Computer Networks Assignment 1
Bhavesh Jain 20110038

a)Source Code: https://github.com/bjain8751/ComputerNetworksA1

b)
Files:
server.py : Run the server
client.py : Run the client
utilities.py : Contains Basic functions. *Code taken from “Learning Python Network Programming”; Pg 213,214; By: Book by M. O. Faruque Sarker and Sam Washington
encryption.py : Contains functions for encrypting the message.

The RTF is built using python socket programming and uses TCP protocol. There are 5 commands which can be sent from the client side. With each command one can use three types of encryption. **The output of the command remains the same irrespective of the encryption method** as the data only remains encrypted while transfer. Once the data is received at either of the ends, it is decrypted.

**NOTE: commands are case sensitive. Must use commands in lower case.

- cwd : tells the current working directory of the server

```
Please enter your command(or quit): cwd
Server Sent:  /Users/bhaveshjain/Desktop/cna1/server
Connection Terminated
```

- ls: lists files and directories in the current directory of the server

```
Please enter your command(or quit): ls
Server Sent:  ['server.py', 'iii.jpeg', 'encryption.py', '.DS_Store', '__pycach
e__', 'ii.jpeg', 'test.txt', 'utilities.py', 'demo.mov']
Connection Terminated
```

- cd <target_directory> : changes the directory to target_directory(given that target_directory is present in the current directory)(cd .. takes us to the parent directory of the current directory)

```
Please enter your command(or quit): cd ..
Server Sent:  /Users/bhaveshjain/Desktop/cna1
Connection Terminated
```

- dwd <file>: downloads the ‘file’ to the client from the server.
    - I have implemented it in such a way that I can **download any type of file from the server (.txt, .pdf, .mov)**. The data is also transferred in the **encrypted form.**

```
Please enter your command(or quit): dwd demo.mov
Recieved:  1368    Total Recieved:  1368
Recieved:  1368    Total Recieved:  2736
Recieved:  1368    Total Recieved:  4104
```

(the RTF tells how many bytes have been received till now)

```
Recieved:  1368    Total Recieved:  88883064
Recieved:  576    Total Recieved:  88883640
Recieved:  0    Total Recieved:  88883640
```

- Code for dwd (client side)

```
elif l[0]=="dwd":
    #sending the request in enrypted mode
    if key==1:
        request=encryption.encode1(request)
    if key==2:
        request=encryption.transpose(request)
    if key==0:
        pass

    utilities.send_msg(client_socket, request)

    file=l[1]

    with open(file, 'wb') as f:
        i=0
        while(True):
            #recieving the data
            data = client_socket.recv(1368)
            i+=len(data)
            print("Recieved: ", len(data), "   Total Recieved: ", i)
            data=data.decode("ascii")

            #decrytping the data according to the key
            if key==1:
                data=encryption.decode1(data)
            if key==2:

                data=encryption.transpose(data)

            if key==0:
                pass

            c= data.encode("ascii")
            if not data:
                print("Download Complete")
                f.close()
                break
            #writing the data in file
            f.write((base64.b64decode((c))))
        f.close()
```

- Code for dwd (server side)
  We have used the base64 library. This is done to change the bytes read from the file into string and then we can use encryption on the string.

```
elif l[0]=="dwd":
    file=l[1]

    with open(file, 'rb') as f:
        i=0
        while(True):
            #reading the data from file and encoding it in base64 format.
            data = base64.b64encode(f.read(1024))
            c = data.decode("ascii")
            # Encrytping the data on the basis of the key
            if key==1:
                c=encryption.encode1(c)
            if key==2:
                c=encryption.transpose(c)
            if key==0:
                pass
            data = c.encode("ascii")
            i+=len(data)
            #sending the data
            print("Sending: ", len(data), "   Total Sent:", i  )
            if not data:
                break
            client_socket.sendall(data)

    f.close()
```

Steps for Transferring File

client requests the file-> server receives the request->server starts reading 1024 bytes from the file-> the bytes are encoded in base64 encoding-> the bytes in base64 encoding are decoded into string using ASCII -> encryption is applied to the string->the string is again encoded in bytes using ASCII ->bytes are send using the TCP->client receives the bytes in base 64 encoding-> client decodes it using ASCII into string -> client decrypts the string -> client again encodes the string in bytes using ASCII-> the bytes in base64 encoding are decoded using ‘b64decode’ -> the decoded bytes are written in file created on the client.

**A similar chain of steps is used while uploading, broadly the role of server and client are reversed.

- upd <file> : Uploads the file to the server
  - The working of the upd command is similar to the working of the dwd command which is explained above.
  - Client can upload any type of file.
  - Client can send the file using any of the encryption methods.

```
Please enter your command(or quit): upd test.txt
Sending:  8    Total Sent: 8
Sending:  0    Total Sent: 8
Upload Success
Connection Terminated
```

- Code for upd (client side)

```
elif l[0]== "upd":
    #sending the request and encrypting it with key
    if key==1:
        request=encryption.encode1(request)
    if key==2:
        request=encryption.transpose(request)
    if key==0:
        pass

    utilities.send_msg(client_socket, request)
    file=l[1]
    with open(file, 'rb') as f:
        i=0
        while(True):
            ##reading the data from file and encoding it in base64 format.
            data = base64.b64encode(f.read(1024))
            c = data.decode("ascii")
            #encryptng the data according to the key
            if key==1:
                c=encryption.encode1(c)
            if key==2:

                c=encryption.transpose(c)

            if key==0:
                pass
            data = c.encode("ascii")
            i+=len(data)
            #sending the data to the server
            print("Sending: ", len(data), "   Total Sent:", i  )
            if (not data):
                break

            client_socket.sendall(data)

    print("Upload Success")

    f.close()
```

- Code for upd(server side)

```
elif l[0]=="upd":
    file=l[1]
    with open(file, 'wb') as f:
        i=0
        while(True):
            #recieving the data in base64 encoding
            data = client_socket.recv(1368)
            i+=len(data)
            print("Recieved: ", len(data), "   Total Recieved: ", i)
            data=data.decode("ascii")
            #decrypting the data on the basis of the key
            if key==1:
                data=encryption.decode1(data)
            if key==2:
                data=encryption.transpose(data)
            if key==0:
                pass
            c= data.encode("ascii")

            if not data:
                print("Download Complete")
                f.close()
                break
            #writing the data in the file
            f.write((base64.b64decode((c))))
        f.close()
```

Working of the RTF

Client gives the integer key for encryption(0: plane-text, 1:substitute, 2:transpose) -> The key(integer) is sent to the server -> client encrypts the request and sends it to the server -> the server decrypts the request -> the server processes the requests and sends the response back in encrypted format -> The client decrypts the response.

Encryption

The RTF supports three types of encryption. Before sending the data, both client and server encrypt the data and similarly, after receiving the data both client and server decrypt the data.

- Plain Text
    - In this the data is not encrypted in any format. The data is simply transferred as it is.

- Substitute
    - This is a Caesar Cipher. I have implemented this with offset-5.
    - There are two functions described in encryption.py to allow the RTF to use this encryption scheme.(encode1 and decode1).
    - Encode1 increases each alpha-numeric character by offset while decode1 decreases each alphanumeric character by offset.

    - Code for encode1 and decode1

```
def encode1(s):
    ans=""
    for i in s:
        if(i.isalnum()): #check if character is alphanu
            if(ord(i)>=97):
                ans+=chr((ord(i)-97 +5)%26+97)
            elif(ord(i)>64):
                ans+=chr((ord(i)-65 +5)%26+65)
            else:
                ans+=chr((ord(i)-48 +5)%10+48)
        else:
            ans+=i
    return ans
def decode1(s):
    ans=""
    for i in s:
        if(i.isalnum()): #check if character is alphanu
            if(ord(i)>=97):
                ans+=chr((ord(i)-97 -5)%26+97)
            elif(ord(i)>64):
                ans+=chr((ord(i)-65 -5)%26+65)
            else:
                ans+=chr((ord(i)-48 -5)%10+48)
        else:
            ans+=i
    return ans
```

- Transpose
    - In this each word is independently reversed. Eg: “I am Bhavesh” becomes “I ma hsevahB”.
    - While transferring a file the Transpose just reverses the string obtained after base64 encoding.

** I tried to split the string obtained by decoding the base64 encoded bytes object using ASCII. I replaced the ‘e’ with space. Split the string and reverse each word. Then I reversed each word again while decrypting after transfer. Now at the other end I replaced space with ‘e’ again. However this led to loss in image data and image was distorted.

- Code for transpose

```
def transpose(s):
    if len(s)==0:#if s is empty then return empty string
        return ""
    if s.isspace():
        return s
    l=s.split()
    if len(l)==0: #if length of l is 0 then return empty string
        return ""
    if len(l)==1: #if string only contains one word, return that word.
        return s[::-1]
    ans=""
    for i in l:
        ans+=i[::-1]+" "
    return ans[0:len(ans)-1] #avoid the last space
```

Challenges Faced

- Downloading and receiving files was a challenge, especially encrypting the bytes while sending them.

** I thought that if we are able to convert bytes into a string then we can use encryption techniques. This led to the use of the base64 library.

- Setting the appropriate buffer size at the receiving end to avoid file corruption was a challenge.

Base64 implementation in program

- End A:
    - Reads 1024 bytes from file. Stores it in a bytes object (let it be A)
    - A new bytes object B is created after encoding A with base64.
    - Each byte in B can be represented by an ASCII character.
    - B is decoded into string(let it be s) using ASCII. (B.decode('ascii'))
    - Any encryption operations can be performed on s.
    - S is again encoded into bytes object K using ASCII

—- K is now sent using the TCP protocol —-

- End B:
    - K is decoded into a string s' using ASCII.
    - Corresponding Decryption operation can be performed on s'.
    - s' is encoded into bytes object P using ASCII.
    - P is decoded into bytes object Q using base64 decoding.
    - Q is now stored in the file.

WireShark Analysis

No.	Time	Source	Destination	Protocol	Length	Info
8	0.000130	127.0.0.1	127.0.0.1	TCP	56	8751 → 50236 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 W
9	0.000118	127.0.0.1	127.0.0.1	TCP	44	50236 → 8751 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
10	0.987776	127.0.0.1	127.0.0.1	TCP	46	50236 → 8751 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
11	0.000076	127.0.0.1	127.0.0.1	TCP	44	8751 → 50236 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
12	1.082559	127.0.0.1	127.0.0.1	TCP	47	50236 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=3
13	0.000071	127.0.0.1	127.0.0.1	TCP	44	8751 → 50236 [ACK] Seq=1 Ack=6 Win=2619648 Len=0
14	0.000983	127.0.0.1	127.0.0.1	TCP	232	8751 → 50236 [PSH, ACK] Seq=1 Ack=6 Win=2619648 Len=188
15	0.000043	127.0.0.1	127.0.0.1	TCP	44	50236 → 8751 [ACK] Seq=6 Ack=189 Win=2619392 Len=0
16	0.000304	127.0.0.1	127.0.0.1	TCP	44	8751 → 50236 [FIN, ACK] Seq=189 Ack=6 Win=2619648 Len=0
17	0.000022	127.0.0.1	127.0.0.1	TCP	44	50236 → 8751 [ACK] Seq=6 Ack=190 Win=2619392 Len=0
18	0.000278	127.0.0.1	127.0.0.1	TCP	44	50236 → 8751 [FIN, ACK] Seq=6 Ack=190 Win=2619392 Len=0
19	0.000114	127.0.0.1	127.0.0.1	TCP	44	8751 → 50236 [ACK] Seq=190 Ack=7 Win=2619648 Len=0

```
> Frame 12: 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
> Transmission Control Protocol, Src Port: 50236, Dst Port: 8751, Seq: 3, Ack: 1, Len: 3
> Data (3 bytes)
```

```
0000  02 00 00 00 45 00 00 2b  2b 15 40 00 80 06 00 00   ····E··+ +·@·····
0010  7f 00 00 01 7f 00 00 01  c4 3c 22 2f d6 2a 18 92   ········ ·<"/·*··
0020  59 93 0e fe 50 18 27 f9  df a0 00 00 6c 73 00      Y···P·'· ····ls·
```

