

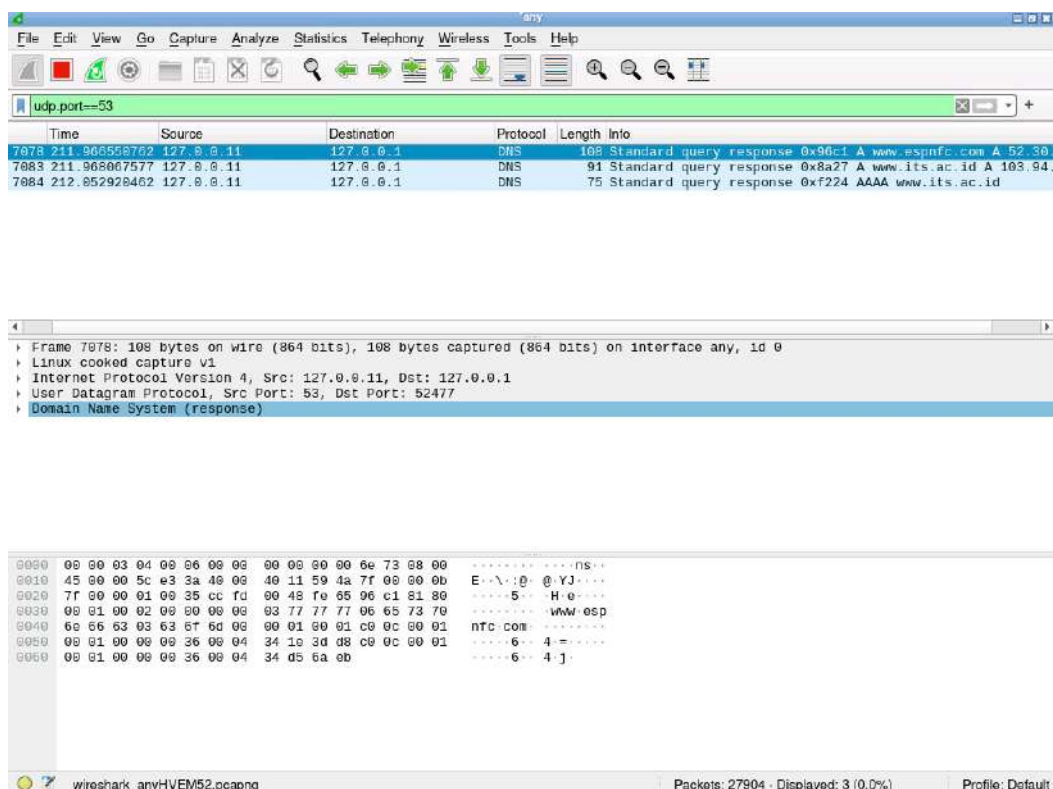
Tugas 1

1. Ketika membuka file socket_info.py ada beberapa hal yang perlu di perbaiki

- Remote_host = 'www.espnfc.cosm'
Pada lane tersebut terdapat typo dan perlu di perbaiki menjadi
Remote_host = 'www.espnfc.com'
- Untuk menjalankan semua fungsi pada main saya uncomment lane
get_my_info()
get_remote_info()

untuk melakukan analysis menggunakan wireshark ada beberapa hal perlu diketahui yaitu DNS di Docker container bersarang di stub (127.0.0.11) oleh karena itu untuk lihat query, capture di loopback/"any". Filer yang digunakan untuk case ini adlaah udp.port==53. Kenapa 53? Karena merupakan port standard DNS

hasil mesin1:



Hasil mesin2:

The image displays a Wireshark packet capture analysis. The top pane shows a list of captured packets. The bottom pane provides a detailed view of a selected packet, including its structure and raw data.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
2718	15.816367004	127.0.0.11	127.0.0.1	DNS	108	Standard query response 0x5d7c A www.epnfc.com A 5...
2725	15.818092039	127.0.0.11	127.0.0.1	DNS	91	Standard query response 0x5b71 A www.its.ac.id A 10...
2726	15.830552838	127.0.0.11	127.0.0.1	DNS	75	Standard query response 0x990e AAAA www.its.ac.id

Packet Details (Frame 2718):

