

# **Assignment - 1**

## **Design Document - Computer Networks**

20110054

Dhairya Shah

GitHub Repository: [https://github.com/DhairyaShah981/Networks\\_Assignment1](https://github.com/DhairyaShah981/Networks_Assignment1)

### **Contents**

- 1) Design Document - Pg 1-4
- 2) Screenshots of outputs - Pg 5-7
- 3) Wireshark Screenshots of all commands - Pg 8-22
- 4) Part 3: Networking Tools - Pg 23-26

### **Introduction**

In this assignment, I have tried to implement a python program using sockets that support the five commands: CWD (prints the current directory of the server), LS (prints the list of files/folders in the server folder), cd <> (changes the directory, and prints the changed directory), DWD <file> (downloads the file from the server to the client directory), UPD<file> (uploads a file from the client directory to the server directory).

### **ReadMe Instructions**

My GitHub repository contains two folders: server and client. The client folder contains utilities.py and client.py. The server folder contains server.py, bruh.txt, and a folder named Images and utilities.py. After cloning the repository, you can open two command prompts and first run the server.py and then run the client.py to test the commands. You will get the outputs and prompts on both the client and server. You may note that I am currently implementing server and client on the same operating system, so it works like two processes communicating with each other. (Inter-Process Communication) Implementing the server on a different system can also work fine if we set the IP address accordingly.

### **Error Statements**

Every assignment is incomplete without solving bugs and errors. While running the commands, you may run into some errors covered in the print statements; for example, KeyboardInterrupt, and ConnectionError are considered socket errors, or if your input is invalid, it prints 'Invalid command.' Specifically, in the cd command, if the path does not exist, it prints 'No such directory exists!'. In dwd and upd if the specified file is unavailable, it prints 'Socket Error,' and you can check the server terminal, which will show 'No such file exist.'

## Layers

The system uses a template N layer model for Remote File Sharing (RFS) client and server. The top 3 layers are the File Service, Crypto Service, and the Networking layer:

- 1) **File Sharing:** To implement the above 5 commands, I am using a few inbuilt python functions from the os library, which, when called, invoke some system calls, which eventually give us the information about the server directory. The file-sharing layer is responsible for calling these Operating Systems APIs (Application Programming Interface), and implementing all the five RFS commands. The file-sharing layer moves the files and messages between the local and remote file systems. The files and messages are transferred from server to client and vice versa using `sendall()`, `recv(1024)`, `send_msg()`, `recv_msg()`.

The protocol design for this layer is as follows. For the `cwd` command, I used the `os.getcwd()` function, which gives the current directory, and then sent this as a message to the client. For the `ls` command, I used `os.listdir()` function, which gives the list of files/folders in the current directory and then sent this as a string message to the client. For the `cd` command, I changed the directory using `os.chdir(path)` and then sent the changed directory as a string message to the client. For the `dwd` command, I am first searching for the given file in the server directory, reading the whole file as string, sending it to the client as packets of size 1024, receiving the data in the client and writing the data in the new file made in the client folder. For the `upd` command, I am first searching for the given file in the client directory, reading the whole file as string, sending it to the server as packets of 1024, receiving the data in server and writing the data in the new file made in the server folder. All the functions for the first 3 commands are in the `utilities.py`, while for the `upd` and `dwd` the process is implemented in the server and client itself.

- 2) **Crypto Service:** Originally, the file transfer was implemented using only the utf-8 encoding, which encodes the characters into bytes. While decoding, the bytes were again converted to characters. As given in the assignment, I have introduced another encryption layer visible in the Wireshark dump. There are three modes of encryption available for the user: Plaintext, Substitute, and Transpose. The user is asked to input an integer from 1, 2, and 3 corresponding to the three encryption layers. Now in both server and client, I have implemented all the 5 commands in 3 'if conditions' (for three encryption layers).
  - a) **Plaintext:** In this encryption mode, the text doesn't change. Hence I have not defined a particular encryption function for this and implemented all the commands without encrypting and decrypting.

- b) **Substitute:** In this encryption mode, all the characters are offset by 2. While decrypting, the characters are offset by -2. Both the encrypt and decrypt functions are implemented in the utilities.py. In the functions, I loop through the message character by character and offset it by manipulating the ASCII values.
  - c) **Transpose:** In this encryption mode, the message is simply reversed. There are two interpretations: should I reverse it completely or reverse it word by word? I realized later that reversing it word by word makes more sense in the encryption paradigm. In the function, I loop through the message word by word, reverse them, and append them to the encrypted message. Also, the encrypt and decrypt functions will be the same for the transpose encryption.
- 3) **Networking Layer:** My program runs on the foundations of the socket library, and that's why we call it a sockets program. When we create a sockets program, we use something that generally is called a sockets library. A sockets library consists of compile-time structures, statically linked support modules, and run-time support modules. In the client.py file, when I create a socket using: `socket.socket(socket.AF_INET, socket.SOCK_STREAM)`, the first argument refers to the IPv4 address, and the second argument refers to the streaming socket, which is the TCP (Transmission Control Protocol). The TCP manages the networking layer whenever we invoke the in-built functions of the socket library. The TCP facilitates communication among the machines using their IP address through sockets. Apart from TCP, I could have used UDP, but in the lectures, I learned that UDP is an unreliable and connectionless protocol. In UDP, there is no function to ensure that data is received in the same order as it was transmitted.

### Challenges Faced

The assignment was lengthy, not in terms of writing code but debugging. My friends and I spent hours debugging and managing the border cases. At one point, I felt the border cases are more than the mainstream cases. The first three commands were easy to implement, but I faced issues managing the edge cases of different path names while adding the encryption layer. `dwd` and `upd` functions were also easy to implement at first without caring about the encryption and edge cases. Starting with the simple `.txt` file, which can only be read as strings by reading it as `'r'` and writing as `'w'` instead of `'rb'` and `'wb'`, for which it doesn't work. I had to implement it using strings because my encryption layer only accepts strings.

If the file name consisted of more than 1 word separated by spaces, my logic only took the first word from them, which threw an error at the start. That's why I traversed through the path and appended all the words in my filename. While downloading and uploading, I was prompted when the download was successful from the server, but the terminal didn't print that even after downloading. That prompt was written in the file itself. I solved this by adding an appropriate break statement. Transferring the messages in bytes and strings and encrypting and decrypting them at appropriate times was very cumbersome, and 1 small mistake cost me hours of debugging.

### Limitations and Further Improvements

My current program only supports the downloading and uploading .txt files because I am using 'r' and 'w', which can only read and write as strings. I tried implementing .png and .jpeg files by converting bytes to strings and vice versa, but the files got corrupted during the process. I found an online resource that says we can implement file transfer using a python library named 'Base64' which can convert an image to a string and vice versa. I haven't implemented it because of time constraints and some new bugs.

### References

- 1) I used the skeleton code of the server, client, and basic utilities like send\_msg(), and recv\_msg() from the [book](#) suggested by the professor. The skeleton code helped me how to set up an echo server and client on the same system.
- 2) For file transfer, I referred to this [resource](#).
- 3) For the in-built os functions, I referred to the python documentation.

## Command Prompt Screenshots of Output

Plaintext: cwd

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 1
Type message in encrypted mode, enter to send, 'exit' to quit
cwd
Sent message: cwd
Received echo: C:\Users\DELL\cnass\server
Closed connection to server
```

Plaintext: ls

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 1
Type message in encrypted mode, enter to send, 'exit' to quit
ls
Sent message: ls
Received echo: ['bruh.txt', 'Images', 'server.py', 'utilities.py', '__pycache__']
Closed connection to server
```

Plaintext: cd Images

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 1
Type message in encrypted mode, enter to send, 'exit' to quit
cd Images
Sent message: cd Images
Received echo: C:\Users\DELL\cnass\server\Images
Closed connection to server
```

Plaintext: dwd bruh.txt

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 1
Type message in encrypted mode, enter to send, 'exit' to quit
dwd bruh.txt
Download Completed!
Closed connection to server
```

Plaintext: upd bruh.txt

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 1
Type message in encrypted mode, enter to send, 'exit' to quit
upd bruh.txt
Upload Completed!
Closed connection to server
```

Substitute: cwd

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 2
Type message, enter to send, 'exit' to quit
cwd
Sent message: cwd
Received echo: C:\Users\DELL\cnass\server
Closed connection to server
```

Substitute: ls

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 2
Type message, enter to send, 'exit' to quit
ls
Sent message: ls
Received echo: ['bruh.txt', 'Images', 'server.py', 'utilities.py', '__pycache__']
Closed connection to server
```

Substitute: cd Images

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 2
Type message, enter to send, 'exit' to quit
cd Images
Sent message: cd Images
Received echo: C:\Users\DELL\cnass\server\Images
Closed connection to server
```

Substitute: dwd bruh.txt

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 2
Type message, enter to send, 'exit' to quit
dwd bruh.txt
Download Completed!
Closed connection to server
```

Substitute: upd bruh.txt

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 2
Type message, enter to send, 'exit' to quit
upd bruh.txt
Upload Completed!
Closed connection to server
```

Transpose: cwd

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 3
Type message in encrypted mode, enter to send, 'exit' to quit
cwd
Sent message: cwd
Received echo: C:\Users\DELL\cnass\server
Closed connection to server
```

Transpose: ls

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 3
Type message in encrypted mode, enter to send, 'exit' to quit
ls
Sent message: ls
Received echo: ['bruh.txt', 'Images', 'server.py', 'utilities.py', '__pycache__']
Closed connection to server
```

Transpose: cd Images

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 3
Type message in encrypted mode, enter to send, 'exit' to quit
cd Images
Sent message: cd Images
Received echo: C:\Users\DELL\cnass\server\Images
Closed connection to server
```

Transpose: dwd bruh.txt

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 3
Type message in encrypted mode, enter to send, 'exit' to quit
dwd bruh.txt
Download Completed!
Closed connection to server
```

Transpose: upd bruh.txt

```
Connected to 192.168.56.1:4040
Select any number from 1, 2, and 3: 3
Type message in encrypted mode, enter to send, 'exit' to quit
upd bruh.txt
Upload Completed!
Closed connection to server
```

# Wireshark Screenshots of Packets

## Plaintext: cwd command

The screenshot shows a Wireshark packet capture on the 'tcp' filter. The packet list displays 12 packets. Packet 1 (Seq=57489) is a PSH, ACK segment. Packet 2 (Seq=4040) is an ACK segment. Packet 3 (Seq=4040) is a PSH, ACK segment. Packet 4 (Seq=57489) is an ACK segment. Packet 5 (Seq=4040) is a FIN, ACK segment. Packet 6 (Seq=57489) is a FIN, ACK segment. Packet 7 (Seq=4040) is an ACK segment. Packet 8 (Seq=57491) is a SYN segment. Packet 9 (Seq=4040) is a SYN, ACK segment. Packet 10 (Seq=57491) is an ACK segment. Packet 11 (Seq=4040) is a TCP Retransmission segment. Packet 12 (Seq=57489) is a TCP ZeroWindow segment.

Frame 1: 48 bytes on wire (384 bits), 48 bytes captured (384 bits) on interface \Device\NPF\_{...}, id 0

- > Null/Loopback
- > Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1
- > Transmission Control Protocol, Src Port: 57489, Dst Port: 4040, Seq: 1, Ack: 1, Len: 4
- > Data (4 bytes)

0000 02 00 00 00 45 00 00 2c c4 ef 40 00 80 06 00 00 ...E... ..@.....  
0010 c0 a8 38 01 c0 a8 38 01 e0 91 0f c8 7f 39 35 d3 ...8...8...95..  
0020 39 1e 61 9a 50 18 27 f9 8e e5 00 00 63 77 64 00 9.a.P.'...cwd..

## Plaintext: cwd response

The screenshot shows a Wireshark packet capture on the 'tcp' filter. The packet list displays 12 packets. Packet 1 (Seq=57489) is a PSH, ACK segment. Packet 2 (Seq=4040) is an ACK segment. Packet 3 (Seq=4040) is a PSH, ACK segment. Packet 4 (Seq=57489) is an ACK segment. Packet 5 (Seq=4040) is a FIN, ACK segment. Packet 6 (Seq=57489) is a FIN, ACK segment. Packet 7 (Seq=4040) is an ACK segment. Packet 8 (Seq=57491) is a SYN segment. Packet 9 (Seq=4040) is a SYN, ACK segment. Packet 10 (Seq=57491) is an ACK segment. Packet 11 (Seq=4040) is a TCP Retransmission segment. Packet 12 (Seq=57489) is a TCP ZeroWindow segment.