ls request plaintext

No.	Time	Source	Destination	Protocol	Length	Info
8	0.000130	127.0.0.1	127.0.0.1	TCP	56	8751 → 50236 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK
9	0.000118	127.0.0.1	127.0.0.1	TCP	44	50236 → 8751 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
10	0.987776	127.0.0.1	127.0.0.1	TCP	46	50236 → 8751 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
11	0.000076	127.0.0.1	127.0.0.1	TCP	44	8751 → 50236 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
12	1.082559	127.0.0.1	127.0.0.1	TCP	47	50236 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=3
13	0.000071	127.0.0.1	127.0.0.1	TCP	44	8751 → 50236 [ACK] Seq=1 Ack=6 Win=2619648 Len=0
14	0.000983	127.0.0.1	127.0.0.1	TCP	232	8751 → 50236 [PSH, ACK] Seq=1 Ack=6 Win=2619648 Len=188
15	0.000043	127.0.0.1	127.0.0.1	TCP	44	50236 → 8751 [ACK] Seq=6 Ack=189 Win=2619392 Len=0
16	0.000304	127.0.0.1	127.0.0.1	TCP	44	8751 → 50236 [FIN, ACK] Seq=189 Ack=6 Win=2619648 Len=0
17	0.000022	127.0.0.1	127.0.0.1	TCP	44	50236 → 8751 [ACK] Seq=6 Ack=190 Win=2619392 Len=0
18	0.000278	127.0.0.1	127.0.0.1	TCP	44	50236 → 8751 [FIN, ACK] Seq=6 Ack=190 Win=2619392 Len=0
19	0.000114	127.0.0.1	127.0.0.1	TCP	44	8751 → 50236 [ACK] Seq=190 Ack=7 Win=2619648 Len=0

```
> Frame 14: 232 bytes on wire (1856 bits), 232 bytes captured (1856 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8751, Dst Port: 50236, Seq: 1, Ack: 6, Len: 188
> Data (188 bytes)
```

```
0000  02 00 00 00 45 00 00 e4  2b 17 40 00 80 06 00 00   ····E··· +·@·····
0010  7f 00 00 01 7f 00 00 01  22 2f c4 3c 59 93 0e fe   ········ "/·<Y···
0020  d6 2a 18 95 50 18 27 f9  05 66 00 00 5b 27 2e 44   ·*··P·'· ·f··['.D
0030  53 5f 53 74 6f 72 65 27  2c 20 27 2e 5f 2e 44 53   S_Store' , '._.DS
0040  5f 53 74 6f 72 65 27 2c  20 27 2e 5f 65 6e 63 72   _Store',  '._encr
0050  79 70 74 69 6f 6e 2e 70  79 27 2c 20 27 2e 5f 74   yption.p y', '._t
0060  65 73 74 2e 74 78 74 27  2c 20 27 2e 5f 75 74 69   est.txt' , '._uti
0070  6c 69 74 69 65 73 2e 70  79 27 2c 20 27 64 65 6d   lities.p y', 'dem
0080  6f 2e 6d 6f 76 27 2c 20  27 65 6e 63 72 79 70 74   o.mov',  'encrypt
0090  69 6f 6e 2e 70 79 27 2c  20 27 69 69 2e 6a 70 65   ion.py',  'ii.jpe
00a0  67 27 2c 20 27 69 69 69  2e 6a 70 65 67 27 2c 20   g', 'iii .jpeg',
00b0  27 73 65 72 76 65 72 2e  70 79 27 2c 20 27 74 65   'server. py', 'te
00c0  73 74 2e 74 78 74 27 2c  20 27 75 74 69 6c 69 74   st.txt',  'utilit
00d0  69 65 73 2e 70 79 27 2c  20 27 5f 5f 70 79 63 61   ies.py',  '__pyca
```

ls response plaintext

No.	Time	Source	Destination	Protocol	Length	Info
206	0.001005	127.0.0.1	127.0.0.1	TCP	47	61424 → 62354 [PSH, ACK] Seq=22 Ack=73 Win=10232 Len=3
207	0.000063	127.0.0.1	127.0.0.1	TCP	44	62354 → 61424 [ACK] Seq=73 Ack=25 Win=10232 Len=0
208	18.324599	127.0.0.1	127.0.0.1	TCP	46	50238 → 8751 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
209	0.000131	127.0.0.1	127.0.0.1	TCP	44	8751 → 50238 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
210	2.716157	127.0.0.1	127.0.0.1	TCP	47	50238 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=3
211	0.000055	127.0.0.1	127.0.0.1	TCP	44	8751 → 50238 [ACK] Seq=1 Ack=6 Win=2619648 Len=0
212	0.000894	127.0.0.1	127.0.0.1	TCP	232	8751 → 50238 [PSH, ACK] Seq=1 Ack=6 Win=2619648 Len=188
213	0.000069	127.0.0.1	127.0.0.1	TCP	44	50238 → 8751 [ACK] Seq=6 Ack=189 Win=2619392 Len=0
214	0.000251	127.0.0.1	127.0.0.1	TCP	44	8751 → 50238 [FIN, ACK] Seq=189 Ack=6 Win=2619648 Len=0
215	0.000035	127.0.0.1	127.0.0.1	TCP	44	50238 → 8751 [ACK] Seq=6 Ack=190 Win=2619392 Len=0
216	0.000355	127.0.0.1	127.0.0.1	TCP	44	50238 → 8751 [FIN, ACK] Seq=6 Ack=190 Win=2619392 Len=0
217	0.000086	127.0.0.1	127.0.0.1	TCP	44	8751 → 50238 [ACK] Seq=190 Ack=7 Win=2619648 Len=0

```
> Frame 210: 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
> Transmission Control Protocol, Src Port: 50238, Dst Port: 8751, Seq: 3, Ack: 1, Len: 3
> Data (3 bytes)
```

```
0000  02 00 00 00 45 00 00 2b  2b 42 40 00 80 06 00 00   ····E··+ +B@·····
0010  7f 00 00 01 7f 00 00 01  c4 3e 22 2f 0b 4e 7f 54   ········ ·>"/·N·T
0020  13 a4 a5 a1 50 18 27 f9  ec 0b 00 00 73 6c 00      ····P·'· ····sl·
```

ls becomes sl

ls request transpose

596	0.001296	127.0.0.1	127.0.0.1	TCP	232	8751 → 57977 [PSH, ACK] Seq=1 Ack=6 Win=2619648 Len=188
597	0.000071	127.0.0.1	127.0.0.1	TCP	44	57977 → 8751 [ACK] Seq=6 Ack=189 Win=2619392 Len=0
598	0.000382	127.0.0.1	127.0.0.1	TCP	44	8751 → 57977 [FIN, ACK] Seq=189 Ack=6 Win=2619648 Len=0
599	0.000048	127.0.0.1	127.0.0.1	TCP	44	57977 → 8751 [ACK] Seq=6 Ack=190 Win=2619392 Len=0
600	0.000250	127.0.0.1	127.0.0.1	TCP	44	57977 → 8751 [FIN, ACK] Seq=6 Ack=190 Win=2619392 Len=0
601	0.000056	127.0.0.1	127.0.0.1	TCP	44	8751 → 57977 [ACK] Seq=190 Ack=7 Win=2619648 Len=0
602	0.001139	127.0.0.1	127.0.0.1	TCP	56	57997 → 8751 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
603	0.000065	127.0.0.1	127.0.0.1	TCP	56	8751 → 57997 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256

```
> Frame 596: 232 bytes on wire (1856 bits), 232 bytes captured (1856 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8751, Dst Port: 57977, Seq: 1, Ack: 6, Len: 188
> Data (188 bytes)
```

```
0000  02 00 00 00 45 00 00 e4  2b ef 40 00 80 06 00 00   ····E··· +·@·····
0010  7f 00 00 01 7f 00 00 01  22 2f e2 79 c1 f6 a6 46   ········ "/·y···F
0020  b0 9b 1c fc 50 18 27 f9  75 38 00 00 2c 27 65 72   ····P·'· u8··,'er
0030  6f 74 53 5f 53 44 2e 27  5b 20 2c 27 65 72 6f 74   otS_SD.' [ ,'erot
0040  53 5f 53 44 2e 5f 2e 27  20 2c 27 79 70 2e 6e 6f   S_SD._.'  ,'yp.no
0050  69 74 70 79 72 63 6e 65  5f 2e 27 20 2c 27 74 78   itpyrcne _.' ,'tx
0060  74 2e 74 73 65 74 5f 2e  27 20 2c 27 79 70 2e 73   t.tset_. ' ,'yp.s
0070  65 69 74 69 6c 69 74 75  5f 2e 27 20 2c 27 76 6f   eitilitu _.' ,'vo
0080  6d 2e 6f 6d 65 64 27 20  2c 27 79 70 2e 6e 6f 69   m.omed'  ,'yp.noi
0090  74 70 79 72 63 6e 65 27  20 2c 27 67 65 70 6a 2e   tpyrcne'  ,'gepj.
00a0  69 69 27 20 2c 27 67 65  70 6a 2e 69 69 69 27 20   ii' ,'ge pj.iii'
00b0  2c 27 79 70 2e 72 65 76  72 65 73 27 20 2c 27 74   ,'yp.rev res' ,'t
00c0  78 74 2e 74 73 65 74 27  20 2c 27 79 70 2e 73 65   xt.tset'  ,'yp.se
00d0  69 74 69 6c 69 74 75 27  20 5d 27 5f 5f 65 68 63   itilitu'  ]'__ehc
```

the names are reversed

ls response transpose

```
1917 1.553718  127.0.0.1  127.0.0.1  TCP   47 57997 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=3
1918 0.000087  127.0.0.1  127.0.0.1  TCP   44 8751 → 57997 [ACK] Seq=1 Ack=6 Win=2619648 Len=0
1919 0.001205  127.0.0.1  127.0.0.1  TCP  232 8751 → 57997 [PSH, ACK] Seq=1 Ack=6 Win=2619648 Len=188
1920 0.000073  127.0.0.1  127.0.0.1  TCP   44 57997 → 8751 [ACK] Seq=6 Ack=189 Win=2619392 Len=0
1921 0.000350  127.0.0.1  127.0.0.1  TCP   44 8751 → 57997 [FIN, ACK] Seq=189 Ack=6 Win=2619648 Len=0

> Frame 1917: 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
> Transmission Control Protocol, Src Port: 57997, Dst Port: 8751, Seq: 3, Ack: 1, Len: 3
> Data (3 bytes)

0000  02 00 00 00 45 00 00 2b  31 08 40 00 80 06 00 00   ····E··+ 1·@·····
0010  7f 00 00 01 7f 00 00 01  e2 8d 22 2f 17 b9 9e c8   ········ ··"/····
0020  4b a5 6c 4d 50 18 27 f9  a5 24 00 00 71 78 00      K·lMP·'· ·$··qx·
```