- Interface id: 0 (any)
- Encapsulation type: Linux cooked-mode capture v1 (25)
- Arrival time: Apr 24, 2025 02:00:33.426485443 UTC
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1745460573.426485443 seconds
- [Time delta from previous captured frame: 0.013451585 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 15.816367094 seconds]
- Frame Number: 2718
- Frame Length: 108 bytes (864 bits)
- Capture Length: 108 bytes (864 bits)
- [Frame is marked: False]
- [Frame is ignored: False]

Raw Data (Hex and ASCII):

```
0000 00 00 03 04 00 06 00 00 00 00 00 00 22 34 08 00 .....4...
0010 45 00 00 5c f8 cc 48 00 48 11 43 b8 7f 00 00 0b E...@.@.C...
0020 7f 00 00 01 00 35 ed b0 00 48 7e 65 6d 7c 81 80 .....5...H.en]...
0030 00 01 00 02 00 00 00 00 03 77 77 77 06 65 73 70 .....www.esp
0040 6e 66 63 03 63 6f 6d 00 00 01 00 01 c0 0e 00 01 nfc.com.....
0050 00 01 00 00 00 36 00 04 34 1e 3d d8 c0 0c 00 01 .....6...4=.....
0060 00 01 00 00 00 36 00 04 34 d5 6a eb .....6...4.j...
```

Status Bar: wireshark_anyECU442.pcapng | Packets: 36002 · Displayed: 3 (0.0%) | Profile: Default

2. Karena pada mesin1 server.py di bind ke 0.0.0.0:10000 yang artinya listen di semua interface mesin1 saja. Ini membuat mesin2 sebagai client dengan hostname localhost, hanya akan mencoba connect ke 127.0.0.1:10000 di mesin2 tapi server tidak ada di sana yang mengakibatkan error

INFO:root:connecting to ('localhost', 10000)

INFO:root:ERROR: [Errno 111]

Connection refused INFO:root:closing

Untuk menangani hal ini, cek ip eth1 pada mesin1, kenapa eth1 karena keterangan di git eth1 menghubungkan antar mesin (isolated).

```
(base) jovyan@6de9b7022a73:~/work/progjar/progjar$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0@if10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 16:88:0e:90:8a:4a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.20.0.2/16 brd 172.20.255.255 scope global eth0
        valid_lft forever preferred_lft forever
3: eth1@if13: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 32:ff:39:4a:03:07 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.16.16.101/24 brd 172.16.16.255 scope global eth1
        valid_lft forever preferred_lft forever
```

Pada mesin2 client.py ubah server_address = ('localhost', 10000) menjadi server_address = ('172.16.16.101', 10000).

Analysis mesin1 (server)

tcp.port==10000

No.	Time	Source	Destination	Protocol	Length	Info
41205	1334.7965382	172.16.16.102	172.16.16.101	TCP	76	53352 → 10000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
41206	1334.7965392	172.16.16.101	172.16.16.102	TCP	76	10000 → 53352 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
41207	1334.7965589	172.16.16.102	172.16.16.101	TCP	68	53352 → 10000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=68
41208	1334.7966084	172.16.16.102	172.16.16.101	TCP	114	53352 → 10000 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=0
41209	1334.7966797	172.16.16.101	172.16.16.102	TCP	68	10000 → 53352 [ACK] Seq=1 Ack=47 Win=65152 Len=0 TSr=68
41210	1334.7973707	172.16.16.101	172.16.16.102	TCP	100	10000 → 53352 [PSH, ACK] Seq=1 Ack=47 Win=65152 Len=0
41211	1334.7973959	172.16.16.102	172.16.16.101	TCP	68	53352 → 10000 [ACK] Seq=47 Ack=33 Win=64256 Len=0 TSval=68
41212	1334.7974738	172.16.16.101	172.16.16.102	TCP	82	10000 → 53352 [PSH, ACK] Seq=33 Ack=47 Win=65152 Len=0
41213	1334.7974789	172.16.16.102	172.16.16.101	TCP	68	53352 → 10000 [ACK] Seq=47 Ack=47 Win=64256 Len=0 TSval=68
41215	1334.7978458	172.16.16.102	172.16.16.101	TCP	68	53352 → 10000 [FIN, ACK] Seq=47 Ack=47 Win=64256 Len=0 TSval=68
41216	1334.7979547	172.16.16.101	172.16.16.102	TCP	68	10000 → 53352 [FIN, ACK] Seq=47 Ack=48 Win=65152 Len=0 TSr=68
41217	1334.7979729	172.16.16.102	172.16.16.101	TCP	68	53352 → 10000 [ACK] Seq=48 Ack=48 Win=64256 Len=0 TSval=68

Frame 41210: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0

Interface id: 0 (any)

Encapsulation type: Linux cooked-mode capture v1 (25)

Arrival Time: Apr 24, 2025 02:37:16.106657834 UTC

[Time shift for this packet: 0.000000000 seconds]

0000 00 04 00 01 00 06 32 ff 30 4a 03 07 28 5d 08 002.9J.BV..

