

E13	5025211239	Najma Ulya Agustina	E
	5025201015	NADYA PERMATA SARI	E

1. 258040667 - 1044861039 - 1044861039 - 258040696

Wireshark · Packet 147 · soal1.pcapng

```

> Frame 147: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_fa:e2:fc (00:0c:29:fa:e2:fc), Dst: VMware_f5:e6:a9 (00:50:56:f5:e6:a9)
> Internet Protocol Version 4, Src: 192.168.254.129, Dst: 10.21.78.111
~ Transmission Control Protocol, Src Port: 58928, Dst Port: 21, Seq: 47, Ack: 593, Len: 29
  Source Port: 58928
  Destination Port: 21
  [Stream index: 4]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 29]
  Sequence Number: 47 (relative sequence number)
  Sequence Number (raw): 258040667
  [Next Sequence Number: 76 (relative sequence number)]
  Acknowledgment Number: 593 (relative ack number)
  Acknowledgment number (raw): 1044861039
  0101 .... = Header Length: 20 bytes (5)

```

Wireshark · Packet 149 · soal1.pcapng

```

> Frame 149: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface eth0, id 0
> Ethernet II, Src: VMware_f5:e6:a9 (00:50:56:f5:e6:a9), Dst: VMware_fa:e2:fc (00:0c:29:fa:e2:fc)
> Internet Protocol Version 4, Src: 10.21.78.111, Dst: 192.168.254.129
~ Transmission Control Protocol, Src Port: 21, Dst Port: 58928, Seq: 593, Ack: 76, Len: 68
  Source Port: 21
  Destination Port: 58928
  [Stream index: 4]
  [Conversation completeness: Complete, WITH_DATA (31)]
  [TCP Segment Len: 68]
  Sequence Number: 593 (relative sequence number)
  Sequence Number (raw): 1044861039
  [Next Sequence Number: 661 (relative sequence number)]
  Acknowledgment Number: 76 (relative ack number)
  Acknowledgment number (raw): 258040696
  0101 .... = Header Length: 20 bytes (5)
  Flags: 0x018 (PSH ACK)

```

## 2. unicorn

Challenge

72 Solved

✕


# SOAL 2

## 432

Author: Elshe

Sebutkan web server yang digunakan pada portal praktikum Jaringan Komputer!

```
nc 10.21.78.111 13579
```

 soal2.pcapng

Flag

Submit

soal2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http

No.	Time	Source	Destination	Protocol	Length	Info
1825	17.375703595	10.21.78.111	192.168.254.129	HTTP	805	HTTP/1.1 200 OK
1856	17.582316901	192.168.254.129	10.21.78.111	HTTP	464	GET /events HTTP/1.1
1862	17.641799383	192.168.254.129	10.21.78.111	HTTP	444	GET /themes/core/static/sounds/notification.webm
1864	17.643289354	192.168.254.129	10.21.78.111	HTTP	556	HEAD /api/v1/notifications?since_id=0 HTTP/1.1
1875	17.694993492	10.21.78.111	192.168.254.129	HTTP	894	HTTP/1.1 403 FORBIDDEN (text/html)
1901	17.780407646	10.21.78.111	192.168.254.129	HTTP	228	HTTP/1.1 200 OK
1905	17.863282769	10.21.78.111	192.168.254.129	HTTP	1252	HTTP/1.1 200 OK (video/webm)
1914	17.964798385	192.168.254.129	10.21.78.111	HTTP	473	GET /themes/core-beta/static/img/favicon.ico?d=36
1916	18.031274311	10.21.78.111	192.168.254.129	HTTP	1522	HTTP/1.1 200 OK (image/vnd.microsoft.icon)
496	5.127416466	192.168.254.129	192.124.249.22	OCSP	467	Request

> Transmission Control Protocol, Src Port: 8000, Dst Port: 45216

▼ Hypertext Transfer Protocol

> HTTP/1.1 200 OK\r\n

Server: unicorn\r\n

Date: Thu, 14 Sep 2023 12:53:02 GMT\r\n

Connection: keep-alive\r\n

Content-Type: text/html; charset=utf-8\r\n

Result-Count: 0\r\n

> Content-Length: 0\r\n

\r\n

[HTTP response 2/2]

0020 fe 81 1f 40 b0 9a 6d f5 37 54 14 ce 9c fc 50 18 ...@..m

0030 fa f0 e8 7a 00 00 48 54 54 50 2f 31 2e 31 20 32 ...z..H

0040 30 30 20 4f 4b 0d 0a 53 65 72 76 65 72 3a 20 67 00 OK..