ls increases by 5 to become qx

ls request substitute

```
1919 0.001205  127.0.0.1  127.0.0.1  TCP  232 8751 → 57997 [PSH, ACK] Seq=1 Ack=6 Win=2619648 Len=188
1920 0.000073  127.0.0.1  127.0.0.1  TCP   44 57997 → 8751 [ACK] Seq=6 Ack=189 Win=2619392 Len=0
1921 0.000350  127.0.0.1  127.0.0.1  TCP   44 8751 → 57997 [FIN, ACK] Seq=189 Ack=6 Win=2619648 Len=0

> Frame 1919: 232 bytes on wire (1856 bits), 232 bytes captured (1856 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8751, Dst Port: 57997, Seq: 1, Ack: 6, Len: 188
> Data (188 bytes)

0000  02 00 00 00 45 00 00 e4  31 0a 40 00 80 06 00 00   ····E··· 1·@·····
0010  7f 00 00 01 7f 00 00 01  22 2f e2 8d 4b a5 6c 4d   ········ "/··K·lM
0020  17 b9 9e cb 50 18 27 f9  58 7c 00 00 5b 27 2e 49   ····P·'· X|··['.I
0030  58 5f 58 79 74 77 6a 27  2c 20 27 2e 5f 2e 49 58   X_Xytwj' , '._.IX
0040  5f 58 79 74 77 6a 27 2c  20 27 2e 5f 6a 73 68 77   _Xytwj',  '._jshw
0050  64 75 79 6e 74 73 2e 75  64 27 2c 20 27 2e 5f 79   duynts.u d', '._y
0060  6a 78 79 2e 79 63 79 27  2c 20 27 2e 5f 7a 79 6e   jxy.ycy' , '._zyn
0070  71 6e 79 6e 6a 78 2e 75  64 27 2c 20 27 69 6a 72   qnynjx.u d', 'ijr
0080  74 2e 72 74 61 27 2c 20  27 6a 73 68 77 64 75 79   t.rta',  'jshwduy
0090  6e 74 73 2e 75 64 27 2c  20 27 6e 6e 2e 6f 75 6a   nts.ud',  'nn.ouj
00a0  6c 27 2c 20 27 6e 6e 6e  2e 6f 75 6a 6c 27 2c 20   l', 'nnn .oujl',
00b0  27 78 6a 77 61 6a 77 2e  75 64 27 2c 20 27 79 6a   'xjwajw. ud', 'yj
00c0  78 79 2e 79 63 79 27 2c  20 27 7a 79 6e 71 6e 79   xy.ycy',  'zynqny
00d0  6e 6a 78 2e 75 64 27 2c  20 27 5f 5f 75 64 68 66   njx.ud',  '__udhf
```

Each character is increased by 5!

ls response substitute

```
2068 3.275150  127.0.0.1  127.0.0.1  TCP  48 58031 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=327424 Len=4
2069 0.000067  127.0.0.1  127.0.0.1  TCP  44 8751 → 58031 [ACK] Seq=1 Ack=7 Win=2619648 Len=0
2070 0.000854  127.0.0.1  127.0.0.1  TCP  67 8751 → 58031 [PSH, ACK] Seq=1 Ack=7 Win=2619648 Len=23
2071 0.000052  127.0.0.1  127.0.0.1  TCP  44 58031 → 8751 [ACK] Seq=7 Ack=24 Win=2619648 Len=0
2072 0.000340  127.0.0.1  127.0.0.1  TCP  44 8751 → 58031 [FIN, ACK] Seq=24 Ack=7 Win=2619648 Len=0
2073 0.000049  127.0.0.1  127.0.0.1  TCP  44 58031 → 8751 [ACK] Seq=7 Ack=25 Win=2619648 Len=0
2074 0.000123  127.0.0.1  127.0.0.1  TCP  44 58031 → 8751 [FIN, ACK] Seq=7 Ack=25 Win=2619648 Len=0
2075 0.000052  127.0.0.1  127.0.0.1  TCP  44 8751 → 58031 [ACK] Seq=25 Ack=8 Win=2619648 Len=0

> Frame 2068: 48 bytes on wire (384 bits), 48 bytes captured (384 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 58031, Dst Port: 8751, Seq: 3, Ack: 1, Len: 4
> Data (4 bytes)
```

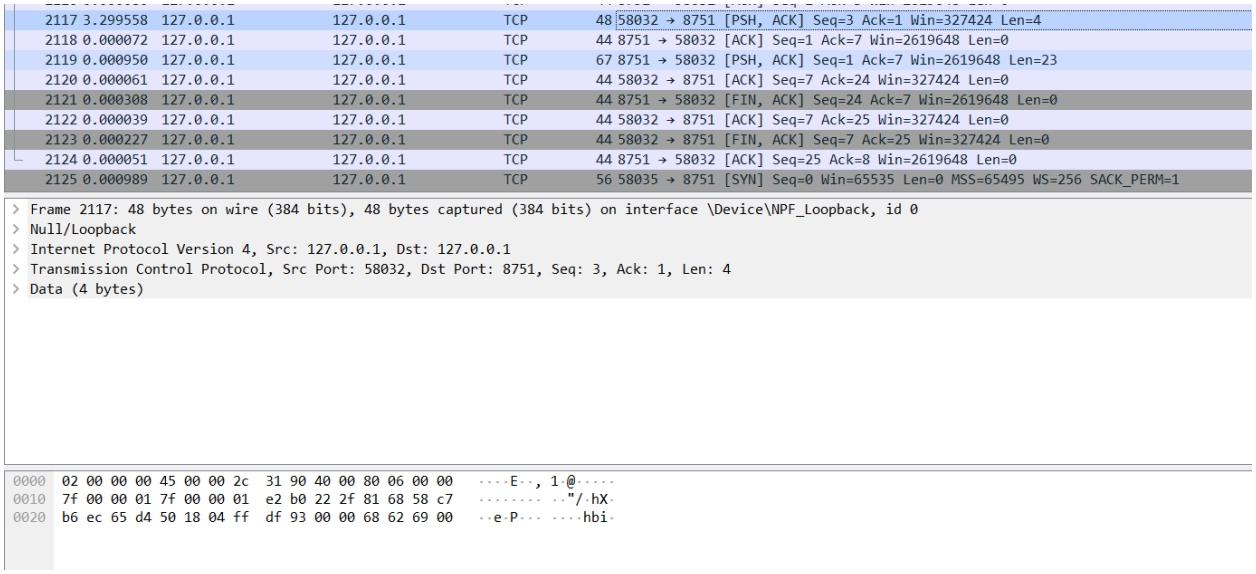
```
0000  02 00 00 00 45 00 00 2c  31 6f 40 00 80 06 00 00   ····E··, 1o@·····
0010  7f 00 00 01 7f 00 00 01  e2 af 22 2f 9f 90 7a 0f   ········ ··"/··z·
0020  e6 1c 91 67 50 18 04 ff  4f 4c 00 00 63 77 64 00   ···gP··· OL··cwd·
```

cwd request plaintext

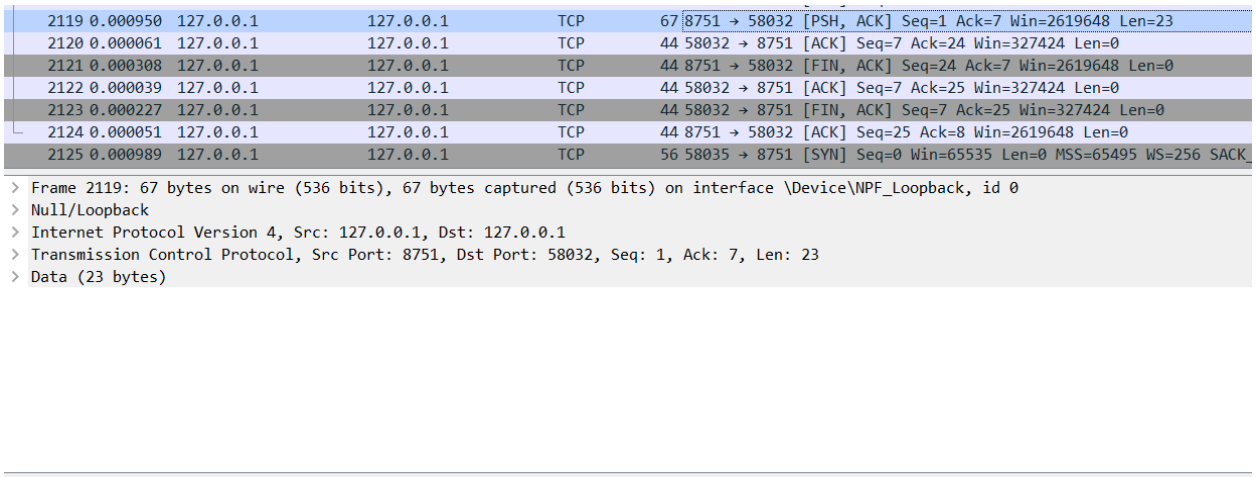
```
2070 0.000854  127.0.0.1  127.0.0.1  TCP  67 8751 → 58031 [PSH, ACK] Seq=1 Ack=7 Win=2619648 Len=23
2071 0.000052  127.0.0.1  127.0.0.1  TCP  44 58031 → 8751 [ACK] Seq=7 Ack=24 Win=2619648 Len=0
2072 0.000340  127.0.0.1  127.0.0.1  TCP  44 8751 → 58031 [FIN, ACK] Seq=24 Ack=7 Win=2619648 Len=0
2073 0.000049  127.0.0.1  127.0.0.1  TCP  44 58031 → 8751 [ACK] Seq=7 Ack=25 Win=2619648 Len=0
2074 0.000123  127.0.0.1  127.0.0.1  TCP  44 58031 → 8751 [FIN, ACK] Seq=7 Ack=25 Win=2619648 Len=0
2075 0.000052  127.0.0.1  127.0.0.1  TCP  44 8751 → 58031 [ACK] Seq=25 Ack=8 Win=2619648 Len=0

> Frame 2070: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8751, Dst Port: 58031, Seq: 1, Ack: 7, Len: 23
> Data (23 bytes)
```

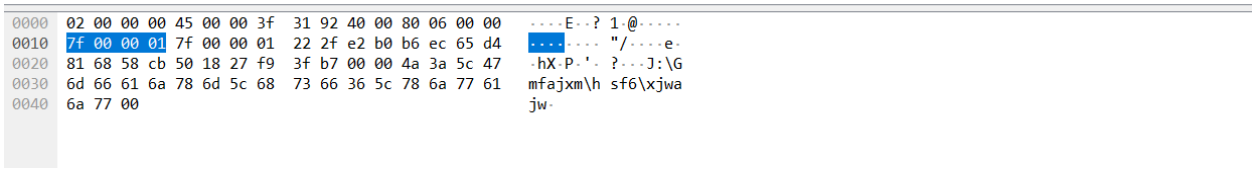
```
0000  02 00 00 00 45 00 00 3f  31 71 40 00 80 06 00 00   ····E··? 1q@·····
0010  7f 00 00 01 7f 00 00 01  22 2f e2 af e6 1c 91 67   ········ "/·····g
0020  9f 90 7a 13 50 18 27 f9  b8 97 00 00 45 3a 5c 42   ··z·P·'· ····E:\B
0030  68 61 76 65 73 68 5c 63  6e 61 31 5c 73 65 72 76   havesh\c na1\serv
0040  65 72 00                                          er·
```

cwd response plaintext



cwd request substitute





cwd response substitute

```
2190 3.509176  127.0.0.1  127.0.0.1  TCP  48 58035 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=327424 Len=4
2191 0.000085  127.0.0.1  127.0.0.1  TCP  44 8751 → 58035 [ACK] Seq=1 Ack=7 Win=2619648 Len=0
2192 0.001113  127.0.0.1  127.0.0.1  TCP  67 8751 → 58035 [PSH, ACK] Seq=1 Ack=7 Win=2619648 Len=23
2193 0.000062  127.0.0.1  127.0.0.1  TCP  44 58035 → 8751 [ACK] Seq=7 Ack=24 Win=327424 Len=0
2194 0.000405  127.0.0.1  127.0.0.1  TCP  44 8751 → 58035 [FIN, ACK] Seq=24 Ack=7 Win=2619648 Len=0
2195 0.000042  127.0.0.1  127.0.0.1  TCP  44 58035 → 8751 [ACK] Seq=7 Ack=25 Win=327424 Len=0
2196 0.000108  127.0.0.1  127.0.0.1  TCP  44 58035 → 8751 [FIN, ACK] Seq=7 Ack=25 Win=327424 Len=0
2197 0.000081  127.0.0.1  127.0.0.1  TCP  44 8751 → 58035 [ACK] Seq=25 Ack=8 Win=2619648 Len=0
```

```
> Frame 2190: 48 bytes on wire (384 bits), 48 bytes captured (384 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 58035, Dst Port: 8751, Seq: 3, Ack: 1, Len: 4
> Data (4 bytes)
```

```
0000  02 00 00 00 45 00 00 2c  31 b9 40 00 80 06 00 00   ····E··, 1·@·····
0010  7f 00 00 01 7f 00 00 01  e2 b3 22 2f 54 67 5c f7   ········ ··"/Tg\·
0020  13 9c 5f 6c 50 18 04 ff  bc 05 00 00 64 77 63 00   ··_lP··· ····dwc·
```