0010 45 00 00 54 83 55 40 00 40 06 3e 63 ac 10 10 65 E..T.Ug. @>c..e

0020 ac 10 10 66 27 10 d0 68 50 ae dc d0 93 a2 95 56 ...f...h.V.....V

0030 80 18 01 fd 79 32 00 00 01 01 08 0a 7c 74 e0 a6y2.....[t...

0040 61 84 a9 e1 49 4e 49 28 41 44 41 4c 41 48 20 44 a...INI ADALAH D

0050 41 54 41 28 59 41 4e 47 28 44 49 4b 49 52 49 4d ATA YANG DIKIRIM

0060 20 41 42 43 ABC

Frame (frame), 100 bytes

Packets: 84672 - Displayed: 12 (0.0%)

Profile: Default

Analisis mesin2 (client)

The image displays a Wireshark packet capture analysis of a client connection. The top pane shows a list of packets with a filter 'tcp.port==10000'. The middle pane shows details for packet 49972, including frame length and capture length. The bottom pane shows the raw packet data in hexadecimal and ASCII.

Time	Source	Destination	Protocol	Length	Info
946.1198.9979979...	127.0.0.1	127.0.0.1	TCP	76	69432 → 10000 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK...
947.1198.9988071...	127.0.0.1	127.0.0.1	TCP	86	18008 → 69432 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
727.1467.5482402...	127.0.0.1	127.0.0.1	TCP	76	34110 → 10000 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK...
728.1467.5482487...	127.0.0.1	127.0.0.1	TCP	86	18008 → 34110 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
969.1678.4958583...	172.16.16.102	172.16.16.101	TCP	76	53352 → 10000 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK...
970.1678.4958100...	172.16.16.101	172.16.16.102	TCP	76	18009 → 53352 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS...
971.1678.4951255...	172.16.16.102	172.16.16.101	TCP	68	53352 → 10000 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=16...
972.1678.4952342...	172.16.16.102	172.16.16.101	TCP	114	53352 → 10000 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=0 TS...
973.1678.4952405...	172.16.16.101	172.16.16.102	TCP	68	18009 → 53352 [ACK] Seq=1 Ack=47 Win=65152 Len=0 TSval=26...
976.1678.4954465...	172.16.16.101	172.16.16.102	TCP	160	18009 → 53352 [PSH, ACK] Seq=1 Ack=47 Win=65152 Len=32 TS...
977.1678.4958528...	172.16.16.102	172.16.16.101	TCP	68	53352 → 10000 [ACK] Seq=47 Ack=33 Win=64256 Len=0 TSval=1...
978.1678.4968446...	172.16.16.101	172.16.16.102	TCP	82	18009 → 53352 [PSH, ACK] Seq=33 Ack=47 Win=65152 Len=14 T...
979.1678.4968462...	172.16.16.102	172.16.16.101	TCP	68	53352 → 10000 [ACK] Seq=47 Ack=47 Win=64256 Len=0 TSval=1...
984.1678.4964965...	172.16.16.102	172.16.16.101	TCP	68	53352 → 10000 [FIN, ACK] Seq=47 Ack=47 Win=64256 Len=0 TS...
985.1678.4965304...	172.16.16.101	172.16.16.102	TCP	68	18008 → 53352 [FIN, ACK] Seq=47 Ack=48 Win=65152 Len=0 TS...
986.1678.4965359...	172.16.16.102	172.16.16.101	TCP	68	53352 → 10000 [ACK] Seq=48 Ack=48 Win=64256 Len=0 TSval=1...