Frame 3: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{...}, id 0

- > Null/Loopback
- > Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1
- > Transmission Control Protocol, Src Port: 4040, Dst Port: 57489, Seq: 1, Ack: 5, Len: 27
- > Data (27 bytes)

0000 02 00 00 00 45 00 00 43 c4 f1 40 00 80 06 00 00 ...E..C..@.....  
0010 c0 a8 38 01 c0 a8 38 01 0f c8 e0 91 39 1e 61 9a ...8...8...9.a..  
0020 7f 39 35 d7 50 18 27 f9 5f 60 00 00 43 3a 5c 55 ...95.P.'...C:\U  
0030 73 65 72 73 5c 44 45 4c 4c 5c 63 6e 61 73 73 5c sers\DEL L\cnass\  
0040 73 65 72 76 65 72 00 server..



## Substitute: cwd command

The image shows a Wireshark packet capture of a TCP connection. The packet list shows a sequence of packets from 49 to 60. Packet 51 is highlighted, showing a TCP ACK with sequence 48. The packet details pane shows the frame structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The data field shows the command 'cwd' being executed.

No.	Time	Source	Destination	Protocol	Length	Info
49	171.603695	192.168.56.1	192.168.56.1	TCP	46	57491 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
50	171.603767	192.168.56.1	192.168.56.1	TCP	44	4040 → 57491 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
51	173.746015	192.168.56.1	192.168.56.1	TCP	48	57491 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=4
52	173.746088	192.168.56.1	192.168.56.1	TCP	44	4040 → 57491 [ACK] Seq=1 Ack=7 Win=2619648 Len=0
53	173.747088	192.168.56.1	192.168.56.1	TCP	71	4040 → 57491 [PSH, ACK] Seq=1 Ack=7 Win=2619648 Len=27
54	173.747142	192.168.56.1	192.168.56.1	TCP	44	57491 → 4040 [ACK] Seq=7 Ack=28 Win=2619648 Len=0
55	173.747355	192.168.56.1	192.168.56.1	TCP	44	4040 → 57491 [FIN, ACK] Seq=28 Ack=7 Win=2619648 Len=0
56	173.747390	192.168.56.1	192.168.56.1	TCP	44	57491 → 4040 [ACK] Seq=7 Ack=29 Win=2619648 Len=0
57	173.747512	192.168.56.1	192.168.56.1	TCP	44	57491 → 4040 [FIN, ACK] Seq=7 Ack=29 Win=2619648 Len=0
58	173.747554	192.168.56.1	192.168.56.1	TCP	44	4040 → 57491 [ACK] Seq=29 Ack=8 Win=2619648 Len=0
59	173.748568	192.168.56.1	192.168.56.1	TCP	56	57515 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
60	173.748657	192.168.56.1	192.168.56.1	TCP	56	4040 → 57515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1

> Frame 51: 48 bytes on wire (384 bits), 48 bytes captured (384 bits) on interface \Device\NPF\_{...}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 57491, Dst Port: 4040, Seq: 3, Ack: 1, Len: 4

> Data (4 bytes)

```
0000 02 00 00 00 45 00 00 2c c4 fd 40 00 80 06 00 00 ...E... ..@.....
0010 c0 a8 38 01 c0 a8 38 01 e0 93 0f c8 03 41 9e d6 ..8...8... ..A...
0020 63 93 8b 4e 50 18 27 f9 49 ad 00 00 65 79 66 00 c..NP..'. I...eyf..
```

## Substitute: cwd response

The image shows a Wireshark packet capture of a TCP connection. The packet list shows a sequence of packets from 49 to 60. Packet 53 is highlighted, showing a TCP ACK with sequence 71. The packet details pane shows the frame structure: Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The data field shows the command 'cwd' being executed.

No.	Time	Source	Destination	Protocol	Length	Info
49	171.603695	192.168.56.1	192.168.56.1	TCP	46	57491 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
50	171.603767	192.168.56.1	192.168.56.1	TCP	44	4040 → 57491 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
51	173.746015	192.168.56.1	192.168.56.1	TCP	48	57491 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=4
52	173.746088	192.168.56.1	192.168.56.1	TCP	44	4040 → 57491 [ACK] Seq=1 Ack=7 Win=2619648 Len=0
53	173.747088	192.168.56.1	192.168.56.1	TCP	71	4040 → 57491 [PSH, ACK] Seq=1 Ack=7 Win=2619648 Len=27
54	173.747142	192.168.56.1	192.168.56.1	TCP	44	57491 → 4040 [ACK] Seq=7 Ack=28 Win=2619648 Len=0
55	173.747355	192.168.56.1	192.168.56.1	TCP	44	4040 → 57491 [FIN, ACK] Seq=28 Ack=7 Win=2619648 Len=0
56	173.747390	192.168.56.1	192.168.56.1	TCP	44	57491 → 4040 [ACK] Seq=7 Ack=29 Win=2619648 Len=0
57	173.747512	192.168.56.1	192.168.56.1	TCP	44	57491 → 4040 [FIN, ACK] Seq=7 Ack=29 Win=2619648 Len=0
58	173.747554	192.168.56.1	192.168.56.1	TCP	44	4040 → 57491 [ACK] Seq=29 Ack=8 Win=2619648 Len=0
59	173.748568	192.168.56.1	192.168.56.1	TCP	56	57515 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
60	173.748657	192.168.56.1	192.168.56.1	TCP	56	4040 → 57515 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1

> Frame 53: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{...}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 4040, Dst Port: 57491, Seq: 1, Ack: 7, Len: 27

> Data (27 bytes)

```
0000 02 00 00 00 45 00 00 43 c4 ff 40 00 80 06 00 00 ...E..C ..@.....
0010 c0 a8 38 01 c0 a8 38 01 0f c8 e0 93 63 93 8b 4e ..8...8... ..c..N
0020 03 41 9e da 50 18 27 f9 08 16 00 00 45 3a 5c 57 ..A..P..'. ....E:\W
0030 75 67 74 75 5c 46 47 4e 4e 5c 65 70 63 75 75 5c ugtu\FGN N\epcuu\
0040 75 67 74 78 67 74 00 ugtxgt..
```

## Transpose: cwd command

No.	Time	Source	Destination	Protocol	Length	Info
113	277.066335	192.168.56.1	192.168.56.1	TCP	44	4040 → 57515 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
131	346.455647	192.168.56.1	192.168.56.1	TCP	48	57515 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=327424 Len=4
132	346.455737	192.168.56.1	192.168.56.1	TCP	44	4040 → 57515 [ACK] Seq=1 Ack=7 Win=2619648 Len=0
133	346.457802	192.168.56.1	192.168.56.1	TCP	71	4040 → 57515 [PSH, ACK] Seq=1 Ack=7 Win=2619648 Len=27
134	346.457887	192.168.56.1	192.168.56.1	TCP	44	57515 → 4040 [ACK] Seq=7 Ack=28 Win=2619648 Len=0
135	346.458503	192.168.56.1	192.168.56.1	TCP	44	4040 → 57515 [FIN, ACK] Seq=28 Ack=7 Win=2619648 Len=0
136	346.458563	192.168.56.1	192.168.56.1	TCP	44	57515 → 4040 [ACK] Seq=7 Ack=29 Win=2619648 Len=0
137	346.460117	192.168.56.1	192.168.56.1	TCP	44	57515 → 4040 [FIN, ACK] Seq=7 Ack=29 Win=2619648 Len=0
138	346.460188	192.168.56.1	192.168.56.1	TCP	44	4040 → 57515 [ACK] Seq=29 Ack=8 Win=2619648 Len=0
139	346.462318	192.168.56.1	192.168.56.1	TCP	56	57523 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
140	346.462437	192.168.56.1	192.168.56.1	TCP	56	4040 → 57523 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
141	346.462541	192.168.56.1	192.168.56.1	TCP	44	57523 → 4040 [ACK] Seq=1 Ack=1 Win=2619648 Len=0

> Frame 131: 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: 192.168.56.1, Dst: 192.168.56.1  
> Transmission Control Protocol, Src Port: 57515, Dst Port: 4040, Seq: 3, Ack: 1, Len: 4  
> Data (4 bytes)

```
0000 02 00 00 00 45 00 00 2c c5 0a 40 00 80 06 00 00 ....E... ..@.....
0010 c0 a8 38 01 c0 a8 38 01 e0 ab 0f c8 0d 0e 60 e9 ..8...8.....Q...
0020 0f 51 86 ee 50 18 04 ff fd 53 00 00 64 77 63 00 .Q..P... ..S...dwc..
```

## Transpose: cwd response

No.	Time	Source	Destination	Protocol	Length	Info
113	277.066335	192.168.56.1	192.168.56.1	TCP	44	4040 → 57515 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
131	346.455647	192.168.56.1	192.168.56.1	TCP	48	57515 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=327424 Len=4
132	346.455737	192.168.56.1	192.168.56.1	TCP	44	4040 → 57515 [ACK] Seq=1 Ack=7 Win=2619648 Len=0
133	346.457802	192.168.56.1	192.168.56.1	TCP	71	4040 → 57515 [PSH, ACK] Seq=1 Ack=7 Win=2619648 Len=27
134	346.457887	192.168.56.1	192.168.56.1	TCP	44	57515 → 4040 [ACK] Seq=7 Ack=28 Win=2619648 Len=0
135	346.458503	192.168.56.1	192.168.56.1	TCP	44	4040 → 57515 [FIN, ACK] Seq=28 Ack=7 Win=2619648 Len=0
136	346.458563	192.168.56.1	192.168.56.1	TCP	44	57515 → 4040 [ACK] Seq=7 Ack=29 Win=2619648 Len=0
137	346.460117	192.168.56.1	192.168.56.1	TCP	44	57515 → 4040 [FIN, ACK] Seq=7 Ack=29 Win=2619648 Len=0
138	346.460188	192.168.56.1	192.168.56.1	TCP	44	4040 → 57515 [ACK] Seq=29 Ack=8 Win=2619648 Len=0
139	346.462318	192.168.56.1	192.168.56.1	TCP	56	57523 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
140	346.462437	192.168.56.1	192.168.56.1	TCP	56	4040 → 57523 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
141	346.462541	192.168.56.1	192.168.56.1	TCP	44	57523 → 4040 [ACK] Seq=1 Ack=1 Win=2619648 Len=0

> Frame 133: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF\_{Loopback}, id 0  
> Null/Loopback  
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1  
> Transmission Control Protocol, Src Port: 4040, Dst Port: 57515, Seq: 1, Ack: 7, Len: 27  
> Data (27 bytes)

```
0000 02 00 00 00 45 00 00 43 c5 0c 40 00 80 06 00 00 ....E..C...@.....
0010 c0 a8 38 01 c0 a8 38 01 0f c8 e0 ab 0f 51 86 ee ..8...8.....Q...
0020 0d 0e 60 ed 50 18 27 f9 bf bf 00 00 72 65 76 72 .P.. ..revr
0030 65 73 5c 73 73 61 6e 63 5c 4c 4c 45 44 5c 73 72 es\ssanc \LLED\sr
0040 65 73 55 5c 3a 43 00 esU\;C..
```

## Plaintext: ls command

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
183	131.827595	192.168.56.1	192.168.56.1	TCP	44	4040 → 57523 [ACK] Seq=1 Ack=3 Win=10233 Len=0
184	133.019213	192.168.56.1	192.168.56.1	TCP	47	57523 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=10233 Len=3
185	133.019303	192.168.56.1	192.168.56.1	TCP	44	4040 → 57523 [ACK] Seq=1 Ack=6 Win=10233 Len=0
186	133.021988	192.168.56.1	192.168.56.1	TCP	111	4040 → 57523 [PSH, ACK] Seq=1 Ack=6 Win=10233 Len=67
187	133.022103	192.168.56.1	192.168.56.1	TCP	44	57523 → 4040 [ACK] Seq=6 Ack=68 Win=10233 Len=0
188	133.022429	192.168.56.1	192.168.56.1	TCP	44	4040 → 57523 [FIN, ACK] Seq=68 Ack=6 Win=10233 Len=0
189	133.022472	192.168.56.1	192.168.56.1	TCP	44	57523 → 4040 [ACK] Seq=6 Ack=69 Win=10233 Len=0
190	133.023017	192.168.56.1	192.168.56.1	TCP	44	57523 → 4040 [FIN, ACK] Seq=6 Ack=69 Win=10233 Len=0
191	133.023083	192.168.56.1	192.168.56.1	TCP	44	4040 → 57523 [ACK] Seq=69 Ack=7 Win=10233 Len=0
192	133.024841	192.168.56.1	192.168.56.1	TCP	56	57537 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
193	133.024911	192.168.56.1	192.168.56.1	TCP	56	4040 → 57537 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
194	133.024950	192.168.56.1	192.168.56.1	TCP	44	57537 → 4040 [ACK] Seq=1 Ack=1 Win=2619648 Len=0

> Frame 184: 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: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 57523, Dst Port: 4040, Seq: 3, Ack: 1, Len: 3

> Data (3 bytes)

```
0000  02 00 00 00 45 00 00 2b c5 17 40 00 80 06 00 00  ....E--+...@-....
0010  c0 a8 38 01 c0 a8 38 01 e0 b3 0f c8 57 f0 98 d3  --8---8-....W...
0020  e3 70 33 25 50 18 27 f9 32 34 00 00 6c 73 00    .p3%P-'. 24...ls.
```