0050 75 6e 69 63 6f 72 6e 0d 0a 44 61 74 65 3a 20 54 unicorn

0060 68 75 2c 20 31 34 20 53 65 70 20 32 30 32 33 20 hu, 14

0070 31 32 3a 35 33 3a 30 32 20 47 4d 54 0d 0a 43 6f 12:53:0

0080 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 nnectic

0090 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 live..C

00a0 70 65 3a 20 74 65 78 74 2f 68 74 6d 6c 3b 20 63 pe: tex

00b0 68 61 72 73 65 74 3d 75 74 66 2d 38 0d 0a 52 65 harset=

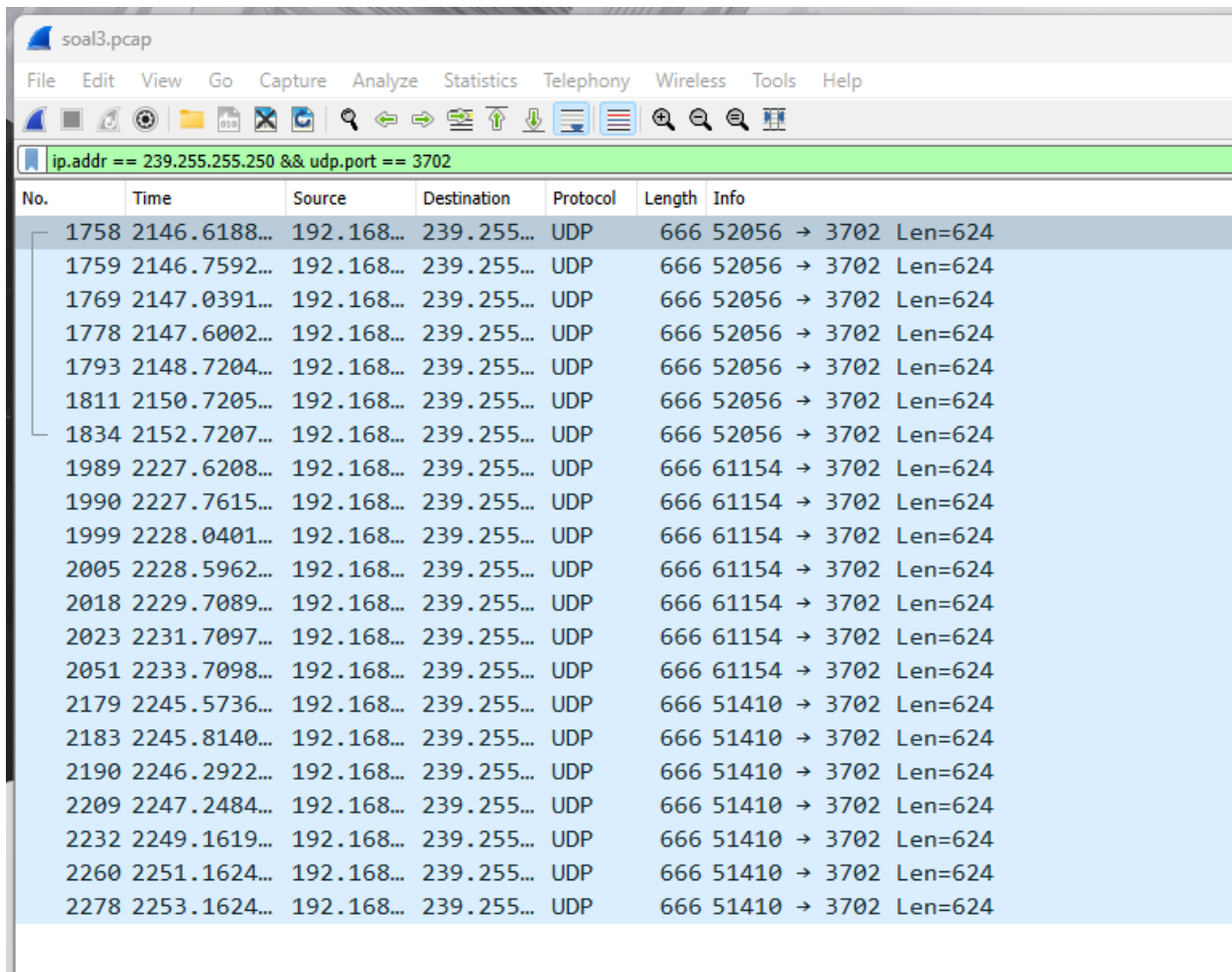
00c0 73 75 6c 74 2d 43 6f 75 6e 74 3a 20 30 0d 0a 43 sult-Co