Details for packet 49972:

- [Time since reference or first frame: 1678.495234240 seconds]
- Frame Number: 49972
- Frame Length: 114 bytes (912 bits)
- Capture Length: 114 bytes (912 bits)
- [Frame is marked: False]
- [Frame is ignored: False]

Raw packet data (hex and ASCII):

```

0000  08 04 50 01 08 08 9e 4b 1e ff 66 b2 6e 2f 08 00  ....K..f n/..
0010  45 09 50 52 82 10 40 00 40 06 3f 92 ac 10 10 66  E..b. @.?. .f
0020  ac 18 10 55 d6 69 27 10 93 a2 95 28 56 ae dc d0  ...e h' ... (V...
0030  08 18 01 f6 79 40 00 00 01 01 00 0a 61 84 a9 e1  ...y@ ... 2...
0040  7c 74 e0 a5 49 4e 49 28 41 44 41 4c 41 48 28 44  |t..INI ADALAH D
0050  41 54 41 28 59 41 4e 47 28 44 49 4b 49 52 49 4d  ATA YANG DIKIRIM
0060  28 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f  ABCDEFG HIJKLMNO
0070  58 51 PQ
  
```

Wireshark any ECU442.pcapng

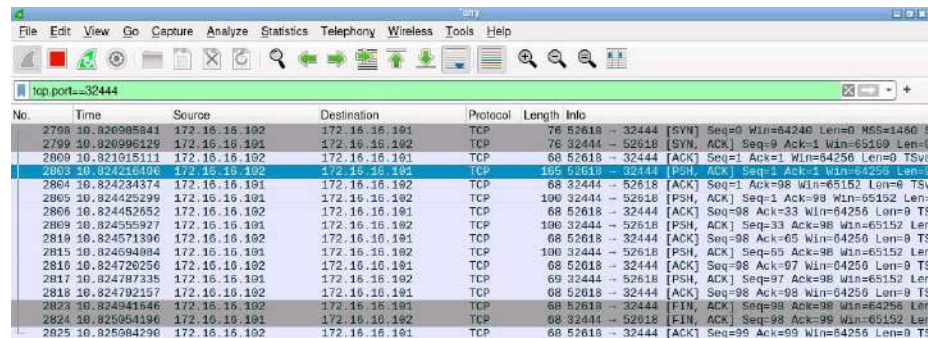
Packets: 87168 · Displayed: 16 (0.0%)

Profile: Default

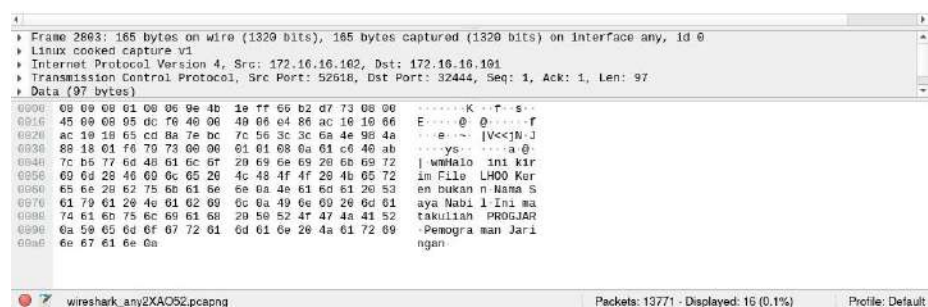
Pada client ada RST karena client mencoba menghubungkan keserver 'localhost', 10000 (saat belum di perbaiki) ini menjelaskan Connection refused di log client. Saat berhasil menghubungkan ke server dapat diperhatikan ada 3-way handshake berjalan sempurna (SYN→SYN+ACK→ACK) dan ada PSH, ACK yang membawa payload teks. Setelah data selesai, koneksi ditutup dengan FIN, ACK berurutan.

3. Pada server saya hanya perlu mengubah port connection ke 32444 sesuai soal. Untuk mesin2, saya perlu membuat file, contohnya disini adalah file.txt denga isi string “Halo ini kirim File LHOO Keren bukannya”. Sedangkan pada client saya juga perlu mengubah port ke 32444 untuk menghubungkan kepada client. Lalu masukkan isi dari file.txt kepada data dan kirimkan menggunakan sock.sendall(). Pada python sebenarnya sekarang dapat menggunakan sock.sendfile(), tetapi menurut saya, sekarang menggunakan metode sock.sendall() saja sudah cukup

Analisis mesin1 (server)