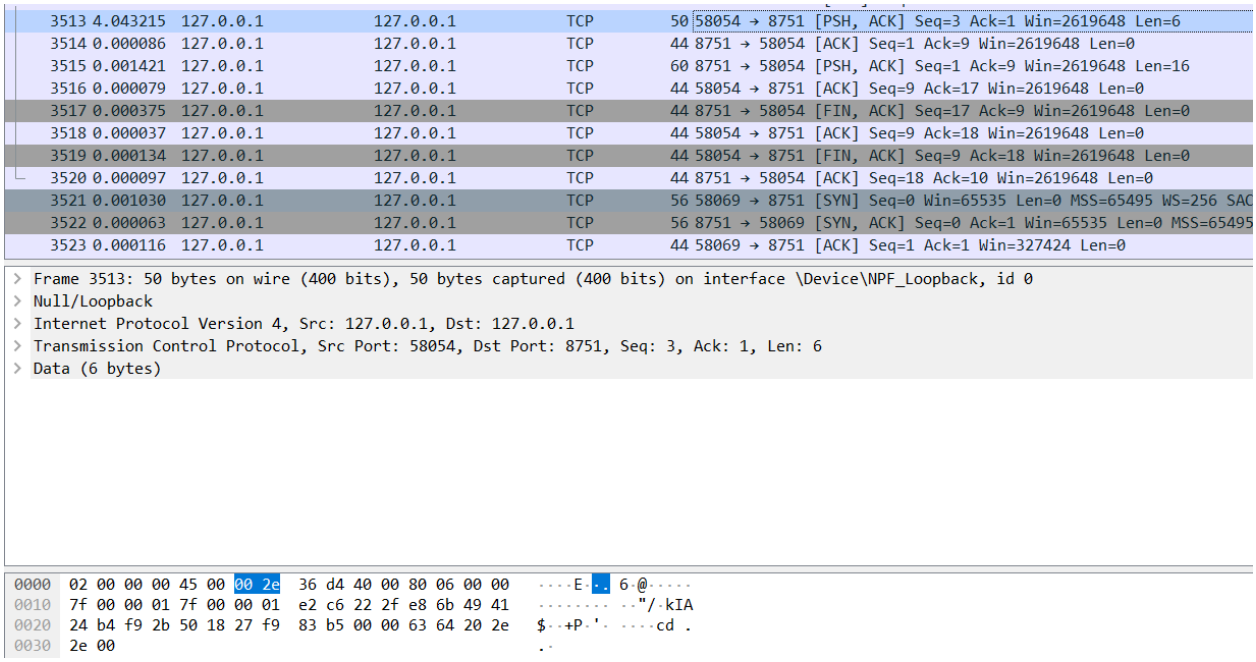
cwd transpose request

```
2191 0.000085  127.0.0.1  127.0.0.1  TCP  44 8751 → 58035 [ACK] Seq=1 Ack=7 Win=2619648 Len=0
2192 0.001113  127.0.0.1  127.0.0.1  TCP  67 8751 → 58035 [PSH, ACK] Seq=1 Ack=7 Win=2619648 Len=23
2193 0.000062  127.0.0.1  127.0.0.1  TCP  44 58035 → 8751 [ACK] Seq=7 Ack=24 Win=327424 Len=0
2194 0.000405  127.0.0.1  127.0.0.1  TCP  44 8751 → 58035 [FIN, ACK] Seq=24 Ack=7 Win=2619648 Len=0
2195 0.000042  127.0.0.1  127.0.0.1  TCP  44 58035 → 8751 [ACK] Seq=7 Ack=25 Win=327424 Len=0
2196 0.000108  127.0.0.1  127.0.0.1  TCP  44 58035 → 8751 [FIN, ACK] Seq=7 Ack=25 Win=327424 Len=0
2197 0.000081  127.0.0.1  127.0.0.1  TCP  44 8751 → 58035 [ACK] Seq=25 Ack=8 Win=2619648 Len=0
```

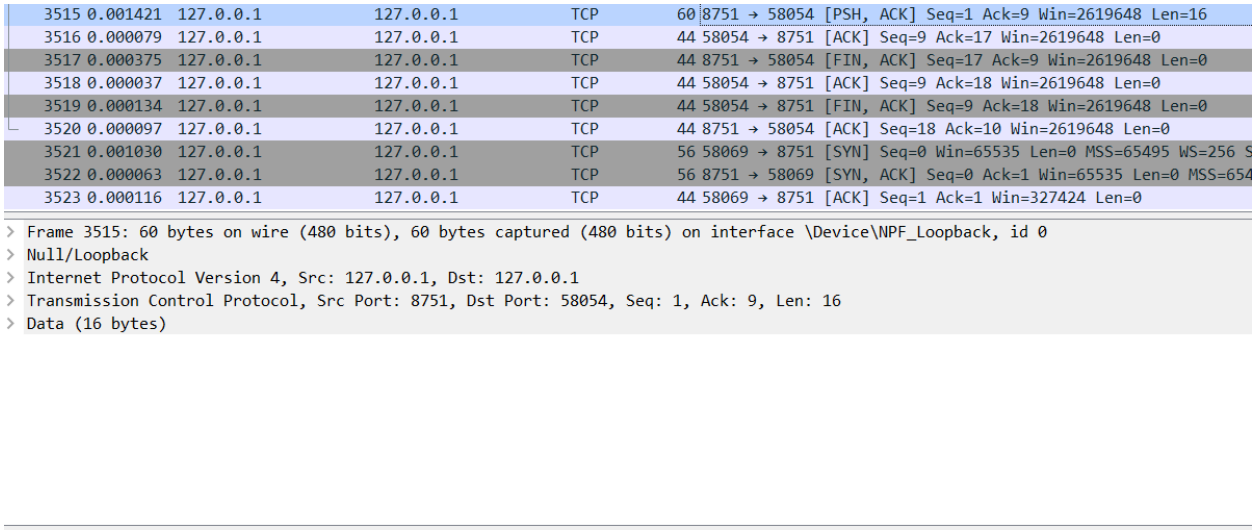
```
> Frame 2192: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8751, Dst Port: 58035, Seq: 1, Ack: 7, Len: 23
> Data (23 bytes)
```

```
0000  02 00 00 00 45 00 00 3f  31 bb 40 00 80 06 00 00   ····E··? 1·@·····
0010  7f 00 00 01 7f 00 00 01  22 2f e2 b3 13 9c 5f 6c   ········ "/····_l
0020  54 67 5c fb 50 18 27 f9  45 31 00 00 72 65 76 72   Tg\·P·'· E1··revr
0030  65 73 5c 31 61 6e 63 5c  68 73 65 76 61 68 42 5c   es\1anc\ hsevahB\
0040  3a 45 00                                          :E·
```

cwd transpose response



cd .. plaintext request



cd .. plaintext response

```
3562 5.984896  127.0.0.1  127.0.0.1  TCP  50 58069 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=327424 Len=6
3563 0.000088  127.0.0.1  127.0.0.1  TCP  44 8751 → 58069 [ACK] Seq=1 Ack=9 Win=2619648 Len=0
3564 0.001321  127.0.0.1  127.0.0.1  TCP  55 8751 → 58069 [PSH, ACK] Seq=1 Ack=9 Win=2619648 Len=11
3565 0.000074  127.0.0.1  127.0.0.1  TCP  44 58069 → 8751 [ACK] Seq=9 Ack=12 Win=327424 Len=0
3566 0.000332  127.0.0.1  127.0.0.1  TCP  44 8751 → 58069 [FIN, ACK] Seq=12 Ack=9 Win=2619648 Len=0
3567 0.000040  127.0.0.1  127.0.0.1  TCP  44 58069 → 8751 [ACK] Seq=9 Ack=13 Win=327424 Len=0
3568 0.000202  127.0.0.1  127.0.0.1  TCP  44 58069 → 8751 [FIN, ACK] Seq=9 Ack=13 Win=327424 Len=0

> Frame 3562: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 58069, Dst Port: 8751, Seq: 3, Ack: 1, Len: 6
> Data (6 bytes)

0000  02 00 00 00 45 00 00 2e  36 f5 40 00 80 06 00 00   ····E··. 6·@·····
0010  7f 00 00 01 7f 00 00 01  e2 d5 22 2f 82 26 2a b8   ········ ··"/·&*·
0020  51 d0 bb 84 50 18 04 ff  36 f5 00 00 68 69 20 2e   Q···P··· 6···hi .
0030  2e 00                                             ··
```

cd .. substitute request

```
3564 0.001321  127.0.0.1  127.0.0.1  TCP  55 8751 → 58069 [PSH, ACK] Seq=1 Ack=9 Win=2619648 Len=11
3565 0.000074  127.0.0.1  127.0.0.1  TCP  44 58069 → 8751 [ACK] Seq=9 Ack=12 Win=327424 Len=0
3566 0.000332  127.0.0.1  127.0.0.1  TCP  44 8751 → 58069 [FIN, ACK] Seq=12 Ack=9 Win=2619648 Len=0
3567 0.000040  127.0.0.1  127.0.0.1  TCP  44 58069 → 8751 [ACK] Seq=9 Ack=13 Win=327424 Len=0
3568 0.000202  127.0.0.1  127.0.0.1  TCP  44 58069 → 8751 [FIN, ACK] Seq=9 Ack=13 Win=327424 Len=0

Frame 3564: 55 bytes on wire (440 bits), 55 bytes captured (440 bits) on interface \Device\NPF_Loopback, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 8751, Dst Port: 58069, Seq: 1, Ack: 9, Len: 11
Data (11 bytes)

000  02 00 00 00 45 00 00 33  36 f7 40 00 80 06 00 00   ····E··3 6·@·····
010  7f 00 00 01 7f 00 00 01  22 2f e2 d5 51 d0 bb 84   ········ "/··Q···
020  82 26 2a be 50 18 27 f9  dc c7 00 00 4a 3a 5c 47   ·&*·P·'· ····J:\G
030  6d 66 61 6a 78 6d 00                              mfajxm·
```

cd .. substitute response

3615	3.661145	127.0.0.1	127.0.0.1	TCP	50	58073 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=6
3616	0.000099	127.0.0.1	127.0.0.1	TCP	44	8751 → 58073 [ACK] Seq=1 Ack=9 Win=2619648 Len=0
3617	0.001299	127.0.0.1	127.0.0.1	TCP	48	8751 → 58073 [PSH, ACK] Seq=1 Ack=9 Win=2619648 Len=4
3618	0.000060	127.0.0.1	127.0.0.1	TCP	44	58073 → 8751 [ACK] Seq=9 Ack=5 Win=2619648 Len=0
3619	0.000384	127.0.0.1	127.0.0.1	TCP	44	8751 → 58073 [FIN, ACK] Seq=5 Ack=9 Win=2619648 Len=0
3620	0.000040	127.0.0.1	127.0.0.1	TCP	44	58073 → 8751 [ACK] Seq=9 Ack=6 Win=2619648 Len=0
3621	0.000145	127.0.0.1	127.0.0.1	TCP	44	58073 → 8751 [FIN, ACK] Seq=9 Ack=6 Win=2619648 Len=0
3622	0.000088	127.0.0.1	127.0.0.1	TCP	44	8751 → 58073 [ACK] Seq=6 Ack=10 Win=2619648 Len=0

```
Frame 3615: 50 bytes on wire (400 bits), 50 bytes captured (400 bits) on interface \Device\NPF_Loopback, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 58073, Dst Port: 8751, Seq: 3, Ack: 1, Len: 6
Data (6 bytes)
```

```
000  02 00 00 00 45 00 00 2e  37 1a 40 00 80 06 00 00   ····E···  7·@·····
010  7f 00 00 01 7f 00 00 01  e2 d9 22 2f 1c 39 84 5e   ········  ··"/·9·^
020  d0 30 1e 7f 50 18 27 f9  42 e9 00 00 64 63 20 2e   ·0··P·'·  B···dc .
030  2e 00                                              ..
```