00d0 6f 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 30 ontent-

00e0 0d 0a 0d 0a ....

```
najmaulya@LAPTOP-6LM7NBGE:~$ nc 10.21.78.111 13579
Sebutkan web server yang digunakan pada portal praktikum Jaringan Komputer!
Your answer: unicorn
Correct answer!
Here is your flag: Jarkom2023{9unic0rn_1s_3cEt81pVg54Sq7N_c00l}
```

### 3. 21 - UDP

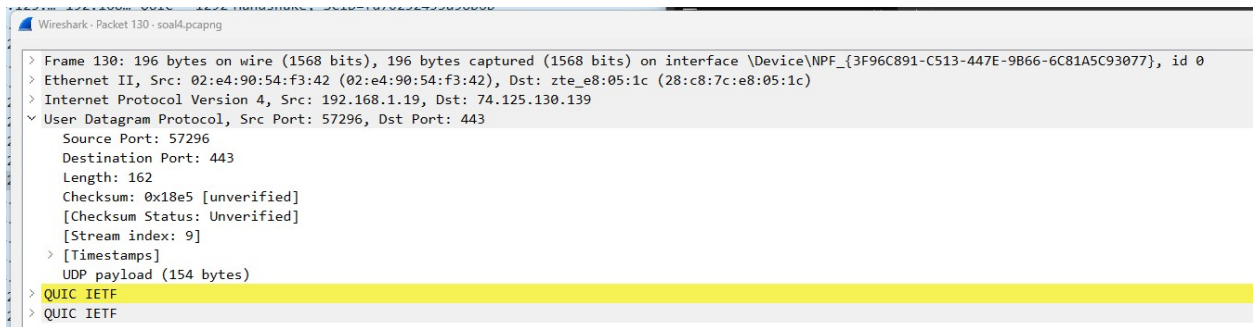


The image shows a Wireshark packet capture of a PCAP file named 'soal3.pcap'. The filter bar at the top shows the filter 'ip.addr == 239.255.255.250 && udp.port == 3702'. The packet list table below shows 20 UDP packets, all with a length of 666 bytes and a destination port of 3702. The 'Info' column for each packet shows '52056 → 3702 Len=624', indicating the source port is 52056 and the payload length is 624 bytes.

No.	Time	Source	Destination	Protocol	Length	Info
1758	2146.6188...	192.168...	239.255...	UDP	666	52056 → 3702 Len=624
1759	2146.7592...	192.168...	239.255...	UDP	666	52056 → 3702 Len=624
1769	2147.0391...	192.168...	239.255...	UDP	666	52056 → 3702 Len=624
1778	2147.6002...	192.168...	239.255...	UDP	666	52056 → 3702 Len=624
1793	2148.7204...	192.168...	239.255...	UDP	666	52056 → 3702 Len=624
1811	2150.7205...	192.168...	239.255...	UDP	666	52056 → 3702 Len=624
1834	2152.7207...	192.168...	239.255...	UDP	666	52056 → 3702 Len=624
1989	2227.6208...	192.168...	239.255...	UDP	666	61154 → 3702 Len=624
1990	2227.7615...	192.168...	239.255...	UDP	666	61154 → 3702 Len=624
1999	2228.0401...	192.168...	239.255...	UDP	666	61154 → 3702 Len=624
2005	2228.5962...	192.168...	239.255...	UDP	666	61154 → 3702 Len=624
2018	2229.7089...	192.168...	239.255...	UDP	666	61154 → 3702 Len=624
2023	2231.7097...	192.168...	239.255...	UDP	666	61154 → 3702 Len=624
2051	2233.7098...	192.168...	239.255...	UDP	666	61154 → 3702 Len=624
2179	2245.5736...	192.168...	239.255...	UDP	666	51410 → 3702 Len=624
2183	2245.8140...	192.168...	239.255...	UDP	666	51410 → 3702 Len=624
2190	2246.2922...	192.168...	239.255...	UDP	666	51410 → 3702 Len=624
2209	2247.2484...	192.168...	239.255...	UDP	666	51410 → 3702 Len=624
2232	2249.1619...	192.168...	239.255...	UDP	666	51410 → 3702 Len=624
2260	2251.1624...	192.168...	239.255...	UDP	666	51410 → 3702 Len=624
2278	2253.1624...	192.168...	239.255...	UDP	666	51410 → 3702 Len=624