No.	Time	Source	Destination	Protocol	Length	Info
2798	10.820985841	172.16.16.102	172.16.16.101	TCP	76	52618 → 32444 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2799	10.820986129	172.16.16.101	172.16.16.102	TCP	76	32444 → 52618 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
2800	10.821915111	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv=
2803	10.824216406	172.16.16.102	172.16.16.101	TCP	105	52618 → 32444 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=0
2804	10.824234374	172.16.16.101	172.16.16.102	TCP	68	32444 → 52618 [ACK] Seq=1 Ack=98 Win=65152 Len=0 TSv=
2805	10.824425299	172.16.16.101	172.16.16.102	TCP	100	32444 → 52618 [PSH, ACK] Seq=1 Ack=98 Win=65152 Len=0
2806	10.824452652	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [ACK] Seq=98 Ack=33 Win=64256 Len=0 TSv=
2809	10.824555927	172.16.16.101	172.16.16.102	TCP	100	32444 → 52618 [PSH, ACK] Seq=33 Ack=98 Win=65152 Len=0
2810	10.824571396	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [ACK] Seq=98 Ack=65 Win=64256 Len=0 TSv=
2815	10.824694984	172.16.16.101	172.16.16.102	TCP	100	32444 → 52618 [PSH, ACK] Seq=65 Ack=98 Win=65152 Len=0
2816	10.824720256	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [ACK] Seq=98 Ack=97 Win=64256 Len=0 TSv=
2817	10.824787335	172.16.16.101	172.16.16.102	TCP	69	32444 → 52618 [PSH, ACK] Seq=97 Ack=98 Win=65152 Len=0
2818	10.824792157	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [ACK] Seq=98 Ack=98 Win=64256 Len=0 TSv=
2822	10.824841646	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [FIN, ACK] Seq=98 Ack=98 Win=64256 Len=0
2824	10.825054196	172.16.16.101	172.16.16.102	TCP	68	32444 → 52618 [FIN, ACK] Seq=98 Ack=99 Win=65152 Len=0
2825	10.825084296	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [ACK] Seq=99 Ack=99 Win=64256 Len=0 TSv=



Frame 2803: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface any, id 0

Linux cooked capture v1

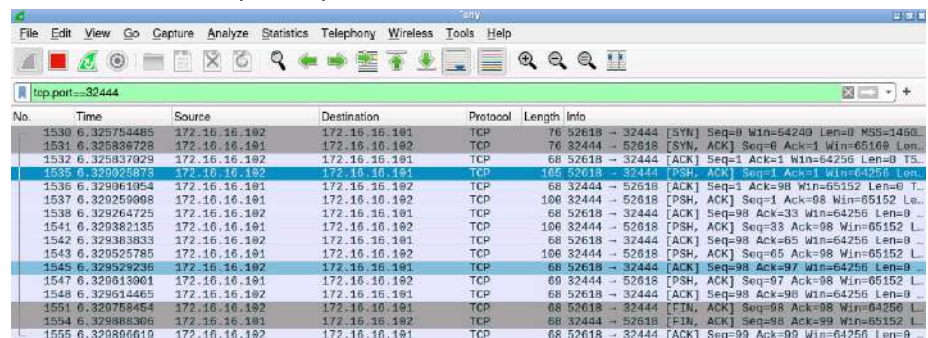
Internet Protocol Version 4, Src: 172.16.16.102, Dst: 172.16.16.101

Transmission Control Protocol, Src Port: 52618, Dst Port: 32444, Seq: 1, Ack: 1, Len: 97

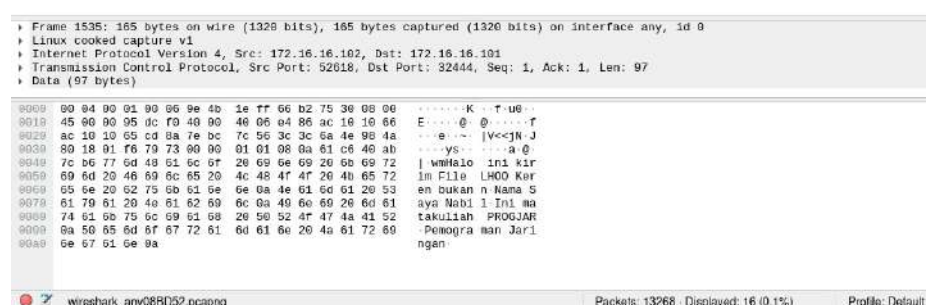
Data (97 bytes)