cd .. transpose request

3617	0.001299	127.0.0.1	127.0.0.1	TCP	48	8751 → 58073 [PSH, ACK] Seq=1 Ack=9 Win=2619648 Len=4
3618	0.000060	127.0.0.1	127.0.0.1	TCP	44	58073 → 8751 [ACK] Seq=9 Ack=5 Win=2619648 Len=0
3619	0.000384	127.0.0.1	127.0.0.1	TCP	44	8751 → 58073 [FIN, ACK] Seq=5 Ack=9 Win=2619648 Len=0
3620	0.000040	127.0.0.1	127.0.0.1	TCP	44	58073 → 8751 [ACK] Seq=9 Ack=6 Win=2619648 Len=0
3621	0.000145	127.0.0.1	127.0.0.1	TCP	44	58073 → 8751 [FIN, ACK] Seq=9 Ack=6 Win=2619648 Len=0
3622	0.000088	127.0.0.1	127.0.0.1	TCP	44	8751 → 58073 [ACK] Seq=6 Ack=10 Win=2619648 Len=0

```
rame 3617: 48 bytes on wire (384 bits), 48 bytes captured (384 bits) on interface \Device\NPF_Loopback, id 0
ull/Loopback
nternet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
ransmission Control Protocol, Src Port: 8751, Dst Port: 58073, Seq: 1, Ack: 9, Len: 4
ata (4 bytes)
```

```
0  02 00 00 00 45 00 00 2c  37 1c 40 00 80 06 00 00   ····E··,  7·@·····
0  7f 00 00 01 7f 00 00 01  22 2f e2 d9 d0 30 1e 7f   ········  "/···0··
0  1c 39 84 64 50 18 27 f9  54 3c 00 00 5c 3a 45 00   ·9·dP·'·  T<··\:E·
```

cd .. transpose response

```
3719 11.215329 127.0.0.1        127.0.0.1        TCP      57 58080 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=327424 Len=13

> Frame 3719: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 58080, Dst Port: 8751, Seq: 3, Ack: 1, Len: 13
> Data (13 bytes)
```

```
0000  02 00 00 00 45 00 00 35  37 4d 40 00 80 06 00 00   ····E··5 7M@·····
0010  7f 00 00 01 7f 00 00 01  e2 e0 22 2f d1 fb 03 df   ········ ··"/····
0020  9e 53 1f 7b 50 18 04 ff  98 04 00 00 75 70 64 20   ·S·{P··· ····upd
0030  69 69 69 2e 6a 70 65 67  00                       iii.jpeg ·
```

upd plain text request

```
3743 0.002559  127.0.0.1  127.0.0.1  TCP  1308 58080 → 8751 [PSH, ACK] Seq=15064 Ack=1 Win=327424 Len=1264
3744 0.000163  127.0.0.1  127.0.0.1  TCP    44 8751 → 58080 [ACK] Seq=1 Ack=16328 Win=2603264 Len=0
3745 0.003164  127.0.0.1  127.0.0.1  TCP    44 58080 → 8751 [FIN, ACK] Seq=16328 Ack=1 Win=327424 Len=0
3746 0.000146  127.0.0.1  127.0.0.1  TCP    44 8751 → 58080 [ACK] Seq=1 Ack=16329 Win=2603264 Len=0
3747 0.002633  127.0.0.1  127.0.0.1  TCP    56 58090 → 8751 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_
3748 0.000218  127.0.0.1  127.0.0.1  TCP    56 8751 → 58090 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 W
3749 0.000237  127.0.0.1  127.0.0.1  TCP    44 58090 → 8751 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
3750 0.001490  127.0.0.1  127.0.0.1  TCP    44 8751 → 58080 [FIN, ACK] Seq=1 Ack=16329 Win=2603264 Len=0
3751 0.000153  127.0.0.1  127.0.0.1  TCP    44 58080 → 8751 [ACK] Seq=16329 Ack=2 Win=2619648 Len=0

> Frame 3743: 1308 bytes on wire (10464 bits), 1308 bytes captured (10464 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 58080, Dst Port: 8751, Seq: 15064, Ack: 1, Len: 1264
> Data (1264 bytes)
```

```
0000  02 00 00 00 45 00 05 18  37 65 40 00 80 06 00 00   ····E··· 7e@·····
0010  7f 00 00 01 7f 00 00 01  e2 e0 22 2f d1 fb 3e b4   ········ ··"/··>·
0020  9e 53 1f 7b 50 18 04 ff  0c 86 00 00 44 6f 77 6e   ·S·{P··· ····Down
0030  6c 6f 61 64 47 52 79 42  6c 77 63 4f 67 70 2b 66   loadGRyB lwcOgp+f
0040  6e 2b 67 34 5a 41 48 6e  7a 35 2f 48 36 6d 2b 2f   n+g4ZAHn z5/H6m+/
0050  77 63 70 56 58 79 4d 7a  4d 31 4e 30 48 41 49 4c   wcpVXyMz M1N0HAIL
0060  30 43 5a 31 36 78 61 4f  66 6e 33 37 6f 63 38 4c   0CZ16xaO fn37oc8L
0070  4c 33 4b 76 30 4d 37 70  39 58 70 73 32 50 67 39   L3Kv0M7p 9Xps2Pg9
0080  31 71 31 66 78 34 2b 7a  32 43 41 57 6f 41 31 7a   1q1fx4+z 2CAWoA1z
0090  64 33 66 48 63 38 38 2b  68 39 36 39 6e 30 48 50   d3fHc88+ h969n0HP
00a0  48 6a 31 46 78 36 45 4b  69 4e 6f 5a 68 61 31 62   Hj1Fx6EK iNoZha1b
00b0  66 38 53 6d 7a 5a 74 77  36 35 62 63 74 2b 57 30   f8SmzZtw 65bct+W0
00c0  5a 53 78 41 4f 2b 48 68  34 59 45 65 54 2f 52 41   ZSxAO+Hh 4YEeT/RA
00d0  65 48 68 33 50 50 62 59  34 35 71 2f 63 62 75 39   eHh3PPbY 45q/cbu9
```

upd plain text response

```
3798 0.000059  127.0.0.1  127.0.0.1  TCP  44 8751 → 58090 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
3799 5.572201  127.0.0.1  127.0.0.1  TCP  57 58090 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
3800 0.000078  127.0.0.1  127.0.0.1  TCP  44 8751 → 58090 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
3801 0.002531  127.0.0.1  127.0.0.1  TCP  1412 58090 → 8751 [PSH, ACK] Seq=16 Ack=1 Win=2619648 Len=1368
3802 0.000070  127.0.0.1  127.0.0.1  TCP  44 8751 → 58090 [ACK] Seq=1 Ack=1384 Win=2618368 Len=0
3803 0.001586  127.0.0.1  127.0.0.1  TCP  1412 58090 → 8751 [PSH, ACK] Seq=1384 Ack=1 Win=2619648 Len=1368
3804 0.000055  127.0.0.1  127.0.0.1  TCP  44 8751 → 58090 [ACK] Seq=1 Ack=2752 Win=2616832 Len=0
3805 0.001850  127.0.0.1  127.0.0.1  TCP  1412 58090 → 8751 [PSH, ACK] Seq=2752 Ack=1 Win=2619648 Len=1368

Frame 3799: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface \Device\NPF_Loopback, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 58090, Dst Port: 8751, Seq: 3, Ack: 1, Len: 13
Data (13 bytes)
```

```
000  02 00 00 00 45 00 00 35  37 84 40 00 80 06 00 00   ····E··5 7·@·····
010  7f 00 00 01 7f 00 00 01  e2 ea 22 2f be bc da 72   ········ ··"/···r
020  49 07 1f ae 50 18 27 f9  e8 b0 00 00 7a 75 69 20   I···P·'· ····zui
030  6e 6e 6e 2e 6f 75 6a 6c  00                       nnn.oujl ·
```

upd becomes zui

upd substitute request

```
3823 0.001544  127.0.0.1  127.0.0.1  TCP  1308 58090 → 8751 [PSH, ACK] Seq=15064 Ack=1 Win=2619648 Len=1264
3824 0.000037  127.0.0.1  127.0.0.1  TCP  44 8751 → 58090 [ACK] Seq=1 Ack=16328 Win=2603264 Len=0
3825 0.001022  127.0.0.1  127.0.0.1  TCP  44 58090 → 8751 [FIN, ACK] Seq=16328 Ack=1 Win=2619648 Len=0
3826 0.000037  127.0.0.1  127.0.0.1  TCP  44 8751 → 58090 [ACK] Seq=1 Ack=16329 Win=2603264 Len=0

Frame 3823: 1308 bytes on wire (10464 bits), 1308 bytes captured (10464 bits) on interface \Device\NPF_Loopback, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 58090, Dst Port: 8751, Seq: 15064, Ack: 1, Len: 1264
Data (1264 bytes)
```

```
000  02 00 00 00 45 00 05 18  37 9c 40 00 80 06 00 00   ····E··· 7·@·····
010  7f 00 00 01 7f 00 00 01  e2 ea 22 2f be bd 15 47   ········ ··"/···G
020  49 07 1f ae 50 18 27 f9  37 b7 00 00 49 74 62 73   I···P·'· 7···Itbs
030  71 74 66 69 4c 57 64 47  71 62 68 54 6c 75 2b 6b   qtfiLWdG qbhTlu+k
040  73 2b 6c 39 45 46 4d 73  65 30 2f 4d 31 72 2b 2f   s+l9EFMs e0/M1r+/
050  62 68 75 41 43 64 52 65  52 36 53 35 4d 46 4e 51   bhuACdRe R6S5MFNQ
060  35 48 45 36 31 63 66 54  6b 73 38 32 74 68 33 51   5HE61cfT ks82th3Q
070  51 38 50 61 35 52 32 75  34 43 75 78 37 55 6c 34   Q8Pa5R2u 4Cux7Ul4
080  36 76 36 6b 63 39 2b 65  37 48 46 42 74 46 36 65   6v6kc9+e 7HFBtF6e
090  69 38 6b 4d 68 33 33 2b  6d 34 31 34 73 35 4d 55   i8kMh33+ m414s5MU
0a0  4d 6f 36 4b 63 31 4a 50  6e 53 74 45 6d 66 36 67   Mo6Kc1JP nStEmf6g
0b0  6b 33 58 72 65 45 79 62  31 30 67 68 79 2b 42 35   k3XreEyb 10ghy+B5
0c0  45 58 63 46 54 2b 4d 6d  39 44 4a 6a 59 2f 57 46   EXcFT+Mm 9DJjY/WF
0d0  6a 4d 6d 38 55 55 67 44  39 30 76 2f 68 67 7a 34   jMm8UUgD 90v/hgz4
```