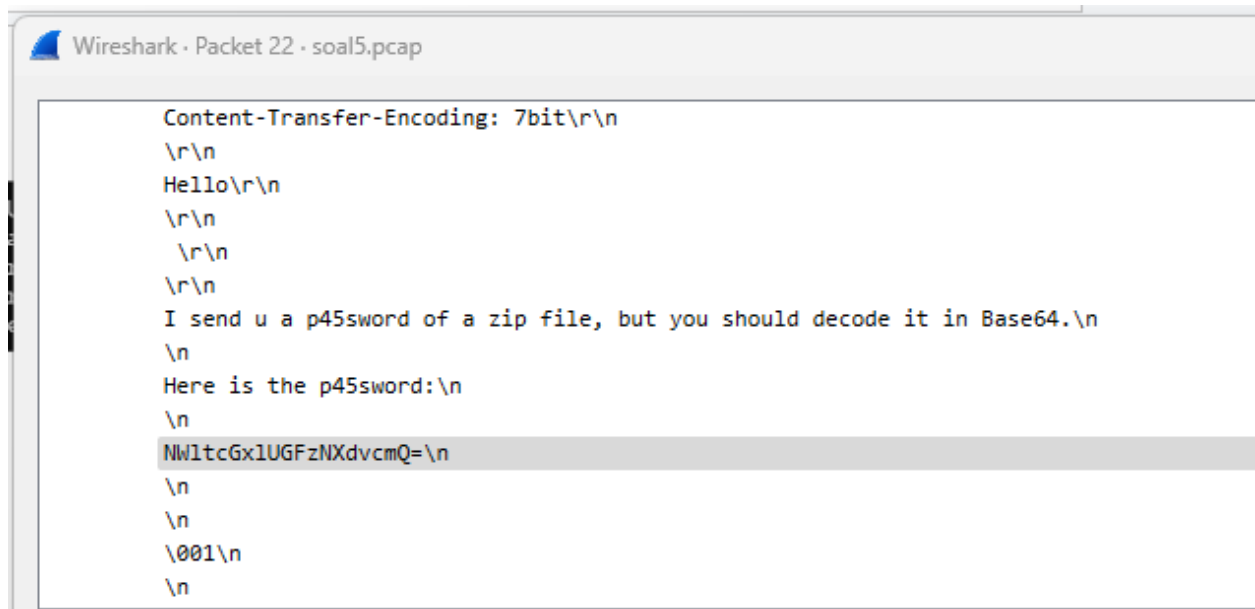
```
C:\Users\Nadya Permata>ncat 10.21.78.111 13591
Berapa nilai checksum yang didapat dari header pada paket nomor 130?
Your answer: 0x18e5
Correct answer!
Here is your flag: Jarkom2023{ch3cksum_is_u5eful_0xcv57}
```

#### 4. 0x18e5



```
C:\Users\Nadya Permata>ncat 10.21.78.111 13591
Berapa nilai checksum yang didapat dari header pada paket nomor 130?
Your answer: 0x18e5
Correct answer!
Here is your flag: Jarkom2023{ch3cksum_is_u5eful_0xcv57}
```

5. 60 - 25 - 74.53.140.153



## Decode from Base64 format

Simply enter your data then push the decode button.