Offset	Hex	ASCII
0000	00 00 00 01 00 00 9e 4b 1e ff 66 b2 d7 73 08 00K...f...
0016	45 00 00 95 dc f0 40 00 40 06 e4 86 ac 18 10 66	E...@...f
0020	ac 10 18 65 cd 8a 7e bc 7c 56 3c 3c 6a 4e 98 4a	...[V<>N]J
0038	88 18 01 f6 70 73 00 00 01 01 08 0a 61 c6 40 ab	...ys...a@
0040	7c b5 77 6d 40 61 6c 67 20 69 6e 69 20 60 69 72	I wmallo ini kir
0050	60 6d 20 46 60 6c 65 20 4c 48 4f 4f 20 4b 65 72	im File LHOO Ker
0060	65 6e 20 62 75 6b 61 6e 6e 0a 4e 61 6d 61 20 53	en bukan n Nana S
0070	61 79 61 20 40 61 62 69 6c 0a 49 6e 60 20 6d 61	aya Nabi l Ini ma
0080	74 61 6b 75 6c 69 61 68 20 50 52 4f 47 4a 41 52	takulliah PROGJAR
0090	0a 50 65 6d 6f 67 72 61 6d 61 6e 20 4a 61 72 69	-Pemogra man Jarl
00a0	6e 67 61 6e 0a	ngan

Analisis mesin2 (client)



No.	Time	Source	Destination	Protocol	Length	Info
1530	6.325754485	172.16.16.102	172.16.16.101	TCP	76	52618 → 32444 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
1531	6.325836728	172.16.16.101	172.16.16.102	TCP	76	32444 → 52618 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
1532	6.325837029	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv=
1535	6.329025873	172.16.16.102	172.16.16.101	TCP	105	52618 → 32444 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=0
1536	6.329061054	172.16.16.101	172.16.16.102	TCP	68	32444 → 52618 [ACK] Seq=1 Ack=98 Win=65152 Len=0 TSv=
1537	6.329250968	172.16.16.101	172.16.16.102	TCP	100	32444 → 52618 [PSH, ACK] Seq=1 Ack=98 Win=65152 Len=0
1538	6.329264725	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [ACK] Seq=98 Ack=33 Win=64256 Len=0 TSv=
1541	6.329382135	172.16.16.101	172.16.16.102	TCP	100	32444 → 52618 [PSH, ACK] Seq=33 Ack=98 Win=65152 Len=0
1542	6.329383833	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [ACK] Seq=98 Ack=65 Win=64256 Len=0 TSv=
1543	6.329525785	172.16.16.101	172.16.16.102	TCP	100	32444 → 52618 [PSH, ACK] Seq=65 Ack=98 Win=65152 Len=0
1545	6.329529238	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [ACK] Seq=98 Ack=97 Win=64256 Len=0 TSv=
1547	6.329613061	172.16.16.101	172.16.16.102	TCP	69	32444 → 52618 [PSH, ACK] Seq=97 Ack=98 Win=65152 Len=0
1548	6.329614465	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [ACK] Seq=98 Ack=98 Win=64256 Len=0 TSv=
1551	6.320758454	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [FIN, ACK] Seq=98 Ack=98 Win=64256 Len=0
1554	6.329883308	172.16.16.101	172.16.16.102	TCP	68	32444 → 52618 [FIN, ACK] Seq=98 Ack=99 Win=65152 Len=0
1555	6.329886619	172.16.16.102	172.16.16.101	TCP	68	52618 → 32444 [ACK] Seq=99 Ack=99 Win=64256 Len=0 TSv=



Frame 1535: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface any, id 0

Linux cooked capture v1

Internet Protocol Version 4, Src: 172.16.16.102, Dst: 172.16.16.101

Transmission Control Protocol, Src Port: 52618, Dst Port: 32444, Seq: 1, Ack: 1, Len: 97

Data (97 bytes)

Offset	Hex	ASCII
0000	00 04 00 01 00 00 9e 4b 1e ff 66 b2 75 30 08 00K...f...u...
0016	45 00 00 95 dc f0 40 00 40 06 e4 86 ac 18 10 66	E...@...f
0020	ac 10 18 65 cd 8a 7e bc 7c 56 3c 3c 6a 4e 98 4a	...[V<>N]J
0038	88 18 91 f6 70 73 00 00 01 01 08 0a 61 c6 40 ab	...ys...a@
0040	7c b5 77 6d 40 61 6c 67 20 69 6e 69 20 60 69 72	I wmallo ini kir
0050	60 6d 20 46 60 6c 65 20 4c 48 4f 4f 20 4b 65 72	im File LHOO Ker
0060	65 6e 20 62 75 6b 61 6e 6e 0a 4e 61 6d 61 20 53	en bukan n Nana S
0070	61 79 61 20 40 61 62 69 6c 0a 49 6e 60 20 6d 61	aya Nabi l Ini ma
0080	74 61 6b 75 6c 69 61 68 20 50 52 4f 47 4a 41 52	takulliah PROGJAR
0090	0a 50 65 6d 6f 67 72 61 6d 61 6e 20 4a 61 72 69	-Pemogra man Jarl
00a0	6e 67 61 6e 0a	ngan