## Plaintext: ls response

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
183	131.827595	192.168.56.1	192.168.56.1	TCP	44	4040 → 57523 [ACK] Seq=1 Ack=3 Win=10233 Len=0
184	133.019213	192.168.56.1	192.168.56.1	TCP	47	57523 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=10233 Len=3
185	133.019303	192.168.56.1	192.168.56.1	TCP	44	4040 → 57523 [ACK] Seq=1 Ack=6 Win=10233 Len=0
186	133.021988	192.168.56.1	192.168.56.1	TCP	111	4040 → 57523 [PSH, ACK] Seq=1 Ack=6 Win=10233 Len=67
187	133.022103	192.168.56.1	192.168.56.1	TCP	44	57523 → 4040 [ACK] Seq=6 Ack=68 Win=10233 Len=0
188	133.022429	192.168.56.1	192.168.56.1	TCP	44	4040 → 57523 [FIN, ACK] Seq=68 Ack=6 Win=10233 Len=0
189	133.022472	192.168.56.1	192.168.56.1	TCP	44	57523 → 4040 [ACK] Seq=6 Ack=69 Win=10233 Len=0
190	133.023017	192.168.56.1	192.168.56.1	TCP	44	57523 → 4040 [FIN, ACK] Seq=6 Ack=69 Win=10233 Len=0
191	133.023083	192.168.56.1	192.168.56.1	TCP	44	4040 → 57523 [ACK] Seq=69 Ack=7 Win=10233 Len=0
192	133.024841	192.168.56.1	192.168.56.1	TCP	56	57537 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
193	133.024911	192.168.56.1	192.168.56.1	TCP	56	4040 → 57537 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
194	133.024950	192.168.56.1	192.168.56.1	TCP	44	57537 → 4040 [ACK] Seq=1 Ack=1 Win=2619648 Len=0

> Frame 186: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 4040, Dst Port: 57523, Seq: 1, Ack: 6, Len: 67

> Data (67 bytes)

```
0000  02 00 00 00 45 00 00 6b c5 19 40 00 80 06 00 00  ....E-+k...@-....
0010  c0 a8 38 01 c0 a8 38 01 0f c8 e0 b3 e3 70 33 25  --8---8-....p3%
0020  57 f0 98 d6 50 18 27 f9 ff ef 00 00 5b 27 62 72  W---P-'. ....['br
0030  75 68 2e 74 78 74 27 2c 20 27 49 6d 61 67 65 73  uh.txt', 'Images
0040  27 2c 20 27 73 65 72 76 65 72 2e 70 79 27 2c 20  ', 'serv er.py',
0050  27 75 74 69 6c 69 74 69 65 73 2e 70 79 27 2c 20  'utiliti es.py',
0060  27 5f 5f 70 79 63 61 63 68 65 5f 5f 27 5d 00    '._pycac he_'].
```

## Substitute: ls command

tcp

No.	Time	Source	Destination	Protocol	Length	Info
188	133.022429	192.168.56.1	192.168.56.1	TCP	44	4040 → 57523 [FIN, ACK] Seq=68 Ack=6 Win=10233 Len=0
189	133.022472	192.168.56.1	192.168.56.1	TCP	44	57523 → 4040 [ACK] Seq=6 Ack=69 Win=10233 Len=0
190	133.023017	192.168.56.1	192.168.56.1	TCP	44	57523 → 4040 [FIN, ACK] Seq=6 Ack=69 Win=10233 Len=0
191	133.023083	192.168.56.1	192.168.56.1	TCP	44	4040 → 57523 [ACK] Seq=69 Ack=7 Win=10233 Len=0
192	133.024841	192.168.56.1	192.168.56.1	TCP	56	57537 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
193	133.024911	192.168.56.1	192.168.56.1	TCP	56	4040 → 57537 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
194	133.024950	192.168.56.1	192.168.56.1	TCP	44	57537 → 4040 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
213	224.871132	192.168.56.1	192.168.56.1	TCP	46	57537 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
214	224.871311	192.168.56.1	192.168.56.1	TCP	44	4040 → 57537 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
215	225.918820	192.168.56.1	192.168.56.1	TCP	47	57537 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=3
216	225.918903	192.168.56.1	192.168.56.1	TCP	44	4040 → 57537 [ACK] Seq=1 Ack=6 Win=2619648 Len=0
217	225.921045	192.168.56.1	192.168.56.1	TCP	111	4040 → 57537 [PSH, ACK] Seq=1 Ack=6 Win=2619648 Len=67

> Frame 215: 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: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 57537, Dst Port: 4040, Seq: 3, Ack: 1, Len: 3

> Data (3 bytes)

```
0000 02 00 00 00 45 00 00 2b c5 24 40 00 80 06 00 00 ....E--+-$@-----
0010 c0 a8 38 01 c0 a8 38 01 e0 c1 0f c8 3a cb e1 73 ..8...8:.....:..s
0020 62 8b e5 e9 50 18 27 f9 d2 c9 00 00 6e 75 00 b...P'..-...nu.
```

## Substitute: ls response

tcp

No.	Time	Source	Destination	Protocol	Length	Info
188	133.022429	192.168.56.1	192.168.56.1	TCP	44	4040 → 57523 [FIN, ACK] Seq=68 Ack=6 Win=10233 Len=0
189	133.022472	192.168.56.1	192.168.56.1	TCP	44	57523 → 4040 [ACK] Seq=6 Ack=69 Win=10233 Len=0
190	133.023017	192.168.56.1	192.168.56.1	TCP	44	57523 → 4040 [FIN, ACK] Seq=6 Ack=69 Win=10233 Len=0
191	133.023083	192.168.56.1	192.168.56.1	TCP	44	4040 → 57523 [ACK] Seq=69 Ack=7 Win=10233 Len=0
192	133.024841	192.168.56.1	192.168.56.1	TCP	56	57537 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
193	133.024911	192.168.56.1	192.168.56.1	TCP	56	4040 → 57537 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
194	133.024950	192.168.56.1	192.168.56.1	TCP	44	57537 → 4040 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
213	224.871132	192.168.56.1	192.168.56.1	TCP	46	57537 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
214	224.871311	192.168.56.1	192.168.56.1	TCP	44	4040 → 57537 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
215	225.918820	192.168.56.1	192.168.56.1	TCP	47	57537 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=3
216	225.918903	192.168.56.1	192.168.56.1	TCP	44	4040 → 57537 [ACK] Seq=1 Ack=6 Win=2619648 Len=0
217	225.921045	192.168.56.1	192.168.56.1	TCP	111	4040 → 57537 [PSH, ACK] Seq=1 Ack=6 Win=2619648 Len=67

> Frame 217: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 4040, Dst Port: 57537, Seq: 1, Ack: 6, Len: 67

> Data (67 bytes)

```
0000 02 00 00 00 45 00 00 6b c5 26 40 00 80 06 00 00 ....E--k-&@-----
0010 c0 a8 38 01 c0 a8 38 01 0f c8 e0 c1 62 8b e5 e9 ..8...8:.....b...
0020 3a cb e1 76 50 18 27 f9 cc 5d 00 00 5b 27 64 74 ..vP'..'..['dt
0030 77 6a 2e 76 7a 76 27 2c 20 27 4b 6f 63 69 67 75 wj.vzv', 'kocigu
0040 27 2c 20 27 75 67 74 78 67 74 2e 72 61 27 2c 20 ', 'ugtX gt.ra',
0050 27 77 76 6b 6e 6b 76 6b 67 75 2e 72 61 27 2c 20 'wvknkvk gu.ra',
0060 27 5f 5f 72 61 65 63 65 6a 67 5f 5f 27 5d 00 '___raece jg_'].
```

## Transpose: ls command

Wireshark packet capture showing a TCP SYN-ACK from 192.168.56.1 to 192.168.56.1 on port 4040. The packet is captured on interface \Device\NPF\_{Loopback}, id 0. The packet details show the following information:

- Frame 248: 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: 192.168.56.1, Dst: 192.168.56.1
- Transmission Control Protocol, Src Port: 57543, Dst Port: 4040, Seq: 3, Ack: 1, Len: 3
- Data (3 bytes)

The packet bytes are displayed in hexadecimal and ASCII:

```
0000 02 00 00 00 45 00 00 2b c5 31 40 00 80 06 00 00 ... E--+ -1@-....
0010 c0 a8 38 01 c0 a8 38 01 e0 c7 0f c8 6f cf 61 d6 ... 8...8- ....o.a-
0020 94 1e 48 a2 50 18 04 ff a7 14 00 00 73 6c 00 ... H.P-... -s1.
```

## Transpose: ls response

Wireshark packet capture showing a TCP ACK from 192.168.56.1 to 192.168.56.1 on port 4040. The packet is captured on interface \Device\NPF\_{Loopback}, id 0. The packet details show the following information:

- Frame 250: 111 bytes on wire (888 bits), 111 bytes captured (888 bits) on interface \Device\NPF\_{Loopback}, id 0
- Null/Loopback
- Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1
- Transmission Control Protocol, Src Port: 4040, Dst Port: 57543, Seq: 1, Ack: 6, Len: 67
- Data (67 bytes)

The packet bytes are displayed in hexadecimal and ASCII:

```
0000 02 00 00 00 45 00 00 6b c5 33 40 00 80 06 00 00 ... E--k -3@-....
0010 c0 a8 38 01 c0 a8 38 01 0f c8 e0 c7 94 1e 48 a2 ... 8...8- ....H-
0020 6f cf 61 d9 50 18 27 f9 ed 3a 00 00 2c 27 74 78 ... o.a.P'-...,'tx
0030 74 2e 68 75 72 62 27 5b 20 2c 27 73 65 67 61 6d ... t.hurb'[ , 'segam
0040 49 27 20 2c 27 79 70 2e 72 65 76 72 65 73 27 20 ... I' , 'yp. revres'
0050 2c 27 79 70 2e 73 65 69 74 69 6c 69 74 75 27 20 ... , 'yp.sei tilitu'
0060 5d 27 5f 5f 65 68 63 61 63 79 70 5f 5f 27 00 ... ]'__ehca cyp__.
```

## Plaintext: cd Images command

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
37	12.231575	192.168.56.1	192.168.56.1	TCP	46	64240 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=10233 Len=2
38	12.231699	192.168.56.1	192.168.56.1	TCP	44	4040 → 64240 [ACK] Seq=1 Ack=3 Win=10233 Len=0
51	18.769285	192.168.56.1	192.168.56.1	TCP	54	64240 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=10233 Len=10
52	18.769364	192.168.56.1	192.168.56.1	TCP	44	4040 → 64240 [ACK] Seq=1 Ack=13 Win=10233 Len=0
53	18.777290	192.168.56.1	192.168.56.1	TCP	78	4040 → 64240 [PSH, ACK] Seq=1 Ack=13 Win=10233 Len=34
54	18.777384	192.168.56.1	192.168.56.1	TCP	44	64240 → 4040 [ACK] Seq=13 Ack=35 Win=10233 Len=0
55	18.782818	192.168.56.1	192.168.56.1	TCP	44	64240 → 4040 [FIN, ACK] Seq=13 Ack=35 Win=10233 Len=0
56	18.782939	192.168.56.1	192.168.56.1	TCP	44	4040 → 64240 [ACK] Seq=35 Ack=14 Win=10233 Len=0
57	18.783530	192.168.56.1	192.168.56.1	TCP	44	4040 → 64240 [FIN, ACK] Seq=35 Ack=14 Win=10233 Len=0
58	18.783577	192.168.56.1	192.168.56.1	TCP	44	64240 → 4040 [ACK] Seq=14 Ack=36 Win=10233 Len=0
59	18.792773	192.168.56.1	192.168.56.1	TCP	56	64243 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
60	18.792913	192.168.56.1	192.168.56.1	TCP	56	4040 → 64243 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1

> Frame 51: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 64240, Dst Port: 4040, Seq: 3, Ack: 1, Len: 10

> Data (10 bytes)

```
0000 02 00 00 00 45 00 00 32 c5 3e 40 00 80 06 00 00 ....E..2.>@.....
0010 c0 a8 38 01 c0 a8 38 01 fa f0 0f c8 1f ce 6c a7 ..8...8- .....1-
0020 71 92 64 78 50 18 27 f9 5d c8 00 00 63 64 20 49 q dxP.'.' ]...cd I
0030 6d 61 67 65 73 00      images.
```