Each char in string encoding(base64) is increased by 5. In this way any file can be encrypted

upd substitute response

3898	12.150077	127.0.0.1	127.0.0.1	TCP	57	61080 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
3899	0.000090	127.0.0.1	127.0.0.1	TCP	44	8751 → 61080 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
3900	0.001439	127.0.0.1	127.0.0.1	TCP	1412	61080 → 8751 [PSH, ACK] Seq=16 Ack=1 Win=2619648 Len=1368
3901	0.000090	127.0.0.1	127.0.0.1	TCP	44	8751 → 61080 [ACK] Seq=1 Ack=1384 Win=2618368 Len=0
3902	0.000736	127.0.0.1	127.0.0.1	TCP	1412	61080 → 8751 [PSH, ACK] Seq=1384 Ack=1 Win=2619648 Len=1368
3903	0.000041	127.0.0.1	127.0.0.1	TCP	44	8751 → 61080 [ACK] Seq=1 Ack=2752 Win=2616832 Len=0
3904	0.000826	127.0.0.1	127.0.0.1	TCP	1412	61080 → 8751 [PSH, ACK] Seq=2752 Ack=1 Win=2619648 Len=1368
3905	0.000053	127.0.0.1	127.0.0.1	TCP	44	8751 → 61080 [ACK] Seq=1 Ack=4120 Win=2615552 Len=0

```
Frame 3898: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface \Device\NPF_Loopback, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 61080, Dst Port: 8751, Seq: 3, Ack: 1, Len: 13
Data (13 bytes)
```

```
0000  02 00 00 00 45 00 00 35  37 c7 40 00 80 06 00 00   ····E··5 7·@·····
0010  7f 00 00 01 7f 00 00 01  ee 98 22 2f aa 50 6a dd   ········ ··"/·Pj·
0020  c8 25 0f 35 50 18 27 f9  43 40 00 00 64 70 75 20   ·%·5P·'· C@··dpu
0030  67 65 70 6a 2e 69 69 69  00                       gepj.iii ·
```

words reversed

upd transpose request

3922	0.000953	127.0.0.1	127.0.0.1	TCP	1308	61080 → 8751 [PSH, ACK] Seq=15064 Ack=1 Win=2619648 Len=1264
3923	0.000042	127.0.0.1	127.0.0.1	TCP	44	8751 → 61080 [ACK] Seq=1 Ack=16328 Win=2603264 Len=0
3924	0.001203	127.0.0.1	127.0.0.1	TCP	44	61080 → 8751 [FIN, ACK] Seq=16328 Ack=1 Win=2619648 Len=0
3925	0.000055	127.0.0.1	127.0.0.1	TCP	44	8751 → 61080 [ACK] Seq=1 Ack=16329 Win=2603264 Len=0
3926	0.001016	127.0.0.1	127.0.0.1	TCP	56	61087 → 8751 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM

```
Frame 3922: 1308 bytes on wire (10464 bits), 1308 bytes captured (10464 bits) on interface \Device\NPF_Loopback, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 61080, Dst Port: 8751, Seq: 15064, Ack: 1, Len: 1264
Data (1264 bytes)
```

```
0000  02 00 00 00 45 00 05 18  37 df 40 00 80 06 00 00   ····E··· 7·@·····
0010  7f 00 00 01 7f 00 00 01  ee 98 22 2f aa 50 a5 b2   ········ ··"/·P··
0020  c8 25 0f 35 50 18 27 f9  85 f3 00 00 3d 3d 67 67   ·%·5P·'· ····==gg
0030  67 4a 6b 72 45 35 55 52  4a 42 41 41 41 41 67 48   gJkrE5UR JBAAAAgH
0040  45 6c 41 45 68 38 47 45  54 39 58 39 6b 69 49 6b   ElAEh8GE T9X9kiIk
0050  4c 59 68 6b 69 41 45 4c  61 68 55 69 41 45 62 61   LYhkiAEL ahUiAEba
0060  69 51 69 41 46 54 4b 69  51 75 67 46 53 4b 43 51   iQiAFTKi QugFSKCQ
0070  73 6f 46 53 4a 43 51 73  70 4a 43 4a 43 55 4d 70   soFSJCQs pJCJCUMp
0080  49 43 35 43 57 49 70 49  41 78 69 57 49 6c 49 41   IC5CWIpI AxiWIlIA
0090  78 6d 6d 49 6b 49 51 78  6b 69 49 6b 4c 59 68 6b   xmmIkIQx kiIkLYhk
00a0  69 41 45 4c 61 68 55 69  41 45 62 61 69 51 69 41   iAELahUi AEbaiQiA
00b0  46 7a 45 69 4a 47 6f 44  6d 58 70 4d 69 51 79 41   FzEiJGoD mXpMiQyA
00c0  64 32 4d 45 4e 4a 2f 61  58 74 61 31 44 4f 35 6b   d2MENJ/a Xta1DO5k
00d0  51 61 47 52 41 4f 50 79  2b 38 77 67 43 4c 76 38   QaGRAOPy +8wgCLv8
```

base64 encoded strings end with "==".
here our string starts with "==" which shows that the overall string has reversed.(whole string does not contain spaces and is treated as one word)

upd transpose response

No.	Time	Source	Destination	Protocol	Length	Info
309	0.000168	127.0.0.1	127.0.0.1	TCP	44	62354 → 61424 [ACK] Seq=109 Ack=37 Win=10232 Len=0
310	25.006503	127.0.0.1	127.0.0.1	TCP	53	62354 → 61424 [PSH, ACK] Seq=109 Ack=37 Win=10232 Len=9
311	0.000046	127.0.0.1	127.0.0.1	TCP	44	61424 → 62354 [ACK] Seq=37 Ack=118 Win=10232 Len=0
312	0.001039	127.0.0.1	127.0.0.1	TCP	47	61424 → 62354 [PSH, ACK] Seq=37 Ack=118 Win=10232 Len=3
313	0.000072	127.0.0.1	127.0.0.1	TCP	44	62354 → 61424 [ACK] Seq=118 Ack=40 Win=10232 Len=0
314	11.119084	127.0.0.1	127.0.0.1	TCP	46	50265 → 8751 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
315	0.000123	127.0.0.1	127.0.0.1	TCP	44	8751 → 50265 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
316	8.117407	127.0.0.1	127.0.0.1	TCP	57	50265 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
317	0.000056	127.0.0.1	127.0.0.1	TCP	44	8751 → 50265 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
318	0.001355	127.0.0.1	127.0.0.1	TCP	1412	8751 → 50265 [PSH, ACK] Seq=1 Ack=16 Win=2619648 Len=1368
319	0.000071	127.0.0.1	127.0.0.1	TCP	44	50265 → 8751 [ACK] Seq=16 Ack=1369 Win=2618368 Len=0
320	0.000680	127.0.0.1	127.0.0.1	TCP	1412	8751 → 50265 [PSH, ACK] Seq=1369 Ack=16 Win=2619648 Len=1368

```
> Frame 316: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 50265, Dst Port: 8751, Seq: 3, Ack: 1, Len: 13
> Data (13 bytes)
```

```
0000  02 00 00 00 45 00 00 35  2b 63 40 00 80 06 00 00   ····E··5 +c@·····
0010  7f 00 00 01 7f 00 00 01  c4 59 22 2f 9c 23 49 4f   ········ ·Y"/·#IO
0020  94 d5 49 73 50 18 27 f9  74 78 00 00 64 77 64 20   ··IsP·'· tx··dwd
0030  69 69 69 2e 6a 70 65 67  00                       iii.jpeg ·
```

dwd plaintext request

No.	Time	Source	Destination	Protocol	Length	Info
331	0.000045	127.0.0.1	127.0.0.1	TCP	44	50265 → 8751 [ACK] Seq=16 Ack=9577 Win=2610176 Len=0
332	0.000550	127.0.0.1	127.0.0.1	TCP	1412	8751 → 50265 [PSH, ACK] Seq=9577 Ack=16 Win=2619648 Len=1368
333	0.000031	127.0.0.1	127.0.0.1	TCP	44	50265 → 8751 [ACK] Seq=16 Ack=10945 Win=2608640 Len=0
334	0.000495	127.0.0.1	127.0.0.1	TCP	1412	8751 → 50265 [PSH, ACK] Seq=10945 Ack=16 Win=2619648 Len=1368
335	0.000044	127.0.0.1	127.0.0.1	TCP	44	50265 → 8751 [ACK] Seq=16 Ack=12313 Win=2607360 Len=0
336	0.000660	127.0.0.1	127.0.0.1	TCP	1412	8751 → 50265 [PSH, ACK] Seq=12313 Ack=16 Win=2619648 Len=1368
337	0.000040	127.0.0.1	127.0.0.1	TCP	44	50265 → 8751 [ACK] Seq=16 Ack=13681 Win=2606080 Len=0
338	0.000925	127.0.0.1	127.0.0.1	TCP	1412	8751 → 50265 [PSH, ACK] Seq=13681 Ack=16 Win=2619648 Len=1368
339	0.000038	127.0.0.1	127.0.0.1	TCP	44	50265 → 8751 [ACK] Seq=16 Ack=15049 Win=2604544 Len=0
340	0.000563	127.0.0.1	127.0.0.1	TCP	1308	8751 → 50265 [PSH, ACK] Seq=15049 Ack=16 Win=2619648 Len=1264
341	0.000039	127.0.0.1	127.0.0.1	TCP	44	50265 → 8751 [ACK] Seq=16 Ack=16313 Win=2603264 Len=0
342	0.000978	127.0.0.1	127.0.0.1	TCP	44	8751 → 50265 [FIN, ACK] Seq=16313 Ack=16 Win=2619648 Len=0

```
> Frame 340: 1308 bytes on wire (10464 bits), 1308 bytes captured (10464 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8751, Dst Port: 50265, Seq: 15049, Ack: 16, Len: 1264
> Data (1264 bytes)
```

```
0000  02 00 00 00 45 00 05 18  2b 7b 40 00 80 06 00 00   ····E··· +{@·····
0010  7f 00 00 01 7f 00 00 01  22 2f c4 59 94 d5 84 3b   ········ "/·Y···;
0020  9c 23 49 5c 50 18 27 f9  d8 00 00 00 44 6f 77 6e   ·#I\P·'· ····Down
0030  6c 6f 61 64 47 52 79 42  6c 77 63 4f 67 70 2b 66   loadGRyB lwcOgp+f
0040  6e 2b 67 34 5a 41 48 6e  7a 35 2f 48 36 6d 2b 2f   n+g4ZAHn z5/H6m+/
0050  77 63 70 56 58 79 4d 7a  4d 31 4e 30 48 41 49 4c   wcpVXyMz M1N0HAIL
0060  30 43 5a 31 36 78 61 4f  66 6e 33 37 6f 63 38 4c   0CZ16xaO fn37oc8L
0070  4c 33 4b 76 30 4d 37 70  39 58 70 73 32 50 67 39   L3Kv0M7p 9Xps2Pg9
0080  31 71 31 66 78 34 2b 7a  32 43 41 57 6f 41 31 7a   1q1fx4+z 2CAWoA1z
0090  64 33 66 48 63 38 38 2b  68 39 36 39 6e 30 48 50   d3fHc88+ h969n0HP
00a0  48 6a 31 46 78 36 45 4b  69 4e 6f 5a 68 61 31 62   Hj1Fx6EK iNoZha1b
00b0  66 38 53 6d 7a 5a 74 77  36 35 62 63 74 2b 57 30   f8SmzZtw 65bct+W0
00c0  5a 53 78 41 4f 2b 48 68  34 59 45 65 54 2f 52 41   ZSxAO+Hh 4YEeT/RA
00d0  65 48 68 33 50 50 62 59  34 35 71 2f 63 62 75 39   eHh3PPbY 45q/cbu9
```