Dari hasil analisis kurang lebih hampir sama seperti pada no2, tetapi yang membedakannya adalah palyload yang besar dapat dilihat pada wireshark data file tersebar di banyak frame, jika mengirimkan file yang cukup panjang isinya.

4. Disini saya mengubah port menjadi 32434 pada sever dan client. Pada client mesin2 saya tetap mengirimkan file sedangkan pada client mesin3 saya akan mengirimkan message.

Analysis mesin1 (server)

```
jovyan@6de9b7022a73: ~/w X server.py
(base) jovyan@6de9b7022a73:~/work/progjar/progjar1$ python3 server.py
INFO:root:starting up on ('0.0.0.0', 32434)
INFO:root:waiting for a connection
INFO:root:connection from ('172.16.16.102', 37534)
INFO:root:received b'Halo ini kirim File LHOO Keren b'
INFO:root:sending back data
INFO:root:received b'ukann\nNama Saya Nabil\nIni matak'
INFO:root:sending back data
INFO:root:received b'liah PROGJAR\nPemograman Jaringan'
INFO:root:sending back data
INFO:root:received b'\n'
INFO:root:sending back data
INFO:root:received b''
INFO:root:waiting for a connection
INFO:root:connection from ('172.16.16.103', 41980)
INFO:root:received b'INI ADALAH DATA YANG DIKIRIM ABC'
INFO:root:sending back data
INFO:root:received b'DFGHIJKLMNOPQ'
INFO:root:sending back data
INFO:root:received b''
INFO:root:waiting for a connection
```

The Wireshark capture shows the following details:

- Filter:** tcp.port==32434
- Packet List:** A series of TCP connections and data exchanges between 172.16.16.102 and 172.16.16.103 on port 32434. The list includes SYN, ACK, PSH, and FIN packets, as well as data packets.
- Packet Details:** The selected packet (Frame 21901) shows the following details:
 - Frame 21901: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface any, id 0
 - Linux cooked capture v1
 - Internet Protocol Version 4, Src: 172.16.16.101, Dst: 172.16.16.103
 - Transmission Control Protocol, Src Port: 32434, Dst Port: 41980, Seq: 1, Ack: 47, Len: 32
 - Data (32 bytes): 00 04 00 01 00 06 32 ff 39 4a 03 07 07 05 08 00 ... 20 41 42 20
- Packet Bytes:** The packet bytes are displayed in hexadecimal and ASCII format, showing the data being transmitted.

Analysis mesin2 (client-1)

The Wireshark interface shows a capture on interface 'any' with filter 'tcp.port==32434'. The packet list displays a series of TCP segments from 172.16.16.102 to 172.16.16.101. Packet 6013 is selected, showing a PSH, ACK segment. The packet details pane shows the raw data of this segment, which is a Telnet session. The data pane shows the raw data of the selected packet, which is a Telnet session. The status bar at the bottom indicates 8763 packets displayed, with 16 (0.2%) shown.

No.	Time	Source	Destination	Protocol	Length	Info
6008	16.624689124	172.16.16.102	172.16.16.101	TCP	76	53910 → 32434 [SYN] Seq=0 Win=64240 Len=0 MSS=1460...
6009	16.624931062	172.16.16.101	172.16.16.102	TCP	76	32434 → 53910 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0...
6010	16.624938133	172.16.16.102	172.16.16.101	TCP	68	53910 → 32434 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS...
6013	16.627076892	172.16.16.102	172.16.16.101	TCP	165	53910 → 32434 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=97...