## Plaintext: cd Images response

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
37	12.231575	192.168.56.1	192.168.56.1	TCP	46	64240 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=10233 Len=2
38	12.231699	192.168.56.1	192.168.56.1	TCP	44	4040 → 64240 [ACK] Seq=1 Ack=3 Win=10233 Len=0
51	18.769285	192.168.56.1	192.168.56.1	TCP	54	64240 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=10233 Len=10
52	18.769364	192.168.56.1	192.168.56.1	TCP	44	4040 → 64240 [ACK] Seq=1 Ack=13 Win=10233 Len=0
53	18.777290	192.168.56.1	192.168.56.1	TCP	78	4040 → 64240 [PSH, ACK] Seq=1 Ack=13 Win=10233 Len=34
54	18.777384	192.168.56.1	192.168.56.1	TCP	44	64240 → 4040 [ACK] Seq=13 Ack=35 Win=10233 Len=0
55	18.782818	192.168.56.1	192.168.56.1	TCP	44	64240 → 4040 [FIN, ACK] Seq=13 Ack=35 Win=10233 Len=0
56	18.782939	192.168.56.1	192.168.56.1	TCP	44	4040 → 64240 [ACK] Seq=35 Ack=14 Win=10233 Len=0
57	18.783530	192.168.56.1	192.168.56.1	TCP	44	4040 → 64240 [FIN, ACK] Seq=35 Ack=14 Win=10233 Len=0
58	18.783577	192.168.56.1	192.168.56.1	TCP	44	64240 → 4040 [ACK] Seq=14 Ack=36 Win=10233 Len=0
59	18.792773	192.168.56.1	192.168.56.1	TCP	56	64243 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
60	18.792913	192.168.56.1	192.168.56.1	TCP	56	4040 → 64243 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1

> Frame 53: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 4040, Dst Port: 64240, Seq: 1, Ack: 13, Len: 34

> Data (34 bytes)

```
0000 02 00 00 00 45 00 00 4a c5 40 40 00 80 06 00 00 ....E..J.@@.....
0010 c0 a8 38 01 c0 a8 38 01 0f c0 fa f0 71 92 64 78 ..8...8- ....q dx
0020 1f ce 6c b1 50 18 27 f9 8e 28 00 00 43 3a 5c 55 ..1.P.'.' (-C:\U
0030 73 65 72 73 5c 44 45 4c 4c 5c 63 6e 61 73 73 5c sers\DEL L\cnass\
0040 73 65 72 76 65 72 5c 49 6d 61 67 65 73 00      server\I mages.
```

## Substitute: cd Images command

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
310	258.819713	192.168.56.1	192.168.56.1	TCP	54	51962 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=10
311	258.819801	192.168.56.1	192.168.56.1	TCP	44	4040 → 51962 [ACK] Seq=1 Ack=13 Win=2619648 Len=0
312	258.826860	192.168.56.1	192.168.56.1	TCP	78	4040 → 51962 [PSH, ACK] Seq=1 Ack=13 Win=2619648 Len=34
313	258.827012	192.168.56.1	192.168.56.1	TCP	44	51962 → 4040 [ACK] Seq=13 Ack=35 Win=2619648 Len=0
314	258.828110	192.168.56.1	192.168.56.1	TCP	44	51962 → 4040 [FIN, ACK] Seq=13 Ack=35 Win=2619648 Len=0
315	258.828162	192.168.56.1	192.168.56.1	TCP	44	4040 → 51962 [ACK] Seq=35 Ack=14 Win=2619648 Len=0
316	258.828559	192.168.56.1	192.168.56.1	TCP	44	4040 → 51962 [FIN, ACK] Seq=35 Ack=14 Win=2619648 Len=0
317	258.828669	192.168.56.1	192.168.56.1	TCP	44	51962 → 4040 [ACK] Seq=14 Ack=36 Win=2619648 Len=0
318	258.835779	192.168.56.1	192.168.56.1	TCP	56	51963 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
319	258.835903	192.168.56.1	192.168.56.1	TCP	56	4040 → 51963 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
320	258.836012	192.168.56.1	192.168.56.1	TCP	44	51963 → 4040 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
339	347.078260	127.0.0.1	127.0.0.1	TCP	56	51969 → 51968 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1

> Frame 310: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 51962, Dst Port: 4040, Seq: 3, Ack: 1, Len: 10

> Data (10 bytes)

```
0000 02 00 00 00 45 00 00 32 c5 65 40 00 80 06 00 00 ....E..2.e@.....
0010 c0 a8 38 01 c0 a8 38 01 ca fa 0f c8 a5 a2 34 21 ..8...8.....4!
0020 c6 df d2 01 50 18 27 f9 75 91 00 00 65 66 20 4b ....P.'..u...ef K
0030 6f 63 69 67 75 00                                ocigu..
```

## Substitute: cd Images response

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
310	258.819713	192.168.56.1	192.168.56.1	TCP	54	51962 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=10
311	258.819801	192.168.56.1	192.168.56.1	TCP	44	4040 → 51962 [ACK] Seq=1 Ack=13 Win=2619648 Len=0
312	258.826860	192.168.56.1	192.168.56.1	TCP	78	4040 → 51962 [PSH, ACK] Seq=1 Ack=13 Win=2619648 Len=34
313	258.827012	192.168.56.1	192.168.56.1	TCP	44	51962 → 4040 [ACK] Seq=13 Ack=35 Win=2619648 Len=0
314	258.828110	192.168.56.1	192.168.56.1	TCP	44	51962 → 4040 [FIN, ACK] Seq=13 Ack=35 Win=2619648 Len=0
315	258.828162	192.168.56.1	192.168.56.1	TCP	44	4040 → 51962 [ACK] Seq=35 Ack=14 Win=2619648 Len=0
316	258.828559	192.168.56.1	192.168.56.1	TCP	44	4040 → 51962 [FIN, ACK] Seq=35 Ack=14 Win=2619648 Len=0
317	258.828669	192.168.56.1	192.168.56.1	TCP	44	51962 → 4040 [ACK] Seq=14 Ack=36 Win=2619648 Len=0
318	258.835779	192.168.56.1	192.168.56.1	TCP	56	51963 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
319	258.835903	192.168.56.1	192.168.56.1	TCP	56	4040 → 51963 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
320	258.836012	192.168.56.1	192.168.56.1	TCP	44	51963 → 4040 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
339	347.078260	127.0.0.1	127.0.0.1	TCP	56	51969 → 51968 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1

> Frame 312: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 4040, Dst Port: 51962, Seq: 1, Ack: 13, Len: 34

> Data (34 bytes)

```
0000 02 00 00 00 45 00 00 4a c5 67 40 00 80 06 00 00 ....E..J..g@.....
0010 c0 a8 38 01 c0 a8 38 01 0f c8 ca fa c6 df d2 01 ..8...8.....
0020 a5 a2 34 2b 50 18 27 f9 91 df 00 00 45 3a 5c 57 ..4+P.'...E:W
0030 75 67 74 75 5c 46 47 4e 4e 5c 65 70 63 75 75 5c ugtu\FGN\epcuu\
0040 75 67 74 78 67 74 5c 4b 6f 63 69 67 75 00      ugtxtg\K ocigu..
```



## Transpose: cd Images command

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
583	553.401713	192.168.56.1	192.168.56.1	TCP	54	51983 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=10
584	553.401779	192.168.56.1	192.168.56.1	TCP	44	4040 → 51983 [ACK] Seq=1 Ack=13 Win=2619648 Len=0
585	553.408920	192.168.56.1	192.168.56.1	TCP	70	4040 → 51983 [PSH, ACK] Seq=1 Ack=13 Win=2619648 Len=26
586	553.409008	192.168.56.1	192.168.56.1	TCP	44	51983 → 4040 [ACK] Seq=13 Ack=27 Win=2619648 Len=0
587	553.409418	192.168.56.1	192.168.56.1	TCP	44	51983 → 4040 [FIN, ACK] Seq=13 Ack=27 Win=2619648 Len=0
588	553.409460	192.168.56.1	192.168.56.1	TCP	44	4040 → 51983 [ACK] Seq=27 Ack=14 Win=2619648 Len=0
589	553.409988	192.168.56.1	192.168.56.1	TCP	44	4040 → 51983 [FIN, ACK] Seq=27 Ack=14 Win=2619648 Len=0
590	553.410040	192.168.56.1	192.168.56.1	TCP	44	51983 → 4040 [ACK] Seq=14 Ack=28 Win=2619648 Len=0
591	553.415110	192.168.56.1	192.168.56.1	TCP	56	51999 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
592	553.415235	192.168.56.1	192.168.56.1	TCP	56	4040 → 51999 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
593	553.415403	192.168.56.1	192.168.56.1	TCP	44	51999 → 4040 [ACK] Seq=1 Ack=1 Win=327424 Len=0
594	557.186834	192.168.56.1	192.168.56.1	TCP	46	51999 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=327424 Len=2

> Frame 583: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 51983, Dst Port: 4040, Seq: 3, Ack: 1, Len: 10

> Data (10 bytes)

0000 02 00 00 00 45 00 00 32 c5 8c 40 00 80 06 00 00 .....E..2..@.....  
0010 c0 a8 38 01 c0 a8 38 01 cb 0f 0f c8 fc 9d 3c b2 --8---8-.....<.  
0020 68 0c 5b 8d 50 18 27 f9 2a 09 00 00 64 63 20 73 h[.P.'.'\*....dc s  
0030 65 67 61 6d 49 00 egamI-

## Transpose: cd Images response

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
604	558.428780	192.168.56.1	192.168.56.1	TCP	56	52000 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
605	558.428927	192.168.56.1	192.168.56.1	TCP	56	4040 → 52000 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
606	558.429005	192.168.56.1	192.168.56.1	TCP	44	52000 → 4040 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
607	560.001012	192.168.56.1	192.168.56.1	TCP	46	52000 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
608	560.001094	192.168.56.1	192.168.56.1	TCP	44	4040 → 52000 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
609	563.623965	192.168.56.1	192.168.56.1	TCP	54	52000 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=10
610	563.624032	192.168.56.1	192.168.56.1	TCP	44	4040 → 52000 [ACK] Seq=1 Ack=13 Win=2619648 Len=0
611	563.627097	192.168.56.1	192.168.56.1	TCP	78	4040 → 52000 [PSH, ACK] Seq=1 Ack=13 Win=2619648 Len=34
612	563.627137	192.168.56.1	192.168.56.1	TCP	44	52000 → 4040 [ACK] Seq=13 Ack=35 Win=2619648 Len=0
613	563.630327	192.168.56.1	192.168.56.1	TCP	44	4040 → 52000 [FIN, ACK] Seq=35 Ack=13 Win=2619648 Len=0
614	563.630377	192.168.56.1	192.168.56.1	TCP	44	52000 → 4040 [ACK] Seq=13 Ack=36 Win=2619648 Len=0
615	563.631462	192.168.56.1	192.168.56.1	TCP	44	52000 → 4040 [FIN, ACK] Seq=13 Ack=36 Win=2619648 Len=0

> Frame 611: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

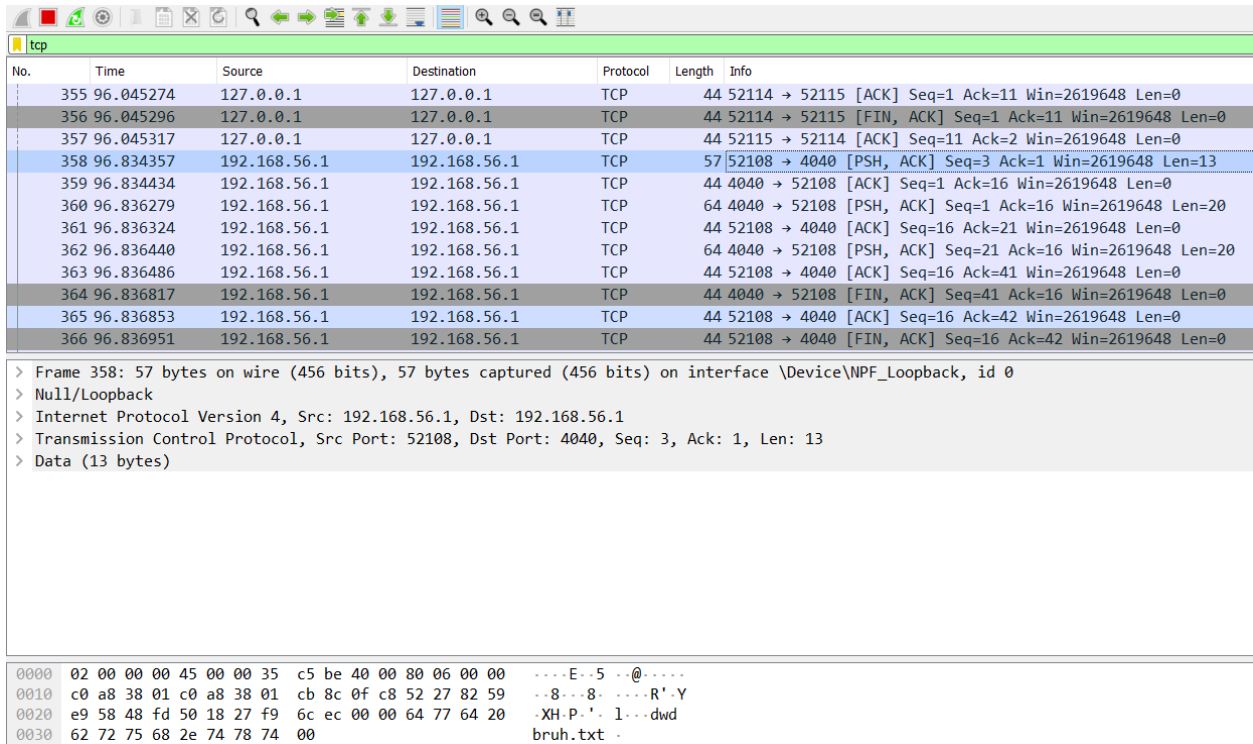
> Transmission Control Protocol, Src Port: 4040, Dst Port: 52000, Seq: 1, Ack: 13, Len: 34