NWItcGxIUGFzNXdvcmQ

**i** For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

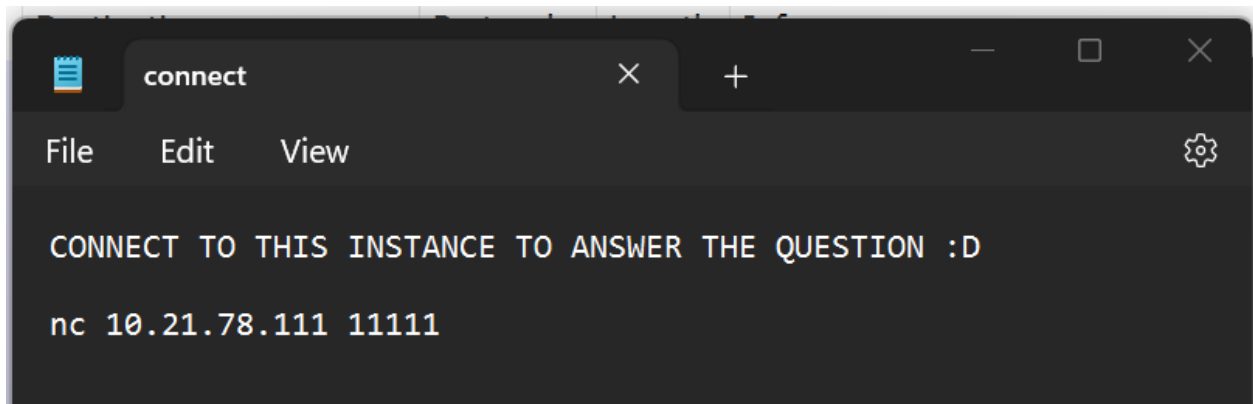
UTF-8 Source character set.

☐ Decode each line separately (useful for when you have multiple entries).

 Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

**< DECODE >** Decodes your data into the area below.

5implePas5word



Wireshark packet capture of an SMTP session. The packet list shows 41 packets. The selected packet (No. 25) is an SMTP DATA fragment (1460 bytes) from 10.10.1.4 to 74.53.140.153. The packet details pane shows the SMTP protocol structure, including the RCPT TO: <raj\_deol2002in@yahoo.co.in> and the DATA fragment.

No.	Time	Source	Destination	Protocol	Length	Info
9	1.074123	74.53.140.153	10.10.1.4	SMTP	191	S: 250-xc90.websitewelcome.com Hello GP [122.162.143.157]   SI
10	1.076669	10.10.1.4	74.53.140.153	SMTP	66	C: AUTH LOGIN
11	1.419021	74.53.140.153	10.10.1.4	SMTP	72	S: 334 VXNlcm5hbWU6
12	1.419595	10.10.1.4	74.53.140.153	SMTP	84	C: User: Z3VycGFydGFWQHBhdHJpb3RzLm1u
13	1.761484	74.53.140.153	10.10.1.4	SMTP	72	S: 334 UGFzc3dvcmQ6
14	1.762058	10.10.1.4	74.53.140.153	SMTP	72	C: Pass: cHVuamFiQDEyMw==
15	2.121738	74.53.140.153	10.10.1.4	SMTP	84	S: 235 Authentication succeeded
16	2.122354	10.10.1.4	74.53.140.153	SMTP	90	C: MAIL FROM: <gurpartap@patriots.in>
17	2.464705	74.53.140.153	10.10.1.4	SMTP	62	S: 250 OK
18	2.465190	10.10.1.4	74.53.140.153	SMTP	93	C: RCPT TO: <raj_deol2002in@yahoo.co.in>
19	2.827648	74.53.140.153	10.10.1.4	SMTP	68	S: 250 Accepted
20	2.828143	10.10.1.4	74.53.140.153	SMTP	60	C: DATA
21	3.169619	74.53.140.153	10.10.1.4	SMTP	110	S: 354 Enter message, ending with "." on a line by itself
22	3.200683	10.10.1.4	74.53.140.153	SMTP	1514	C: DATA fragment, 1460 bytes
23	3.200726	10.10.1.4	74.53.140.153	SMTP	1514	C: DATA fragment, 1460 bytes
24	3.200744	10.10.1.4	74.53.140.153	SMTP	1514	C: DATA fragment, 1460 bytes
25	3.200763	10.10.1.4	74.53.140.153	SMTP	1514	[TCP Window Full] C: DATA fragment, 1460 bytes
38	4.002121	10.10.1.4	74.53.140.153	SMTP	1506	C: DATA fragment, 1452 bytes
39	4.002139	10.10.1.4	74.53.140.153	SMTP	1506	C: DATA fragment, 1452 bytes
41	4.342568	10.10.1.4	74.53.140.153	SMTP	1506	C: DATA fragment, 1452 bytes

Frame 6: 235 bytes on wire (1880 bits). 235 bytes captured (1880 bits) on interface 0

Simple Mail Transfer Protocol: Protocol

Packets: 60 · Displayed: 32 (53.3%)

Profile: Default

Reveal the location of any IP address.