Frame 6013: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits) on interface any, id 9
Linux cooked capture v1
Internet Protocol Version 4, Src: 172.16.16.102, Dst: 172.16.16.101
Transmission Control Protocol, Src Port: 53910, Dst Port: 32434, Seq: 1, Ack: 1, Len: 97
Data (97 bytes)

```
0000 00 04 00 01 00 06 0e 4b 1e ff 66 b2 31 37 08 60 .....K...f.17..
0010 45 00 00 95 96 ba 40 00 40 06 2a bd ac 10 10 66 E...@...f
0020 ac 10 10 05 d2 96 7e b2 84 71 c0 f2 35 f9 1b 42 ...e...q...5..8
0030 80 18 01 f6 79 73 09 00 01 01 08 0a 61 05 71 bb .....ys...a.q.
0040 7c c5 a8 7d 43 61 6c 6f 20 69 6e 69 20 6b 69 72 |..}Halo ini kir
0050 09 0d 20 40 09 0c 05 20 4c 48 4f 4f 20 4b 05 72 im File LH00 Ker
0060 65 6e 20 62 75 6b 61 6e 6e 0a 4e 61 6d 61 20 53 en bukan n>Nama S
0070 61 70 61 20 4e 61 62 69 6c 0a 49 6e 69 20 6d 61 aya Nabi l.Ini ma
0080 74 61 6b 75 6c 69 61 68 20 50 52 4f 47 4a 41 52 takuliah PROGJAR
0090 0a 50 65 6d 6f 67 72 61 6d 61 6e 20 4a 61 72 69 .Pemograman Jarl
00a0 6e 67 61 6e 0a ngan.
```

Analysis mesin3 (client-2)

The Wireshark interface shows a capture on interface 'any' with filter 'tcp.port==32434'. The packet list displays a series of TCP segments from 172.16.16.103 to 172.16.16.101. Packet 9676 is selected, showing a PSH, ACK segment. The packet details pane shows the raw data of this segment, which is a Telnet session. The data pane shows the raw data of the selected packet, which is a Telnet session. The status bar at the bottom indicates 24580 packets displayed, with 13 (0.1%) shown.

No.	Time	Source	Destination	Protocol	Length	Info
9540	102.325996284	172.16.16.102	172.16.16.101	TCP	76	37534 → 32434 [SYN] Seq=0 Win=64240 Len=0 MSS=1460...
9673	105.786804600	172.16.16.103	172.16.16.101	TCP	76	41980 → 32434 [SYN] Seq=0 Win=64240 Len=0 MSS=1460...
9674	105.786856674	172.16.16.101	172.16.16.103	TCP	76	32434 → 41980 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0...
9675	105.786867223	172.16.16.103	172.16.16.101	TCP	68	41980 → 32434 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TS...
9676	105.786954710	172.16.16.103	172.16.16.101	TCP	114	41980 → 32434 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=48...

Frame 9676: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface any, id 9
Linux cooked capture v1
Internet Protocol Version 4, Src: 172.16.16.103, Dst: 172.16.16.101
Transmission Control Protocol, Src Port: 41980, Dst Port: 32434, Seq: 1, Ack: 1, Len: 48
Data (48 bytes)

```
0000 00 04 00 01 00 06 ca ce c6 c5 de f0 8c f7 08 00 .....b.e@...D...g
0010 45 00 00 62 b1 65 40 00 40 06 10 44 ac 10 10 67 E...@...f...T...
0020 ac 10 10 05 a3 7c 7e b2 cb 66 1a a8 65 63 05 00 ...e...t...
0030 80 18 01 f6 79 41 00 00 01 01 08 0a 76 c2 0a 7b .....yA...v...{
0040 cc db c0 02 49 4e 49 20 41 44 41 4c 41 48 20 44 ---INI ADALAH D
0050 41 54 41 20 59 41 4e 47 20 44 49 4b 49 52 49 4d ATA YANG DIKIRIM
0060 26 41 42 43 44 45 46 47 48 49 4a 4b 4c 4d 4e 4f ABCDEFGHIJKLMNOP
0070 5e 51 PQ
```


FIN, ACK menandakan pesan dari mesin-2 sudah selesai mengirimkan data dan ingin tutup koneksi dengan server. Client-2 dapat melakukan 3-way-handshake kapan saja tanpa perlu menunggu koneksi dari client-1 selesai. Karena server TCP bisa melayani banyak koneksi secara parallel.

172.16.16.101 → Merupakan ip dari server

172.16.16.102 → Merupakan ip dari client-1 (mesin2)

172.16.16.103 → Merupakan ip dari client-2 (mesin3)