> Data (34 bytes)

0000 02 00 00 00 45 00 00 4a c5 a8 40 00 80 06 00 00 .....J..@.....  
0010 c0 a8 38 01 c0 a8 38 01 0f c8 cb 20 cf 25 5b 19 --8---8-...-%[.  
0020 60 03 91 26 50 18 27 f9 05 1a 00 00 73 65 67 61 `..&P.'.'....sega  
0030 6d 49 5c 72 65 76 72 65 73 5c 73 73 61 6e 63 5c mI\revre s\ssanc\  
0040 4c 4c 45 44 5c 73 72 65 73 55 5c 3a 43 00 LLED\sre sU\C-



## Plaintext: dwd bruh.txt command



tcp

No.	Time	Source	Destination	Protocol	Length	Info
355	96.045274	127.0.0.1	127.0.0.1	TCP	44	52114 → 52115 [ACK] Seq=1 Ack=11 Win=2619648 Len=0
356	96.045296	127.0.0.1	127.0.0.1	TCP	44	52114 → 52115 [FIN, ACK] Seq=1 Ack=11 Win=2619648 Len=0
357	96.045317	127.0.0.1	127.0.0.1	TCP	44	52115 → 52114 [ACK] Seq=11 Ack=2 Win=2619648 Len=0
358	96.834357	192.168.56.1	192.168.56.1	TCP	57	52108 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
359	96.834434	192.168.56.1	192.168.56.1	TCP	44	4040 → 52108 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
360	96.836279	192.168.56.1	192.168.56.1	TCP	64	4040 → 52108 [PSH, ACK] Seq=1 Ack=16 Win=2619648 Len=20
361	96.836324	192.168.56.1	192.168.56.1	TCP	44	52108 → 4040 [ACK] Seq=16 Ack=21 Win=2619648 Len=0
362	96.836440	192.168.56.1	192.168.56.1	TCP	64	4040 → 52108 [PSH, ACK] Seq=21 Ack=16 Win=2619648 Len=20
363	96.836486	192.168.56.1	192.168.56.1	TCP	44	52108 → 4040 [ACK] Seq=16 Ack=41 Win=2619648 Len=0
364	96.836817	192.168.56.1	192.168.56.1	TCP	44	4040 → 52108 [FIN, ACK] Seq=41 Ack=16 Win=2619648 Len=0
365	96.836853	192.168.56.1	192.168.56.1	TCP	44	52108 → 4040 [ACK] Seq=16 Ack=42 Win=2619648 Len=0
366	96.836951	192.168.56.1	192.168.56.1	TCP	44	52108 → 4040 [FIN, ACK] Seq=16 Ack=42 Win=2619648 Len=0

> Frame 358: 57 bytes on wire (456 bits), 57 bytes captured (456 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

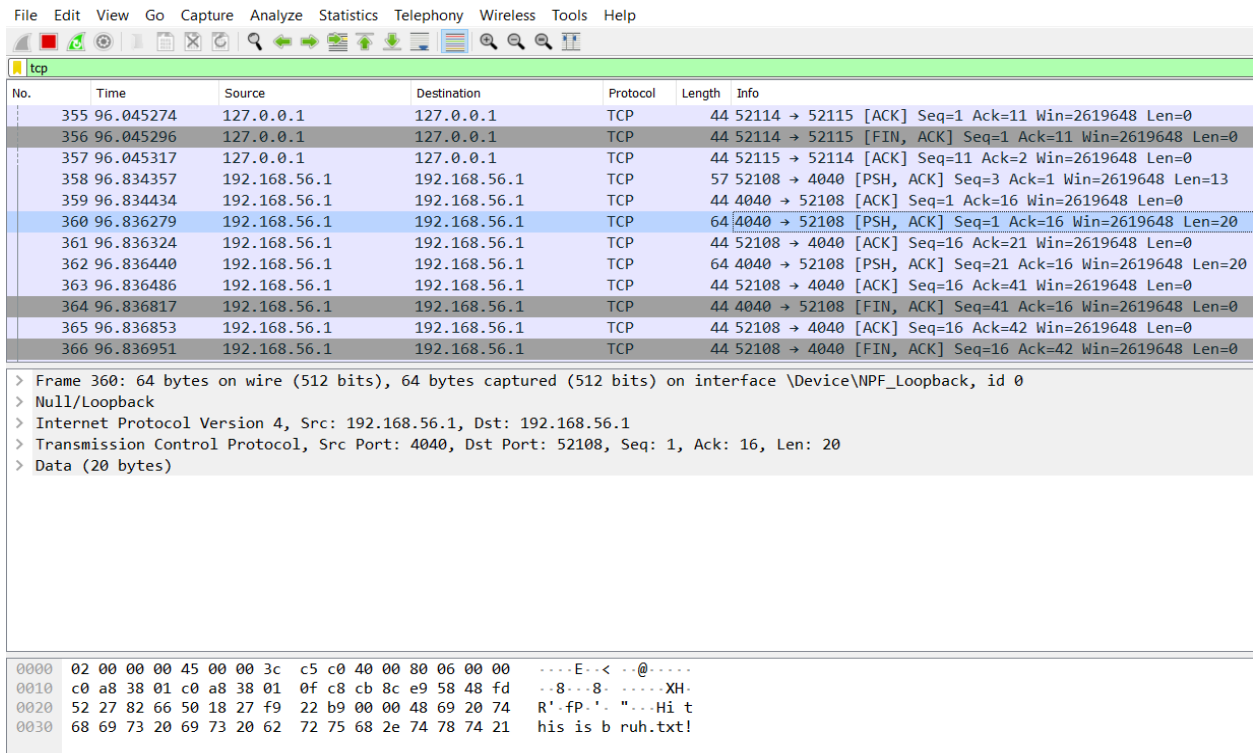
> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 52108, Dst Port: 4040, Seq: 3, Ack: 1, Len: 13

> Data (13 bytes)

```
0000  02 00 00 00 45 00 00 35 c5 be 40 00 80 06 00 00  ....E..5..@.....
0010  c0 a8 38 01 c0 a8 38 01 cb 8c 0f c8 52 27 82 59  ..8...8...R'.Y
0020  e9 58 48 fd 50 18 27 f9 6c ec 00 00 64 77 64 20  .XH.P.'..l...dwd
0030  62 72 75 68 2e 74 78 74 00                      bruh.txt ..
```

## Plaintext: dwd bruh.txt response



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
355	96.045274	127.0.0.1	127.0.0.1	TCP	44	52114 → 52115 [ACK] Seq=1 Ack=11 Win=2619648 Len=0
356	96.045296	127.0.0.1	127.0.0.1	TCP	44	52114 → 52115 [FIN, ACK] Seq=1 Ack=11 Win=2619648 Len=0
357	96.045317	127.0.0.1	127.0.0.1	TCP	44	52115 → 52114 [ACK] Seq=11 Ack=2 Win=2619648 Len=0
358	96.834357	192.168.56.1	192.168.56.1	TCP	57	52108 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
359	96.834434	192.168.56.1	192.168.56.1	TCP	44	4040 → 52108 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
360	96.836279	192.168.56.1	192.168.56.1	TCP	64	4040 → 52108 [PSH, ACK] Seq=1 Ack=16 Win=2619648 Len=20
361	96.836324	192.168.56.1	192.168.56.1	TCP	44	52108 → 4040 [ACK] Seq=16 Ack=21 Win=2619648 Len=0
362	96.836440	192.168.56.1	192.168.56.1	TCP	64	4040 → 52108 [PSH, ACK] Seq=21 Ack=16 Win=2619648 Len=20
363	96.836486	192.168.56.1	192.168.56.1	TCP	44	52108 → 4040 [ACK] Seq=16 Ack=41 Win=2619648 Len=0
364	96.836817	192.168.56.1	192.168.56.1	TCP	44	4040 → 52108 [FIN, ACK] Seq=41 Ack=16 Win=2619648 Len=0
365	96.836853	192.168.56.1	192.168.56.1	TCP	44	52108 → 4040 [ACK] Seq=16 Ack=42 Win=2619648 Len=0
366	96.836951	192.168.56.1	192.168.56.1	TCP	44	52108 → 4040 [FIN, ACK] Seq=16 Ack=42 Win=2619648 Len=0

> Frame 360: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 4040, Dst Port: 52108, Seq: 1, Ack: 16, Len: 20

> Data (20 bytes)

```
0000  02 00 00 00 45 00 00 3c c5 c0 40 00 80 06 00 00  ....E...<..@.....
0010  c0 a8 38 01 c0 a8 38 01 0f c8 cb 8c e9 58 48 fd  ..8...8...XH.
0020  52 27 82 66 50 18 27 f9 22 b9 00 00 48 69 20 74  R'.fP.'.. "...Hi t
0030  68 69 73 20 69 73 20 62 72 75 68 2e 74 78 74 21  his is b ruh.txt!
```

## Substitute: dwd bruh.txt command

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
466	168.448666	192.168.56.1	192.168.56.1	TCP	44	4040 → 52119 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
467	173.637604	192.168.56.1	192.168.56.1	TCP	57	52119 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
468	173.637697	192.168.56.1	192.168.56.1	TCP	44	4040 → 52119 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
469	173.639606	192.168.56.1	192.168.56.1	TCP	64	4040 → 52119 [PSH, ACK] Seq=1 Ack=16 Win=2619648 Len=20
470	173.639672	192.168.56.1	192.168.56.1	TCP	44	52119 → 4040 [ACK] Seq=16 Ack=21 Win=2619648 Len=0
471	173.639812	192.168.56.1	192.168.56.1	TCP	64	4040 → 52119 [PSH, ACK] Seq=21 Ack=16 Win=2619648 Len=20
472	173.639934	192.168.56.1	192.168.56.1	TCP	44	52119 → 4040 [ACK] Seq=16 Ack=41 Win=2619648 Len=0
473	173.640240	192.168.56.1	192.168.56.1	TCP	44	4040 → 52119 [FIN, ACK] Seq=41 Ack=16 Win=2619648 Len=0
474	173.640298	192.168.56.1	192.168.56.1	TCP	44	52119 → 4040 [ACK] Seq=16 Ack=42 Win=2619648 Len=0
475	173.640701	192.168.56.1	192.168.56.1	TCP	44	52119 → 4040 [FIN, ACK] Seq=16 Ack=42 Win=2619648 Len=0
476	173.640779	192.168.56.1	192.168.56.1	TCP	44	4040 → 52119 [ACK] Seq=42 Ack=17 Win=2619648 Len=0
477	173.641619	192.168.56.1	192.168.56.1	TCP	56	52149 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1

> Frame 467: 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: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 52119, Dst Port: 4040, Seq: 3, Ack: 1, Len: 13

> Data (13 bytes)

```
0000 02 00 00 00 45 00 00 35 c5 cd 40 00 80 06 00 00  ....E--5 --@-----
0010 c0 a8 38 01 c0 a8 38 01 cb 97 0f c8 0c 42 9b 43  ..8...8- .....B.C
0020 15 11 75 d5 50 18 27 f9 37 42 00 00 66 79 66 20  ..u.P.'- 7B--fyf
0030 64 74 77 6a 2e 76 7a 76 00 dtwj.vzv -
```

## Substitute: dwd bruh.txt response

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
466	168.448666	192.168.56.1	192.168.56.1	TCP	44	4040 → 52119 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
467	173.637604	192.168.56.1	192.168.56.1	TCP	57	52119 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
468	173.637697	192.168.56.1	192.168.56.1	TCP	44	4040 → 52119 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
469	173.639606	192.168.56.1	192.168.56.1	TCP	64	4040 → 52119 [PSH, ACK] Seq=1 Ack=16 Win=2619648 Len=20
470	173.639672	192.168.56.1	192.168.56.1	TCP	44	52119 → 4040 [ACK] Seq=16 Ack=21 Win=2619648 Len=0
471	173.639812	192.168.56.1	192.168.56.1	TCP	64	4040 → 52119 [PSH, ACK] Seq=21 Ack=16 Win=2619648 Len=20
472	173.639934	192.168.56.1	192.168.56.1	TCP	44	52119 → 4040 [ACK] Seq=16 Ack=41 Win=2619648 Len=0
473	173.640240	192.168.56.1	192.168.56.1	TCP	44	4040 → 52119 [FIN, ACK] Seq=41 Ack=16 Win=2619648 Len=0
474	173.640298	192.168.56.1	192.168.56.1	TCP	44	52119 → 4040 [ACK] Seq=16 Ack=42 Win=2619648 Len=0
475	173.640701	192.168.56.1	192.168.56.1	TCP	44	52119 → 4040 [FIN, ACK] Seq=16 Ack=42 Win=2619648 Len=0
476	173.640779	192.168.56.1	192.168.56.1	TCP	44	4040 → 52119 [ACK] Seq=42 Ack=17 Win=2619648 Len=0
477	173.641619	192.168.56.1	192.168.56.1	TCP	56	52149 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1