dwd plaintext response

```
4006 1.644161  127.0.0.1  127.0.0.1  TCP  57  61087 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
4007 0.000094  127.0.0.1  127.0.0.1  TCP  44  8751 → 61087 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
4008 0.011723  127.0.0.1  127.0.0.1  TCP  1412  8751 → 61087 [PSH, ACK] Seq=1 Ack=16 Win=2619648 Len=1368
4009 0.000067  127.0.0.1  127.0.0.1  TCP  44  61087 → 8751 [ACK] Seq=16 Ack=1369 Win=2618368 Len=0
4010 0.001608  127.0.0.1  127.0.0.1  TCP  1412  8751 → 61087 [PSH, ACK] Seq=1369 Ack=16 Win=2619648 Len=1368
4011 0.000053  127.0.0.1  127.0.0.1  TCP  44  61087 → 8751 [ACK] Seq=16 Ack=2737 Win=2616832 Len=0

Frame 4006: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface \Device\NPF_Loopback, id 0
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
Transmission Control Protocol, Src Port: 61087, Dst Port: 8751, Seq: 3, Ack: 1, Len: 13
Data (13 bytes)
   Data: 696269206e6e6e2e6f756a6c00
   [Length: 13]

000  02 00 00 00 45 00 00 35  38 12 40 00 80 06 00 00   ····E··5 8·@·····
010  7f 00 00 01 7f 00 00 01  ee 9f 22 2f 52 4c 50 1c   ········ ··"/RLP·
020  7e b9 ec 44 50 18 27 f9  e2 8c 00 00 69 62 69 20   ~··DP·'· ····ibi
030  6e 6e 6e 2e 6f 75 6a 6c  00                       nnn.oujl ·
```

dwd substitute request

```
4030 0.001805  127.0.0.1  127.0.0.1  TCP  1308  8751 → 61087 [PSH, ACK] Seq=15049 Ack=16 Win=2619648 Len=1264
4031 0.000051  127.0.0.1  127.0.0.1  TCP  44  61087 → 8751 [ACK] Seq=16 Ack=16313 Win=2603264 Len=0
4032 0.001143  127.0.0.1  127.0.0.1  TCP  44  8751 → 61087 [FIN, ACK] Seq=16313 Ack=16 Win=2619648 Len=0
4033 0.000048  127.0.0.1  127.0.0.1  TCP  44  61087 → 8751 [ACK] Seq=16 Ack=16314 Win=2603264 Len=0

> Frame 4030: 1308 bytes on wire (10464 bits), 1308 bytes captured (10464 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8751, Dst Port: 61087, Seq: 15049, Ack: 16, Len: 1264
v Data (1264 bytes)
    Data: 49746273717466694c576447716268546c752b6b732b6c3945464d7365302f4d31722b2f…
    [Length: 1264]

0020  52 4c 50 29 50 18 27 f9  20 80 00 00 49 74 62 73   RLP)P·'· ···Itbs
0030  71 74 66 69 4c 57 64 47  71 62 68 54 6c 75 2b 6b   qtfiLWdG qbhTlu+k
0040  73 2b 6c 39 45 46 4d 73  65 30 2f 4d 31 72 2b 2f   s+l9EFMs e0/M1r+/
0050  62 68 75 41 43 64 52 65  52 36 53 35 4d 46 4e 51   bhuACdRe R6S5MFNQ
0060  35 48 45 36 31 63 66 54  6b 73 38 32 74 68 33 51   5HE61cfT ks82th3Q
0070  51 38 50 61 35 52 32 75  34 43 75 78 37 55 6c 34   Q8Pa5R2u 4Cux7Ul4
0080  36 76 36 6b 63 39 2b 65  37 48 46 42 74 46 36 65   6v6kc9+e 7HFBtF6e
0090  69 38 6b 4d 68 33 33 2b  6d 34 31 34 73 35 4d 55   i8kMh33+ m414s5MU
00a0  4d 6f 36 4b 63 31 4a 50  6e 53 74 45 6d 66 36 67   Mo6Kc1JP nStEmf6g
00b0  6b 33 58 72 65 45 79 62  31 30 67 68 79 2b 42 35   k3XreEyb 10ghy+B5
00c0  45 58 63 46 54 2b 4d 6d  39 44 4a 6a 59 2f 57 46   EXcFT+Mm 9DJjY/WF
00d0  6a 4d 6d 38 55 55 67 44  39 30 76 2f 68 67 7a 34   jMm8UUgD 90v/hgz4
00e0  58 5a 79 55 62 2b 32 69  61 37 49 43 77 75 2b 63   XZyUb+2i a7ICwu+c
00f0  33 31 6a 69 61 49 64 41  73 42 46 47 37 76 72 56   31jiaIdA sBFG7vrV
```

dwd substitute response

No.	Time	Source	Destination	Protocol	Length	Info
380	0.000084	127.0.0.1	127.0.0.1	TCP	44	62354 → 61424 [ACK] Seq=154 Ack=52 Win=10232 Len=0
381	25.009642	127.0.0.1	127.0.0.1	TCP	53	62354 → 61424 [PSH, ACK] Seq=154 Ack=52 Win=10232 Len=9
382	0.000052	127.0.0.1	127.0.0.1	TCP	44	61424 → 62354 [ACK] Seq=52 Ack=163 Win=10232 Len=0
383	0.000746	127.0.0.1	127.0.0.1	TCP	47	61424 → 62354 [PSH, ACK] Seq=52 Ack=163 Win=10232 Len=3
384	0.000058	127.0.0.1	127.0.0.1	TCP	44	62354 → 61424 [ACK] Seq=163 Ack=55 Win=10232 Len=0
385	14.617030	127.0.0.1	127.0.0.1	TCP	46	57965 → 8751 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
386	0.000090	127.0.0.1	127.0.0.1	TCP	44	8751 → 57965 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
387	6.723416	127.0.0.1	127.0.0.1	TCP	57	57965 → 8751 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
388	0.000066	127.0.0.1	127.0.0.1	TCP	44	8751 → 57965 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
389	0.006144	127.0.0.1	127.0.0.1	TCP	1412	8751 → 57965 [PSH, ACK] Seq=1 Ack=16 Win=2619648 Len=1368
390	0.000068	127.0.0.1	127.0.0.1	TCP	44	57965 → 8751 [ACK] Seq=16 Ack=1369 Win=2618368 Len=0
391	0.000798	127.0.0.1	127.0.0.1	TCP	1412	8751 → 57965 [PSH, ACK] Seq=1369 Ack=16 Win=2619648 Len=1368

```
> Frame 387: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 57965, Dst Port: 8751, Seq: 3, Ack: 1, Len: 13
> Data (13 bytes)
```

```
0000  02 00 00 00 45 00 00 35  2b 9a 40 00 80 06 00 00   ····E··5 +·@·····
0010  7f 00 00 01 7f 00 00 01  e2 6d 22 2f 6a b9 b6 3b   ········ ·m"/j··;
0020  6a be 83 4f 50 18 27 f9  3d ea 00 00 64 77 64 20   j··OP·'· =···dwd
0030  67 65 70 6a 2e 69 69 69  00                       gepj.iii ·
```

dwd transpose request

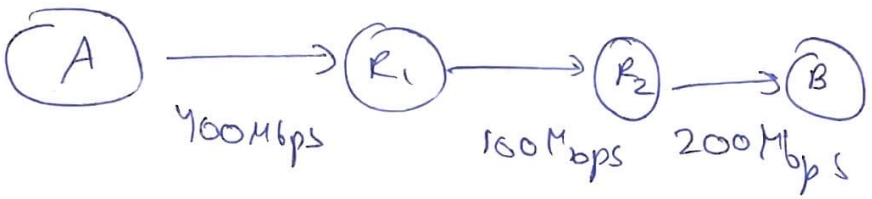
No.	Time	Source	Destination	Protocol	Length	Info
409	0.000766	127.0.0.1	127.0.0.1	TCP	1412	8751 → 57965 [PSH, ACK] Seq=13681 Ack=16 Win=2619648 Len=1368
410	0.000039	127.0.0.1	127.0.0.1	TCP	44	57965 → 8751 [ACK] Seq=16 Ack=15049 Win=2604544 Len=0
411	0.000697	127.0.0.1	127.0.0.1	TCP	1308	8751 → 57965 [PSH, ACK] Seq=15049 Ack=16 Win=2619648 Len=1264
412	0.000061	127.0.0.1	127.0.0.1	TCP	44	57965 → 8751 [ACK] Seq=16 Ack=16313 Win=2603264 Len=0
413	0.000867	127.0.0.1	127.0.0.1	TCP	44	8751 → 57965 [FIN, ACK] Seq=16313 Ack=16 Win=2619648 Len=0
414	0.000046	127.0.0.1	127.0.0.1	TCP	44	57965 → 8751 [ACK] Seq=16 Ack=16314 Win=2603264 Len=0
415	0.001135	127.0.0.1	127.0.0.1	TCP	44	57965 → 8751 [FIN, ACK] Seq=16 Ack=16314 Win=2603264 Len=0
416	0.000061	127.0.0.1	127.0.0.1	TCP	44	8751 → 57965 [ACK] Seq=16314 Ack=17 Win=2619648 Len=0
417	0.000898	127.0.0.1	127.0.0.1	TCP	56	57977 → 8751 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
418	0.000078	127.0.0.1	127.0.0.1	TCP	56	8751 → 57977 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
419	0.000080	127.0.0.1	127.0.0.1	TCP	44	57977 → 8751 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
420	3.648249	127.0.0.1	127.0.0.1	TCP	53	62354 → 61424 [PSH, ACK] Seq=163 Ack=55 Win=10232 Len=9

```
> Frame 411: 1308 bytes on wire (10464 bits), 1308 bytes captured (10464 bits) on interface \Device\NPF_Loopback, id 0
> Null/Loopback
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 8751, Dst Port: 57965, Seq: 15049, Ack: 16, Len: 1264
> Data (1264 bytes)
```

```
0000  02 00 00 00 45 00 05 18  2b b2 40 00 80 06 00 00   ····E··· +·@·····
0010  7f 00 00 01 7f 00 00 01  22 2f e2 6d 6a be be 17   ········ "/·mj···
0020  6a b9 b6 48 50 18 27 f9  6f a4 00 00 3d 3d 67 67   j··HP·'· o···==gg
0030  67 4a 6b 72 45 35 55 52  4a 42 41 41 41 41 67 48   gJkrE5UR JBAAAAgH
0040  45 6c 41 45 68 38 47 45  54 39 58 39 6b 69 49 6b   ElAEh8GE T9X9kiIk
0050  4c 59 68 6b 69 41 45 4c  61 68 55 69 41 45 62 61   lYhkiAEL ahUiAEba
0060  69 51 69 41 46 54 4b 69  51 75 67 46 53 4b 43 51   iQiAFTKi QugFSKCQ
0070  73 6f 46 53 4a 43 51 73  70 4a 43 4a 43 55 4d 70   soFSJCQs pJCJCUMp
0080  49 43 35 43 57 49 70 49  41 78 69 57 49 6c 49 41   IC5CWIpI AxiWIlIA
0090  78 6d 6d 49 6b 49 51 78  6b 69 49 6b 4c 59 68 6b   xmmIkIQx kiIkLYhk
00a0  69 41 45 4c 61 68 55 69  41 45 62 61 69 51 69 41   iAELahUi AEbaiQiA
00b0  46 7a 45 69 4a 47 6f 44  6d 58 70 4d 69 51 79 41   FzEiJGoD mXpMiQyA
00c0  64 32 4d 45 4e 4a 2f 61  58 74 61 31 44 4f 35 6b   d2MENJ/a Xta1DO5k
00d0  51 61 47 52 41 4f 50 79  2b 38 77 67 43 4c 76 38   QaGRAOPy +8wgCLv8
```

dwd transpose response

(2) a)



Message size = 100 KB = 800 kbits

Meta data = 100 B = 800 bits

a) 1 Packet.

Packet size = 1001 × 800 bits

$T = t_1 + t_2 + t_3$

$= 1001 \times 800 \left(\frac{1}{400 \times 10^6} + \frac{1}{100 \times 10^6} + \frac{1}{200 \times 10^6} \right)$

$= \frac{1001 \times 2}{10^6} \left[\frac{1}{4} + \frac{3}{2} \right]$

$= \frac{1001 \times 2 \times 7}{10^6}$ s = 14.014 ms

(b) 10 Packets

Packet size = $\frac{10100 \times 8}{10}$ $\left[\frac{100 \times 10^3 + 800}{10}\right]$

Transmission delays :-

$= \frac{80800}{4 \times 10^8}$, $\frac{80800}{10^8}$, $\frac{80800}{2 \times 10^8}$ for l_1, l_2, l_3

$= 202\,us$, $808\,us$, $404\,us$.