74.53.140.153 Lookup

IP Address: 74.53.140.153	IP Address: 74.53.140.153
ASN: 36351	ASN: 36351
City: San Jose	City:
State/Region: California	State/Region:
Country: United States of America	Country: United States
Postal Code: 95101	Postal Code:
ISP: SoftLayer Technologies Inc.	ISP: Softlayer DAL
Time Zone: -07:00	Time Zone:
<a href="#">IP2Location.com</a> Results	<a href="#">IPData.co</a> Results

```
C:\Users\Nadya Permata>ncat 10.21.78.111 11111
a. Berapa banyak packet yang berhasil di capture dari file pcap tersebut?
Your answer: 60
Correct answer!
b. Port berapakah pada server yang digunakan untuk service SMTP?
Your answer: 25
Correct answer!
c. Dari semua alamat IP yang tercapture, IP berapakah yang merupakan public IP?
Your answer: 74.53.140.153
Correct answer!
Correct answers, you are good at analysis!
Here is your flag: Jarkom2023{k0w4lski_8474_DiAFzRiNjBi_4nalysis}
```

6.

7. 6

soal6-9.pcapng

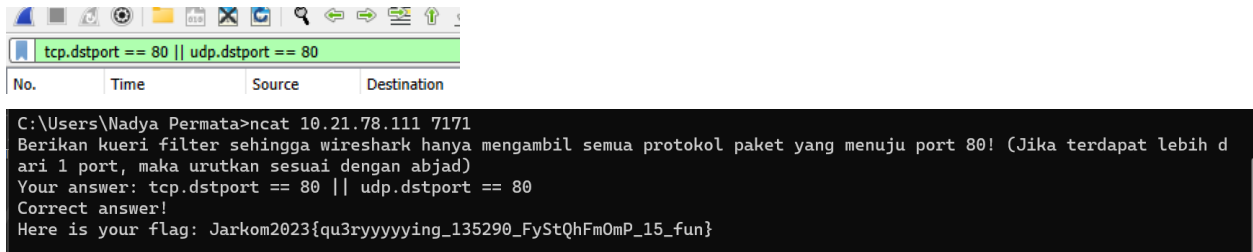
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 184.87.193.88

No.	Time	Source	Destination	Protocol	Length	Info
7536	443.883050	10.100....	184.87....	TCP	66	55761 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7538	443.974799	10.100....	184.87....	TCP	54	55761 → 80 [ACK] Seq=1 Ack=1 Win=131584 Len=0
7539	443.975181	10.100....	184.87....	HTTP	208	GET /connecttest.txt HTTP/1.1
7541	443.991579	10.100....	184.87....	TCP	66	[TCP Dup ACK 7538#1] 55761 → 80 [ACK] Seq=155 Ack=1 Win=131584 Len=0 SLE=0 SRE=1
7544	444.017559	10.100....	184.87....	TCP	54	55761 → 80 [FIN, ACK] Seq=155 Ack=188 Win=131328 Len=0
7546	444.029868	10.100....	184.87....	TCP	54	55761 → 80 [ACK] Seq=156 Ack=189 Win=131328 Len=0



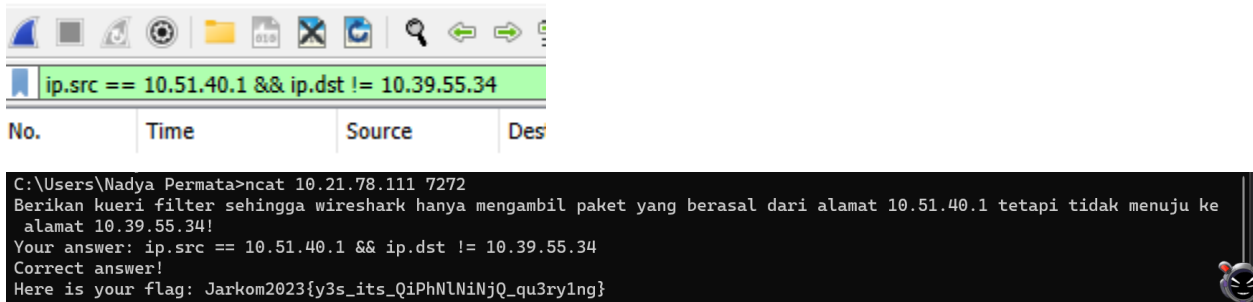
8. tcp.dstport == 80 || udp.dstport == 80