> Frame 469: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 4040, Dst Port: 52119, Seq: 1, Ack: 16, Len: 20

> Data (20 bytes)

```
0000 02 00 00 00 45 00 00 3c c5 cf 40 00 80 06 00 00  ....E--< --@-----
0010 c0 a8 38 01 c0 a8 38 01 0f c8 cb 97 15 11 75 d5  ..8...8- .....u.
0020 0c 42 9b 50 50 18 27 f9 e7 0a 00 00 4a 6b 20 76  -B.PP.'- ....Jk v
0030 6a 6b 75 20 6b 75 20 64 74 77 6a 2e 76 7a 76 21  jku ku d twj.vzv!
```

## Transpose: dwd bruh.txt command

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
475	173.640701	192.168.56.1	192.168.56.1	TCP	44	52119 → 4040 [FIN, ACK] Seq=16 Ack=42 Win=2619648 Len=0
476	173.640779	192.168.56.1	192.168.56.1	TCP	44	4040 → 52119 [ACK] Seq=42 Ack=17 Win=2619648 Len=0
477	173.641619	192.168.56.1	192.168.56.1	TCP	56	52149 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
478	173.641688	192.168.56.1	192.168.56.1	TCP	56	4040 → 52149 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
479	173.641753	192.168.56.1	192.168.56.1	TCP	44	52149 → 4040 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
495	249.232841	192.168.56.1	192.168.56.1	TCP	46	52149 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
496	249.232939	192.168.56.1	192.168.56.1	TCP	44	4040 → 52149 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
499	252.940580	192.168.56.1	192.168.56.1	TCP	57	52149 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
500	252.940680	192.168.56.1	192.168.56.1	TCP	44	4040 → 52149 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
501	252.942014	192.168.56.1	192.168.56.1	TCP	64	4040 → 52149 [PSH, ACK] Seq=1 Ack=16 Win=2619648 Len=20
502	252.942058	192.168.56.1	192.168.56.1	TCP	44	52149 → 4040 [ACK] Seq=16 Ack=21 Win=2619648 Len=0
503	252.942215	192.168.56.1	192.168.56.1	TCP	64	4040 → 52149 [PSH, ACK] Seq=21 Ack=16 Win=2619648 Len=20

> Frame 499: 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: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 52149, Dst Port: 4040, Seq: 3, Ack: 1, Len: 13

> Data (13 bytes)

```
0000 02 00 00 00 45 00 00 35 c5 dc 40 00 80 06 00 00 ....E--5 --@-----
0010 c0 a8 38 01 c0 a8 38 01 cb b5 0f c8 f6 64 e6 b5 ..8...8. ....d..
0020 9b 3e 4b fd 50 18 27 f9 6a 88 00 00 64 77 64 20 ->K.P.' j...dwd
0030 74 78 74 2e 68 75 72 62 00 txt.hurb ..
```

## Transpose: dwd bruh.txt response

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
475	173.640701	192.168.56.1	192.168.56.1	TCP	44	52119 → 4040 [FIN, ACK] Seq=16 Ack=42 Win=2619648 Len=0
476	173.640779	192.168.56.1	192.168.56.1	TCP	44	4040 → 52119 [ACK] Seq=42 Ack=17 Win=2619648 Len=0
477	173.641619	192.168.56.1	192.168.56.1	TCP	56	52149 → 4040 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
478	173.641688	192.168.56.1	192.168.56.1	TCP	56	4040 → 52149 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
479	173.641753	192.168.56.1	192.168.56.1	TCP	44	52149 → 4040 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
495	249.232841	192.168.56.1	192.168.56.1	TCP	46	52149 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
496	249.232939	192.168.56.1	192.168.56.1	TCP	44	4040 → 52149 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
499	252.940580	192.168.56.1	192.168.56.1	TCP	57	52149 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
500	252.940680	192.168.56.1	192.168.56.1	TCP	44	4040 → 52149 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
501	252.942014	192.168.56.1	192.168.56.1	TCP	64	4040 → 52149 [PSH, ACK] Seq=1 Ack=16 Win=2619648 Len=20
502	252.942058	192.168.56.1	192.168.56.1	TCP	44	52149 → 4040 [ACK] Seq=16 Ack=21 Win=2619648 Len=0
503	252.942215	192.168.56.1	192.168.56.1	TCP	64	4040 → 52149 [PSH, ACK] Seq=21 Ack=16 Win=2619648 Len=20

> Frame 501: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 4040, Dst Port: 52149, Seq: 1, Ack: 16, Len: 20

> Data (20 bytes)

```
0000 02 00 00 00 45 00 00 3c c5 de 40 00 80 06 00 00 ....E--< --@-----
0010 c0 a8 38 01 c0 a8 38 01 0f c8 cb b5 9b 3e 4b fd ..8...8. ....>K.
0020 f6 64 e6 c2 50 18 27 f9 38 3d 00 00 69 48 20 73 .d .P.' 8=...iH s
0030 69 68 74 20 73 69 20 21 74 78 74 2e 68 75 72 62 iht si ! txt.hurb
```

## Plaintext: upd bruh.txt command

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
13	3.575794	192.168.56.1	192.168.56.1	TCP	46	52153 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=1279 Len=2
14	3.575899	192.168.56.1	192.168.56.1	TCP	44	4040 → 52153 [ACK] Seq=1 Ack=3 Win=10233 Len=0
15	7.962544	192.168.56.1	192.168.56.1	TCP	57	52153 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=1279 Len=13
16	7.962645	192.168.56.1	192.168.56.1	TCP	44	4040 → 52153 [ACK] Seq=1 Ack=16 Win=10233 Len=0
17	7.963532	192.168.56.1	192.168.56.1	TCP	64	52153 → 4040 [PSH, ACK] Seq=16 Ack=1 Win=1279 Len=20
18	7.963570	192.168.56.1	192.168.56.1	TCP	44	4040 → 52153 [ACK] Seq=1 Ack=36 Win=10233 Len=0
19	7.965185	192.168.56.1	192.168.56.1	TCP	62	4040 → 52153 [PSH, ACK] Seq=1 Ack=36 Win=10233 Len=18
20	7.965246	192.168.56.1	192.168.56.1	TCP	44	52153 → 4040 [ACK] Seq=36 Ack=19 Win=1279 Len=0
21	7.965590	192.168.56.1	192.168.56.1	TCP	44	4040 → 52153 [FIN, ACK] Seq=19 Ack=36 Win=10233 Len=0
22	7.965652	192.168.56.1	192.168.56.1	TCP	44	52153 → 4040 [FIN, ACK] Seq=36 Ack=19 Win=1279 Len=0
23	7.965662	192.168.56.1	192.168.56.1	TCP	44	52153 → 4040 [ACK] Seq=37 Ack=20 Win=1279 Len=0
24	7.965839	192.168.56.1	192.168.56.1	TCP	44	4040 → 52153 [ACK] Seq=20 Ack=37 Win=10233 Len=0

> Frame 15: 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: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 52153, Dst Port: 4040, Seq: 3, Ack: 1, Len: 13

> Data (13 bytes)

```
0000 02 00 00 00 45 00 00 35 c5 eb 40 00 80 06 00 00  ....E..5 ..@....
0010 c0 a8 38 01 c0 a8 38 01 cb b9 0f c8 6f a9 73 2d  ..8...8- .....o-s-
0020 30 b0 b9 84 50 18 04 ff b8 8b 00 00 75 70 64 20  0...P... ..upd
0030 62 72 75 68 2e 74 78 74 00                    bruh.txt ..
```

## Plaintext: upd bruh.txt response

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
13	3.575794	192.168.56.1	192.168.56.1	TCP	46	52153 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=1279 Len=2
14	3.575899	192.168.56.1	192.168.56.1	TCP	44	4040 → 52153 [ACK] Seq=1 Ack=3 Win=10233 Len=0
15	7.962544	192.168.56.1	192.168.56.1	TCP	57	52153 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=1279 Len=13
16	7.962645	192.168.56.1	192.168.56.1	TCP	44	4040 → 52153 [ACK] Seq=1 Ack=16 Win=10233 Len=0
17	7.963532	192.168.56.1	192.168.56.1	TCP	64	52153 → 4040 [PSH, ACK] Seq=16 Ack=1 Win=1279 Len=20
18	7.963570	192.168.56.1	192.168.56.1	TCP	44	4040 → 52153 [ACK] Seq=1 Ack=36 Win=10233 Len=0
19	7.965185	192.168.56.1	192.168.56.1	TCP	62	4040 → 52153 [PSH, ACK] Seq=1 Ack=36 Win=10233 Len=18
20	7.965246	192.168.56.1	192.168.56.1	TCP	44	52153 → 4040 [ACK] Seq=36 Ack=19 Win=1279 Len=0
21	7.965590	192.168.56.1	192.168.56.1	TCP	44	4040 → 52153 [FIN, ACK] Seq=19 Ack=36 Win=10233 Len=0
22	7.965652	192.168.56.1	192.168.56.1	TCP	44	52153 → 4040 [FIN, ACK] Seq=36 Ack=19 Win=1279 Len=0
23	7.965662	192.168.56.1	192.168.56.1	TCP	44	52153 → 4040 [ACK] Seq=37 Ack=20 Win=1279 Len=0
24	7.965839	192.168.56.1	192.168.56.1	TCP	44	4040 → 52153 [ACK] Seq=20 Ack=37 Win=10233 Len=0

> Frame 17: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 52153, Dst Port: 4040, Seq: 16, Ack: 1, Len: 20

> Data (20 bytes)

```
0000 02 00 00 00 45 00 00 3c c5 ed 40 00 80 06 00 00  ....E...< ..@....
0010 c0 a8 38 01 c0 a8 38 01 cb b9 0f c8 6f a9 73 3a  ..8...8- .....o-s:
0020 30 b0 b9 84 50 18 04 ff 7f 51 00 00 48 69 20 74  0...P... ..Q..Hi t
0030 68 69 73 20 69 73 20 62 72 75 68 2e 74 78 74 21  his is b ruh.txt!
```

## Substitute: upd bruh.txt command

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
325	299.067471	192.168.56.1	192.168.56.1	TCP	46	52225 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
326	299.067562	192.168.56.1	192.168.56.1	TCP	44	4040 → 52225 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
327	304.197182	192.168.56.1	192.168.56.1	TCP	57	52225 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
328	304.197264	192.168.56.1	192.168.56.1	TCP	44	4040 → 52225 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
329	304.198260	192.168.56.1	192.168.56.1	TCP	64	52225 → 4040 [PSH, ACK] Seq=16 Ack=1 Win=2619648 Len=20
330	304.198299	192.168.56.1	192.168.56.1	TCP	44	4040 → 52225 [ACK] Seq=1 Ack=36 Win=2619648 Len=0
331	304.203949	192.168.56.1	192.168.56.1	TCP	62	4040 → 52225 [PSH, ACK] Seq=1 Ack=36 Win=2619648 Len=18
332	304.204021	192.168.56.1	192.168.56.1	TCP	44	52225 → 4040 [ACK] Seq=36 Ack=19 Win=2619648 Len=0
333	304.204597	192.168.56.1	192.168.56.1	TCP	44	52225 → 4040 [FIN, ACK] Seq=36 Ack=19 Win=2619648 Len=0
334	304.204648	192.168.56.1	192.168.56.1	TCP	44	4040 → 52225 [FIN, ACK] Seq=19 Ack=36 Win=2619648 Len=0
335	304.204655	192.168.56.1	192.168.56.1	TCP	44	4040 → 52225 [ACK] Seq=20 Ack=37 Win=2619648 Len=0
336	304.204749	192.168.56.1	192.168.56.1	TCP	44	52225 → 4040 [ACK] Seq=37 Ack=20 Win=2619648 Len=0

> Frame 327: 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: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 52225, Dst Port: 4040, Seq: 3, Ack: 1, Len: 13

