → 50345 [PSH, ACK] Seq=1332 Ack=498054 Win=8296 Len=22                                    |
|     | 157   | 1465.179086    | 127.0.0.1             | 127.0.0.1           | TCP         | 44 50345 → 52587 [ACK] Seq=498054 Ack=1354 Win=8437 Len=0                                          |
|     | 1579  | 1465.183510    | 127.0.0.1             | 127.0.0.1           | TCP         | 58 50345 → 52587 [PSH, ACK] Seq=498054 Ack=1354 Win=8437 Len=14 [TCP segment of a reassembled PDU] |
|     | 1580  | 1465.183554    | 127.0.0.1             | 127.0.0.1           | TCP         | 44 52587 → 50345 [ACK] Seq=1354 Ack=498068 Win=8296 Len=0                                          |
|     | 158   | 1465.183686    | 127.0.0.1             | 127.0.0.1           | TCP         | 47 52587 → 50345 [PSH, ACK] Seq=1354 Ack=498068 Win=8296 Len=3                                     |
|     | 158   | 1465.183711    | 127.0.0.1             | 127.0.0.1           | TCP         | 44 50345 → 52587 [ACK] Seq=498068 Ack=1357 Win=8437 Len=0                                          |
|     | 158   | 1465.184098    | 127.0.0.1             | 127.0.0.1           | TCP         | 47 50345 → 52587 [PSH, ACK] Seq=498068 Ack=1357 Win=8437 Len=3 [TCP segment of a reassembled PDU]  |
|     | 1584  | 1465.184124    | 127.0.0.1             | 127.0.0.1           | TCP         | 44 52587 → 50345 [ACK] Seq=1357 Ack=498071 Win=8296 Len=0                                          |
|     | 158   | 1465.184974    | 127.0.0.1             | 127.0.0.1           | TCP         | 53 52587 → 50345 [PSH, ACK] Seq=1357 Ack=498071 Win=8296 Len=9                                     |
| >   | Frame | 1577: 66 byte  | s on wire (528 bits). | 66 bytes captured   | (528 bits)  | on interface \Device\NPF Loopback, id 0                                                            |
|     |       | Loopback       | ` //                  | , ,                 | ` ′         |                                                                                                    |
| >   | Inter | net Protocol V | ersion 4, Src: 127.0. | 0.1, Dst: 127.0.0.1 |             |                                                                                                    |
| 00  | 00 0  | 2 00 00 00 15  | 00 00 3e 21 34 40 00  | 80 06 00 00         | E 140       |                                                                                                    |
|     |       |                | 00 00 01 cd 6b c4 a9  |                     |             |                                                                                                    |
| 00  |       |                | 18 20 68 4f 24 00 00  |                     |             |                                                                                                    |
| 00  |       |                | 65 6c 69 66 5f 64 61  |                     | .eli f_daol |                                                                                                    |
| 00  | 40 6  | f 64           |                       | od                  | _           |                                                                                                    |
|     |       |                |                       |                     |             |                                                                                                    |

Fig 25

Fig 25 shows that the command was 'DWD download\_file.txt.' But on the network, we can see that it got reversed word-by-word as 'DWD txt.elif\_doadnwod' Hence, our data is correctly encrypted.

NOTE: The wireshark dump of the above commands was very huge as I also did some other commands without saving the previous dump.

Hence, the dump provided has the information of the following commands:

**Comm 1: LS (MODE = 0)** 

Comm 2: MODE 1

Comm 3: LS

Comm 4: MODE 2

Comm 5: DWD download\_file.txt

Comm 6: UPD ex1.pnq

Comm 7: BYE (the application closes)

Therefore, the Wireshark dump verifies the correctness of the encryption in all three modes.

\*\*\*