$\Rightarrow$ Bottleneck = 2nd link

$\therefore$ Total time = $(202 + (10-1) 808 + 404)\,us$

(no. of packets)

$= 8.686\,ms$

(c) 50 packets

Size of packet = $\frac{100kB}{50} + 100B \cong 16800$ Bits.

Transmission delays :-

$\frac{16800}{4 \times 10^3}$, $\frac{16800}{10^8}$, $\frac{16800}{2 \times 10^8} = 42\,us, 168\,us, 84\,us$

for l_1, l_2, l_3

Total time $= 42 * 50 \times 168 + 84$

$= 8.576 ms$

(d) 100 Packets.

Packet size $= 8800$ Bits $\left[\frac{100kB}{100} + 100B\right]$

Transmission times $= \frac{8800}{4\times10^8}, \frac{8800}{10^8}, \frac{8800}{2*10^8}$

$= 22us, 88us, 44us$ for l_1, l_2, l_3

Total time $= 22 + 100 \times 88 + 44 = 8.866 ms$

∴ 50 packets have the best delivery time 1.

3) (a) Propagation delay $= \frac{10 \times 10^3}{2 \times 3 \times 10^8}$ $\left[\frac{\text{Distance}}{\text{speed}}\right]$

$= 50 \times 10^{-6} = 50\ \mu s$

(b) Maximum Number of bits sent by R_1 till first bit reaches R_2

$=$

No. of bits sent in t = propagation delay

$= 50 \times 10^{-6} \times 100 \times 10^9$

$= 5\text{Mb}$

(c) Bit width $= \frac{\text{Distance}}{\text{Max no. of bits at a time in that distance}}$

$= 2\text{mm}$ $\left[\frac{10 \times 10^3}{5 \times 10^6}\right]$

4) RTT = 10 ms

webpage = 1 KB

n = 10

Size of Object = 100 KB

Assuming transmission time to be

t ms per KB

(a) $$T = \sum_{i=1}^{n} (2RTT) + (1*10\times100)$$

$$= 220 + 1001 * t \text{ ms}$$

(b) $$T = RTT + \sum_{i=1}^{n} RTT + \text{file transition time}$$

$$= 12 \times 10 + 1001 t \text{ ms}$$

$$= (120 + (1001 t))_{ms}$$

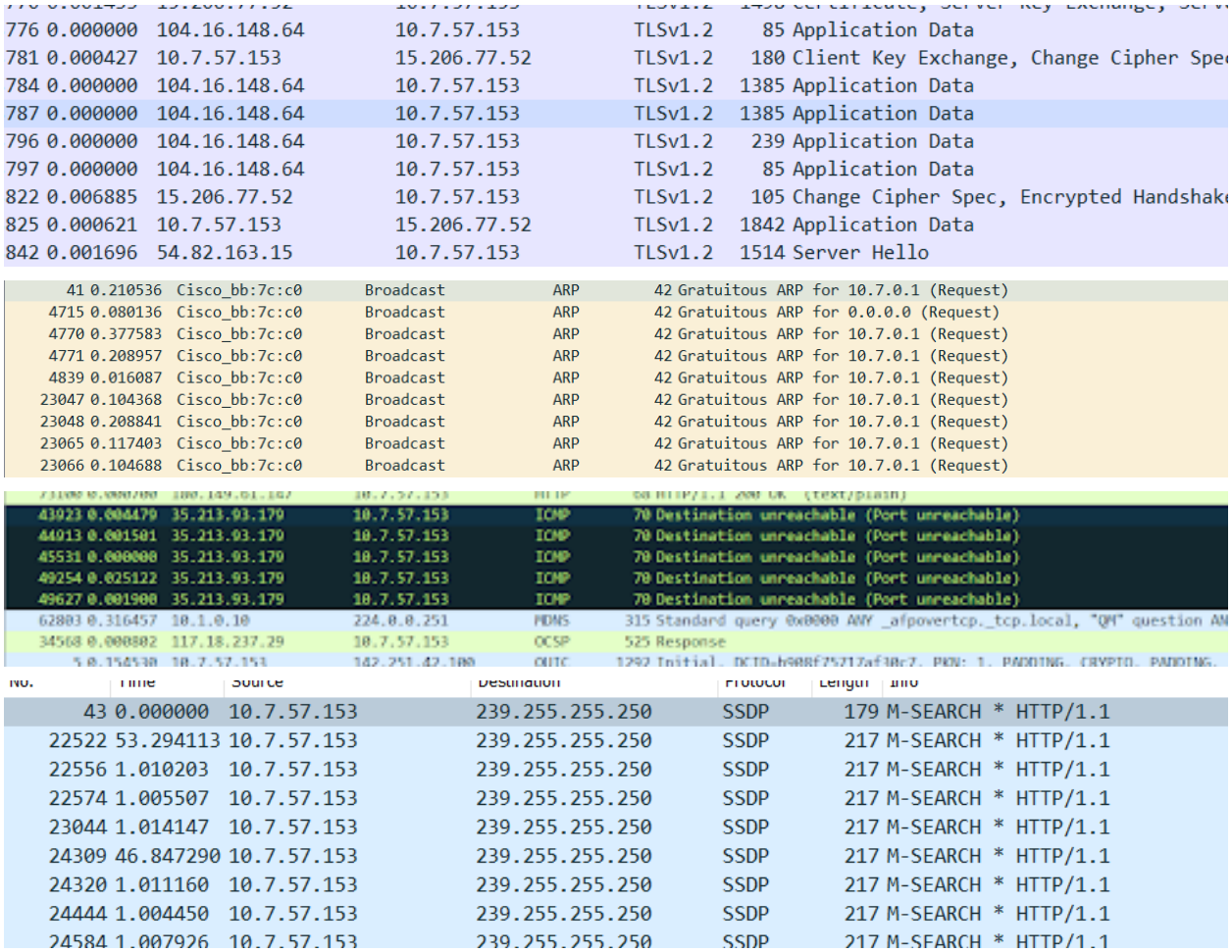
(1) T = RTT (connection) + RTT (webpage)
+ RTT (objects) +
+ file transmission time

T = (10 + 10 + 10) ms + 100 t

= (30 ms + 100 t) ms

Q5)

A. New Protocols



776	0.000000	104.16.148.64	10.7.57.153	TLSv1.2	85	Application Data
781	0.000427	10.7.57.153	15.206.77.52	TLSv1.2	180	Client Key Exchange, Change Cipher Spec
784	0.000000	104.16.148.64	10.7.57.153	TLSv1.2	1385	Application Data
787	0.000000	104.16.148.64	10.7.57.153	TLSv1.2	1385	Application Data
796	0.000000	104.16.148.64	10.7.57.153	TLSv1.2	239	Application Data
797	0.000000	104.16.148.64	10.7.57.153	TLSv1.2	85	Application Data
822	0.006885	15.206.77.52	10.7.57.153	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake
825	0.000621	10.7.57.153	15.206.77.52	TLSv1.2	1842	Application Data
842	0.001696	54.82.163.15	10.7.57.153	TLSv1.2	1514	Server Hello

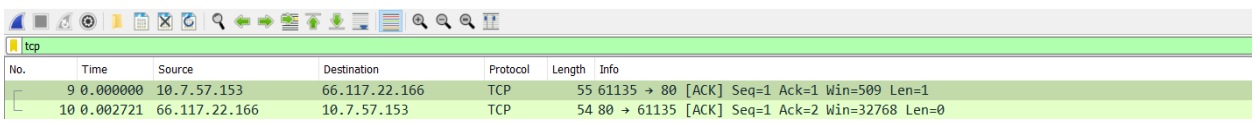
41	0.210536	Cisco_bb:7c:c0	Broadcast	ARP	42	Gratuitous ARP for 10.7.0.1 (Request)
4715	0.080136	Cisco_bb:7c:c0	Broadcast	ARP	42	Gratuitous ARP for 0.0.0.0 (Request)
4770	0.377583	Cisco_bb:7c:c0	Broadcast	ARP	42	Gratuitous ARP for 10.7.0.1 (Request)
4771	0.208957	Cisco_bb:7c:c0	Broadcast	ARP	42	Gratuitous ARP for 10.7.0.1 (Request)
4839	0.016087	Cisco_bb:7c:c0	Broadcast	ARP	42	Gratuitous ARP for 10.7.0.1 (Request)
23047	0.104368	Cisco_bb:7c:c0	Broadcast	ARP	42	Gratuitous ARP for 10.7.0.1 (Request)
23048	0.208841	Cisco_bb:7c:c0	Broadcast	ARP	42	Gratuitous ARP for 10.7.0.1 (Request)
23065	0.117403	Cisco_bb:7c:c0	Broadcast	ARP	42	Gratuitous ARP for 10.7.0.1 (Request)
23066	0.104688	Cisco_bb:7c:c0	Broadcast	ARP	42	Gratuitous ARP for 10.7.0.1 (Request)

43923	0.004479	35.213.93.179	10.7.57.153	ICMP	70	Destination unreachable (Port unreachable)
44013	0.001501	35.213.93.179	10.7.57.153	ICMP	70	Destination unreachable (Port unreachable)
45531	0.000000	35.213.93.179	10.7.57.153	ICMP	70	Destination unreachable (Port unreachable)
49254	0.025122	35.213.93.179	10.7.57.153	ICMP	70	Destination unreachable (Port unreachable)
49627	0.001908	35.213.93.179	10.7.57.153	ICMP	70	Destination unreachable (Port unreachable)
62803	0.316457	10.1.0.10	224.0.0.251	MDNS	315	Standard query 0x0000 ANY _afpovertcp._tcp.local, "QM" question AN
34568	0.000802	117.18.237.29	10.7.57.153	OCSP	525	Response

No.	Time	Source	Destination	Protocol	Length	Info
43	0.000000	10.7.57.153	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
22522	53.294113	10.7.57.153	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
22556	1.010203	10.7.57.153	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
22574	1.005507	10.7.57.153	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
23044	1.014147	10.7.57.153	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
24309	46.847290	10.7.57.153	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
24320	1.011160	10.7.57.153	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
24444	1.004450	10.7.57.153	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
24584	1.007926	10.7.57.153	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1

TLSv1.2: Provides Security in network communications. Transport layer protocol RFC-5246
ARP: Network layer protocol. Used to get hardware addresses. RFC-826
ICMP: Network layer Protocol. Used to find network communication issues. RFC- 792
OCSP: Check validity of certificate. RFC-6960
MDNS: Name resolution in small networks. RFC-6762
SSDP: Used for advertisement. Network layer protocol

B.



tcp

No.	Time	Source	Destination	Protocol	Length	Info
9	0.000000	10.7.57.153	66.117.22.166	TCP	55	61135 → 80 [ACK] Seq=1 Ack=1 Win=509 Len=1
10	0.002721	66.117.22.166	10.7.57.153	TCP	54	80 → 61135 [ACK] Seq=1 Ack=2 Win=32768 Len=0

RTT = 0.002721s

C.

Cookies before login

Request Cookies Show filtered out request cookies

Name	Value	Domain	Path	Expire…	Size	HttpOnly	Secure	Same…	Same…	Partiti…	Priority
_ga	GA1.3.82086891.1610028425	.iitgn.a…	/	2024-…	28						Medium

Cookies after login

Name	Value	Domain	Path	Expire..	Size	HttpO..	Secure	Same…	Same…	Partiti…	Prio…
_ga	GA1.3.82086891.1610028425	.iitgn.…	/	2024-…	28						Medium

Response Cookies

Name	Value	Domain	Path	Expire..	Size	HttpO..	Secure	Same…	Same…	Partiti…	Prio…
RequestToken	g44cs525us3dm3serb05ybf2	ims.iit…	/	Session	69	✓		Lax			Medium