> Data (13 bytes)

```
0000 02 00 00 00 45 00 00 35 c6 0a 40 00 80 06 00 00 ....E--5..@.....
0010 c0 a8 38 01 c0 a8 38 01 cc 01 0f c8 ce bd 9a 87 ..8...8-.....
0020 e5 d8 a2 13 50 18 27 f9 67 19 00 00 77 72 66 20 ....P.'..g...wrf
0030 64 74 77 6a 2e 76 7a 76 00 dtwj.vzv -
```

## Substitute: upd bruh.txt response

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
325	299.067471	192.168.56.1	192.168.56.1	TCP	46	52225 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
326	299.067562	192.168.56.1	192.168.56.1	TCP	44	4040 → 52225 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
327	304.197182	192.168.56.1	192.168.56.1	TCP	57	52225 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
328	304.197264	192.168.56.1	192.168.56.1	TCP	44	4040 → 52225 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
329	304.198260	192.168.56.1	192.168.56.1	TCP	64	52225 → 4040 [PSH, ACK] Seq=16 Ack=1 Win=2619648 Len=20
330	304.198299	192.168.56.1	192.168.56.1	TCP	44	4040 → 52225 [ACK] Seq=1 Ack=36 Win=2619648 Len=0
331	304.203949	192.168.56.1	192.168.56.1	TCP	62	4040 → 52225 [PSH, ACK] Seq=1 Ack=36 Win=2619648 Len=18
332	304.204021	192.168.56.1	192.168.56.1	TCP	44	52225 → 4040 [ACK] Seq=36 Ack=19 Win=2619648 Len=0
333	304.204597	192.168.56.1	192.168.56.1	TCP	44	52225 → 4040 [FIN, ACK] Seq=36 Ack=19 Win=2619648 Len=0
334	304.204648	192.168.56.1	192.168.56.1	TCP	44	4040 → 52225 [FIN, ACK] Seq=19 Ack=36 Win=2619648 Len=0
335	304.204655	192.168.56.1	192.168.56.1	TCP	44	4040 → 52225 [ACK] Seq=20 Ack=37 Win=2619648 Len=0
336	304.204749	192.168.56.1	192.168.56.1	TCP	44	52225 → 4040 [ACK] Seq=37 Ack=20 Win=2619648 Len=0

> Frame 329: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 52225, Dst Port: 4040, Seq: 16, Ack: 1, Len: 20

> Data (20 bytes)

```
0000 02 00 00 00 45 00 00 3c c6 0c 40 00 80 06 00 00 ....E--<..@.....
0010 c0 a8 38 01 c0 a8 38 01 cc 01 0f c8 ce bd 9a 94 ..8...8-.....
0020 e5 d8 a2 13 50 18 27 f9 27 db 00 00 4a 6b 20 76 ....P.'..'..Jk v
0030 6a 6b 75 20 6b 75 20 64 74 77 6a 2e 76 7a 76 21 jku ku d twj.vzv!
```

## Transpose: upd bruh.txt command

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
395	368.362856	127.0.0.1	127.0.0.1	TCP	44	63427 → 63428 [ACK] Seq=1 Ack=11 Win=2619648 Len=0
396	368.362965	127.0.0.1	127.0.0.1	TCP	44	63427 → 63428 [FIN, ACK] Seq=1 Ack=11 Win=2619648 Len=0
397	368.363019	127.0.0.1	127.0.0.1	TCP	44	63428 → 63427 [ACK] Seq=11 Ack=2 Win=2619648 Len=0
412	404.402151	192.168.56.1	192.168.56.1	TCP	46	63410 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
413	404.402242	192.168.56.1	192.168.56.1	TCP	44	4040 → 63410 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
418	407.397286	192.168.56.1	192.168.56.1	TCP	57	63410 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
419	407.397375	192.168.56.1	192.168.56.1	TCP	44	4040 → 63410 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
420	407.398300	192.168.56.1	192.168.56.1	TCP	64	63410 → 4040 [PSH, ACK] Seq=16 Ack=1 Win=2619648 Len=20
421	407.398374	192.168.56.1	192.168.56.1	TCP	44	4040 → 63410 [ACK] Seq=1 Ack=36 Win=2619648 Len=0
422	407.400995	192.168.56.1	192.168.56.1	TCP	62	4040 → 63410 [PSH, ACK] Seq=1 Ack=36 Win=2619648 Len=18
423	407.401057	192.168.56.1	192.168.56.1	TCP	44	63410 → 4040 [ACK] Seq=36 Ack=19 Win=2619648 Len=0
424	407.402776	192.168.56.1	192.168.56.1	TCP	44	4040 → 63410 [FIN, ACK] Seq=19 Ack=36 Win=2619648 Len=0

> Frame 418: 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: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 63410, Dst Port: 4040, Seq: 3, Ack: 1, Len: 13

> Data (13 bytes)

```
0000  02 00 00 00 45 00 00 35 c6 19 40 00 80 06 00 00  ....E..5..@.....
0010  c0 a8 38 01 c0 a8 38 01 f7 b2 0f c8 57 55 98 8c  ...8...8....WU..
0020  5c 2c 52 40 50 18 27 f9 53 9a 00 00 64 70 75 20  \,R@P.'.'S...dpu
0030  74 78 74 2e 68 75 72 62 00                      txt.hurb ..
```

## Transpose: upd bruh.txt response

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
395	368.362856	127.0.0.1	127.0.0.1	TCP	44	63427 → 63428 [ACK] Seq=1 Ack=11 Win=2619648 Len=0
396	368.362965	127.0.0.1	127.0.0.1	TCP	44	63427 → 63428 [FIN, ACK] Seq=1 Ack=11 Win=2619648 Len=0
397	368.363019	127.0.0.1	127.0.0.1	TCP	44	63428 → 63427 [ACK] Seq=11 Ack=2 Win=2619648 Len=0
412	404.402151	192.168.56.1	192.168.56.1	TCP	46	63410 → 4040 [PSH, ACK] Seq=1 Ack=1 Win=2619648 Len=2
413	404.402242	192.168.56.1	192.168.56.1	TCP	44	4040 → 63410 [ACK] Seq=1 Ack=3 Win=2619648 Len=0
418	407.397286	192.168.56.1	192.168.56.1	TCP	57	63410 → 4040 [PSH, ACK] Seq=3 Ack=1 Win=2619648 Len=13
419	407.397375	192.168.56.1	192.168.56.1	TCP	44	4040 → 63410 [ACK] Seq=1 Ack=16 Win=2619648 Len=0
420	407.398300	192.168.56.1	192.168.56.1	TCP	64	63410 → 4040 [PSH, ACK] Seq=16 Ack=1 Win=2619648 Len=20
421	407.398374	192.168.56.1	192.168.56.1	TCP	44	4040 → 63410 [ACK] Seq=1 Ack=36 Win=2619648 Len=0
422	407.400995	192.168.56.1	192.168.56.1	TCP	62	4040 → 63410 [PSH, ACK] Seq=1 Ack=36 Win=2619648 Len=18
423	407.401057	192.168.56.1	192.168.56.1	TCP	44	63410 → 4040 [ACK] Seq=36 Ack=19 Win=2619648 Len=0
424	407.402776	192.168.56.1	192.168.56.1	TCP	44	4040 → 63410 [FIN, ACK] Seq=19 Ack=36 Win=2619648 Len=0

> Frame 420: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 192.168.56.1

> Transmission Control Protocol, Src Port: 63410, Dst Port: 4040, Seq: 16, Ack: 1, Len: 20

> Data (20 bytes)

```
0000  02 00 00 00 45 00 00 3c c6 1b 40 00 80 06 00 00  ....E-<..@.....
0010  c0 a8 38 01 c0 a8 38 01 f7 b2 0f c8 57 55 98 99  ...8...8....WU..
0020  5c 2c 52 40 50 18 27 f9 32 48 00 00 69 48 20 73  \,R@P.'.'2H...iH s
0030  69 68 74 20 73 69 20 21 74 78 74 2e 68 75 72 62  iht si ! txt.hurb
```



## Part 3: Network Tools

5) a) List at-least 5 different network protocols that we have not discussed so far in the classroom and describe in 1-2 sentences the operation/usage of protocol and its layer of operation and indicate the associated RFC number if any

a) **MDNS**: Multicast DNS (mDNS) protocol resolves hostnames to IP addresses within small networks that do not include a local name server. Its RFC number is 6762.

Capturing from Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
175	60.139793	10.7.56.70	10.7.63.255	NBNS	82	Name query NB HTTPS<00>
176	60.140932	192.168.56.1	192.168.56.255	NBNS	82	Name query NB HTTPS<00>
177	60.355244	192.168.56.1	224.0.0.251	MDNS	61	Standard query 0x0000 A https.local, "QM" question
178	60.355835	10.7.56.70	224.0.0.251	MDNS	61	Standard query 0x0000 A https.local, "QM" question
179	60.356593	fe80::e881:538f:733..ff02::fb		MDNS	81	Standard query 0x0000 A https.local, "QM" question
180	60.356798	fe80::e881:7249:277..ff02::fb		MDNS	81	Standard query 0x0000 A https.local, "QM" question
181	60.357146	192.168.56.1	224.0.0.251	MDNS	61	Standard query 0x0000 AAAA https.local, "QM" question
182	60.357355	10.7.56.70	224.0.0.251	MDNS	61	Standard query 0x0000 AAAA https.local, "QM" question
183	60.357585	fe80::e881:538f:733..ff02::fb		MDNS	81	Standard query 0x0000 AAAA https.local, "QM" question
184	60.357730	fe80::e881:7249:277..ff02::fb		MDNS	81	Standard query 0x0000 AAAA https.local, "QM" question
185	60.401827	192.168.56.1	224.0.0.251	MDNS	61	Standard query 0x0000 A https.local, "QM" question
186	60.402246	10.7.56.70	224.0.0.251	MDNS	61	Standard query 0x0000 A https.local, "QM" question

> Frame 60: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF\_{...}\_Loopback, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 10.7.56.70, Dst: 10.7.63.255

> User Datagram Protocol, Src Port: 137, Dst Port: 137

> NetBIOS Name Service

0000 02 00 00 00 45 00 00 4e f7 c3 00 00 80 11 00 00 .....N.....  
0010 0a 07 38 46 0a 07 3f ff 00 89 00 89 00 3a f0 58 --BF--?.....X  
0020 e6 39 01 10 00 01 00 00 00 00 00 20 45 45 45 -9.....EEE  
0030 46 46 44 45 4c 46 45 45 50 46 41 43 4e 46 42 44 FDELFEE PFACFBD  
0040 44 45 44 45 46 44 49 45 49 44 48 42 4d 00 20 DEFEFDE IDHBM  
0050 00 01 ..

b) **SSDP**: The Simple Service Discovery Protocol (SSDP) is a network protocol based on the Internet protocol suite for advertisement and discovery of network services and presence information.

Capturing from Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
6	1.012350	10.7.56.70	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
7	1.016326	192.168.56.1	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
8	1.016366	10.7.56.70	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
9	2.022011	192.168.56.1	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
10	2.022229	10.7.56.70	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
11	2.025154	192.168.56.1	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
12	2.025225	10.7.56.70	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
13	3.035192	192.168.56.1	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
14	3.035206	192.168.56.1	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
15	3.035276	10.7.56.70	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
16	3.035330	10.7.56.70	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
17	9.527980	:::1	:::1	UDP	84	55818 → 55818 Len=32

> Frame 1: 207 bytes on wire (1656 bits), 207 bytes captured (1656 bits) on interface \Device\NPF\_{...}\_Loopback, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.56.1, Dst: 239.255.255.250

> User Datagram Protocol, Src Port: 64784, Dst Port: 1900

> Simple Service Discovery Protocol

0000 02 00 00 00 45 00 00 cb f1 88 00 00 01 11 00 00 .....E.....  
0010 c0 a8 38 01 ef ff ff fa fd 10 07 6c 00 b7 93 c5 --8.....1....  
0020 4d 2d 53 45 41 52 43 48 20 2a 20 48 54 54 50 2f M-SEARCH \* HTTP/  
0030 31 2e 31 0d 0a 48 4f 53 54 3a 20 32 33 39 2e 32 1.1: HOS T: 239.2  
0040 35 35 2e 32 35 2e 32 35 30 3a 31 39 30 30 0d 55.255.2 50:1900  
0050 0a 4d 41 4e 3a 20 22 73 73 64 70 3a 64 69 73 63 .MAN: "s:sd:disc  
0060 6f 76 65 72 22 0d 0a 4d 58 3a 20 31 0d 0a 53 54 over":M X: 1-ST  
0070 3a 20 75 72 6e 3a 64 69 61 6c 2d 6d 75 6c 74 69 : urn:di al-multi  
0080 73 63 72 65 65 6e 2d 6f 72 67 3a 73 65 72 76 69 screen-o rg:servi  
0090 63 65 3a 64 69 61 6c 3a 31 0d 0a 55 53 45 52 2d ce:dial: 1-USER  
00a0 41 47 45 4e 54 3a 20 4d 69 63 72 6f 73 6f 66 74 AGENT: M icrosoft  
00b0 20 45 64 67 65 2f 31 30 35 2e 30 2e 31 33 34 33 Edge/10 5.0.1343  
00c0 2e 33 33 20 57 69 6e 64 6f 77 73 0d 0a 00 0a .33 Wind ows----

c) **NBNS**: NBNS stands for NetBIO Name Service, which is a protocol for name resolution. NBNS performs the same function as LLMNR, but using UDP broadcast packets instead of multi cast packets. Its RFC number is 1001.

Capturing from Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
50	15.335866	127.0.0.1	127.0.0.1	TCP	44	63350 → 63348 [FIN, ACK] Seq=10 Ack=1 Win=2619648 Len=0
51	15.335891	127.0.0.1	127.0.0.1	TCP	44	63348 → 63350 [ACK] Seq=1 Ack=11 Win=2619648 Len=0
52	15.335911	127.0.0.1	127.0.0.1	TCP	44	63348 → 63350 [FIN, ACK] Seq=1 Ack=11 Win=2619648 Len=0
53	15.335928	127.0.0.1	127.0.0.1	TCP	44	63350 → 63348 [ACK] Seq=11 Ack=2 Win=2619648 Len=0
54	15.343037	127.0.0.1	127.0.0.1	TCP	44	63351 → 63349 [FIN, ACK] Seq=10 Ack=1 Win=2619648 Len=0
55	15.343071	127.0.0.1	127.0.0.1	TCP	44	63349 → 63351 [ACK] Seq=1 Ack=11 Win=2619648 Len=0
56	15.343105	127.0.0.1	127.0.0.1	TCP	44	63349 → 63351 [FIN, ACK] Seq=1 Ack=11 Win=2619648 Len=0
57	15.343131	127.0.0.1	127.0.0.1	TCP	44	63351 → 63349 [ACK] Seq=11 Ack=2 Win=2619648 Len=0
58	15.721454	192.168.56.1	192.168.56.255	NBNS	82	Name query NB DESKTOP-Q3CE8H7<1c>
59	16.478653	10.7.56.70	10.7.63.255	NBNS	82	Name query NB DESKTOP-Q3CE8H7<1c>
60	17.235364	10.7.56.70	10.7.63.255	NBNS	82	Name query NB DESKTOP-Q3CE8H7<1c>
61	17.991474	10.7.56.70	10.7.63.255	NBNS	82	Name query NB DESKTOP-Q3CE8H7<1c>

> Frame 60: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF\_{...}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 10.7.56.70, Dst: 10.7.63.255

> User Datagram Protocol, Src Port: 137, Dst Port: 137

> NetBIOS Name Service

0000 02 00 00 00 45 00 00 4e f7 c3 00 00 00 11 00 00 ....E--N .....

0010 0a 07 38 46 0a 07 3f ff 00 89 00 89 00 3a f0 58 --8F--? : .....X

0020 e6 39 01 10 00 01 00 00 00 00 20 45 45 45 45 9-..... EEE

0030 46 46 44 45 4c 46 45 45 50 46 41 43 4e 46 42 44 FFDELFEE PFACNFB

0040 44 45 44 45 46 44 49 45 49 44 48 42 4d 00 20 DEDEFDIE IDHBM--

0050 00 01 .....

d) **LLMNR**: The Link-Local Multicast Name Resolution (LLMNR) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link. Its RFC number is 4795.

Capturing from Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
154	59.391634	fe80::e881:7249:277...	ff02::1:3	LLMNR	75	Standard query 0x5b0c AAAA https
155	59.391799	10.7.56.70	224.0.0.252	LLMNR	55	Standard query 0x5b0c AAAA https
156	59.761090	fe80::105c:538f:733...	ff02::1:3	LLMNR	75	Standard query 0x8f36 AAAA https
157	59.761103	fe80::105c:538f:733...	ff02::1:3	LLMNR	75	Standard query 0xed71 A https
158	59.761232	192.168.56.1	224.0.0.252	LLMNR	55	Standard query 0x8f36 AAAA https
159	59.761239	192.168.56.1	224.0.0.252	LLMNR	55	Standard query 0xed71 A https
160	59.761290	fe80::e881:7249:277...	ff02::1:3	LLMNR	75	Standard query 0xed71 A https
161	59.761297	fe80::e881:7249:277...	ff02::1:3	LLMNR	75	Standard query 0x8f36 AAAA https
162	59.761364	10.7.56.70	224.0.0.252	LLMNR	55	Standard query 0xed71 A https
163	59.761402	10.7.56.70	224.0.0.252	LLMNR	55	Standard query 0x8f36 AAAA https
164	59.809187	fe80::105c:538f:733...	ff02::1:3	LLMNR	75	Standard query 0x4a50 A https
165	59.809351	fe80::105c:538f:733...	ff02::1:3	LLMNR	75	Standard query 0x5b0c AAAA https

> Frame 60: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF\_{...}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 10.7.56.70, Dst: 10.7.63.255

> User Datagram Protocol, Src Port: 137, Dst Port: 137

> NetBIOS Name Service

0000 02 00 00 00 45 00 00 4e f7 c3 00 00 00 11 00 00 ....E--N .....

0010 0a 07 38 46 0a 07 3f ff 00 89 00 89 00 3a f0 58 --8F--? : .....X

0020 e6 39 01 10 00 01 00 00 00 00 20 45 45 45 45 9-..... EEE

0030 46 46 44 45 4c 46 45 45 50 46 41 43 4e 46 42 44 FFDELFEE PFACNFB

0040 44 45 44 45 46 44 49 45 49 44 48 42 4d 00 20 DEDEFDIE IDHBM--

0050 00 01 .....



e) ICMP: The Internet Control Message Protocol (ICMP) is a network layer protocol used by network devices to diagnose network communication issues. ICMP is mainly used to determine whether or not data is reaching its intended destination in a timely manner. Its RFC number is 792.

Capturing from Adapter for loopback traffic capture

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
114	93.069202	127.0.0.1	127.0.0.1	TCP	44	63697 → 63696 [ACK] Seq=11 Ack=2 Win=2619648 Len=0
115	104.489889	10.7.56.70	10.7.56.70	ICMP	84	Destination unreachable (Host unreachable)
116	104.490091	10.7.56.70	10.7.56.70	ICMP	84	Destination unreachable (Host unreachable)
117	108.994065	10.7.56.70	10.7.56.70	ICMP	84	Destination unreachable (Host unreachable)
118	108.994101	10.7.56.70	10.7.56.70	ICMP	84	Destination unreachable (Host unreachable)
119	113.001643	10.7.56.70	10.7.56.70	ICMP	84	Destination unreachable (Host unreachable)
120	113.001668	10.7.56.70	10.7.56.70	ICMP	84	Destination unreachable (Host unreachable)
121	120.996212	10.7.56.70	10.7.56.70	ICMP	84	Destination unreachable (Host unreachable)
122	120.996308	10.7.56.70	10.7.56.70	ICMP	84	Destination unreachable (Host unreachable)
123	137.158297	192.168.56.1	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
124	137.158451	10.7.56.70	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1
125	137.164167	192.168.56.1	239.255.255.250	SSDP	207	M-SEARCH * HTTP/1.1

> Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface \Device\NPF\_{...}\_id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 10.7.56.70, Dst: 10.7.56.70

> Internet Control Message Protocol

0000 02 00 00 00 45 00 00 50 01 c8 00 00 80 01 00 00 ...E..P..:....

0010 0a 07 38 46 0a 07 38 46 03 01 95 14 00 00 00 00 ...8F..8F.....

0020 45 00 00 34 62 d5 40 00 80 06 00 00 0a 07 38 46 E..4b@.....8F

0030 0a 07 26 25 f8 b1 1e 00 0e bf 61 c9 00 00 00 00 ...8x.....a....

0040 00 02 fa f0 7a 6c 00 00 02 04 05 b4 01 03 03 08 ...z1.....

0050 01 01 04 02 .....

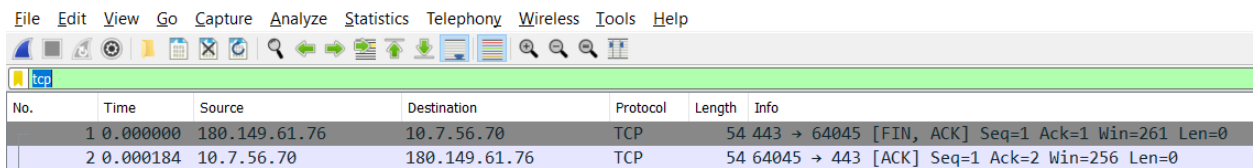
Adapter for loopback traffic capture: <live capture in progress>

Packets: 195 · Displayed: 195 (100.0%)

Profile: Default

00:20 16-09-2022

5) b) Identify any one connection and try to estimate the RTT of that connection.

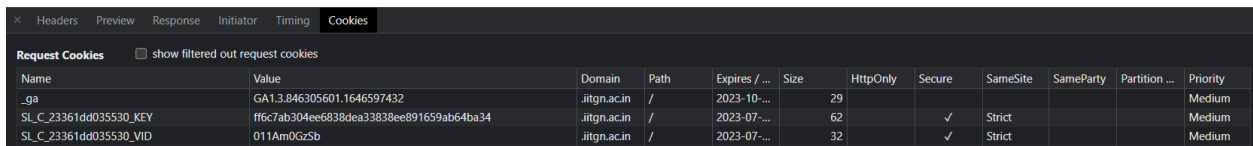


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	180.149.61.76	10.7.56.70	TCP	54	443 → 64045 [FIN, ACK] Seq=1 Ack=1 Win=261 Len=0
2	0.000184	10.7.56.70	180.149.61.76	TCP	54	64045 → 443 [ACK] Seq=1 Ack=2 Win=256 Len=0

To find RTT I filtered all the TCP connections and in the view menu, and in the Time Display Format, I selected the seconds since the previously displayed bracket. Therefore in the screenshot it is clear that the RTT is 0.000184 seconds.

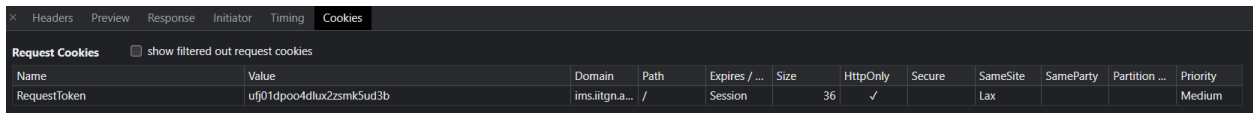
5) c) List the cookies and identify the characteristics of the cookies setup when you visit ims.iitgn.ac.in and also when you login to the student portal.

Ims in normal Google Chrome: Found 3 cookies out of which 2 are secure. None of the cookies are http only.



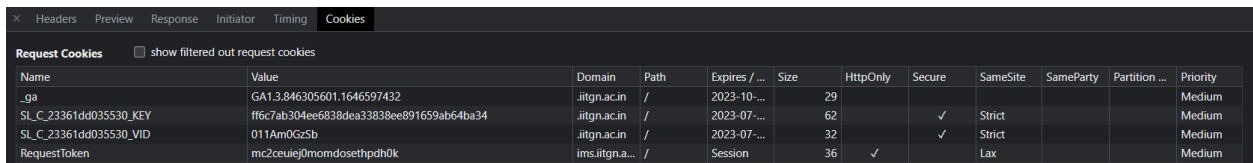
Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	SameParty	Partition ...	Priority
_ga	GA1.3.846305601.1646597432	.iitgn.ac.in	/	2023-10-...	29						Medium
SL_C_23361dd035530_KEY	ff6c7ab304ee6838dea33838ee891659ab64ba34	.iitgn.ac.in	/	2023-07-...	62		✓	Strict			Medium
SL_C_23361dd035530_VID	011Am0GzSb	.iitgn.ac.in	/	2023-07-...	32		✓	Strict			Medium

Ims through logging in Incognito tab: Found 1 cookie in the incognito tab which is not secure. The cookie is http only.



Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	SameParty	Partition ...	Priority
RequestToken	ufj01dpoo4dlux2zsmkSud3b	ims.iitgn.a...	/	Session	36	✓		Lax			Medium

Ims through logging in normal Google Chrome: Found 4 cookies in the normal browser after signing in out of which 2 are secure. 1 cookie is http only.



Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	SameParty	Partition ...	Priority
_ga	GA1.3.846305601.1646597432	.iitgn.ac.in	/	2023-10-...	29						Medium
SL_C_23361dd035530_KEY	ff6c7ab304ee6838dea33838ee891659ab64ba34	.iitgn.ac.in	/	2023-07-...	62		✓	Strict			Medium
SL_C_23361dd035530_VID	011Am0GzSb	.iitgn.ac.in	/	2023-07-...	32		✓	Strict			Medium
RequestToken	mc2ceuiog0mormdosethpdh0k	ims.iitgn.a...	/	Session	36	✓		Lax			Medium