The image shows a Wireshark window with the filter `tcp.dstport == 80 || udp.dstport == 80` applied. Below it, a terminal window displays the following text:

```
C:\Users\Nadya Permata>ncat 10.21.78.111 7171
Berikan kueri filter sehingga wireshark hanya mengambil semua protokol paket yang menuju port 80! (Jika terdapat lebih d
ari 1 port, maka urutkan sesuai dengan abjad)
Your answer: tcp.dstport == 80 || udp.dstport == 80
Correct answer!
Here is your flag: Jarkom2023{qu3ryyyyinyng_135290_FyStQhFm0mP_15_fun}
```

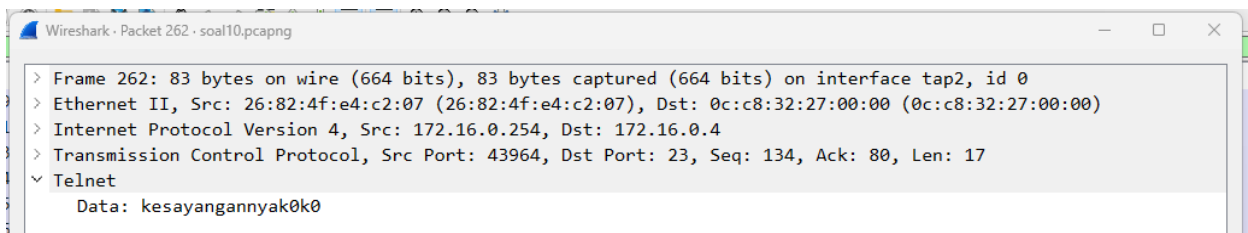
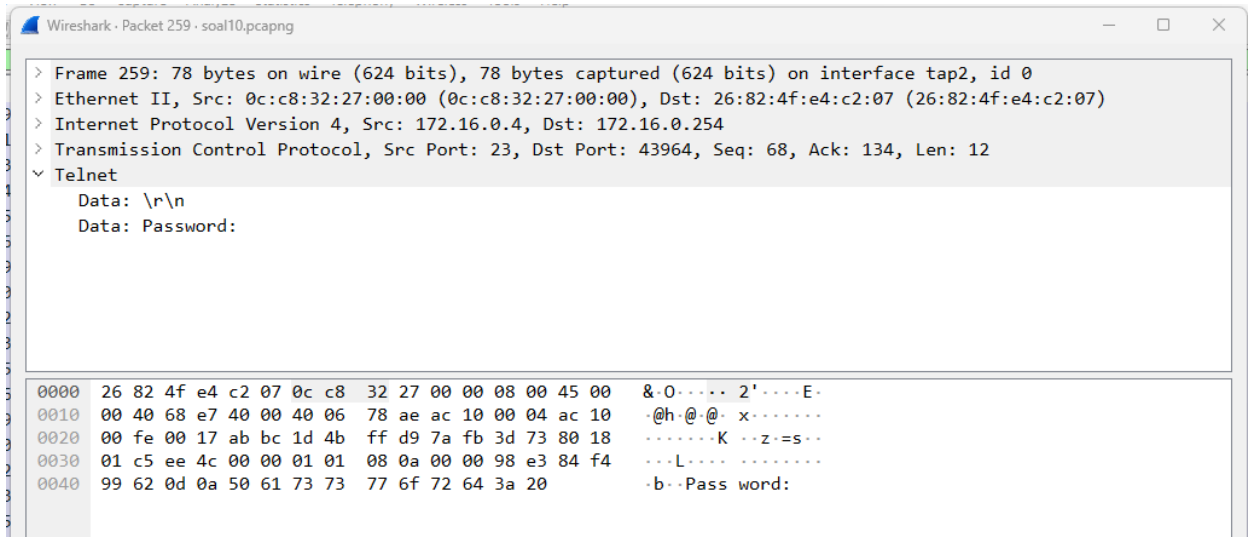
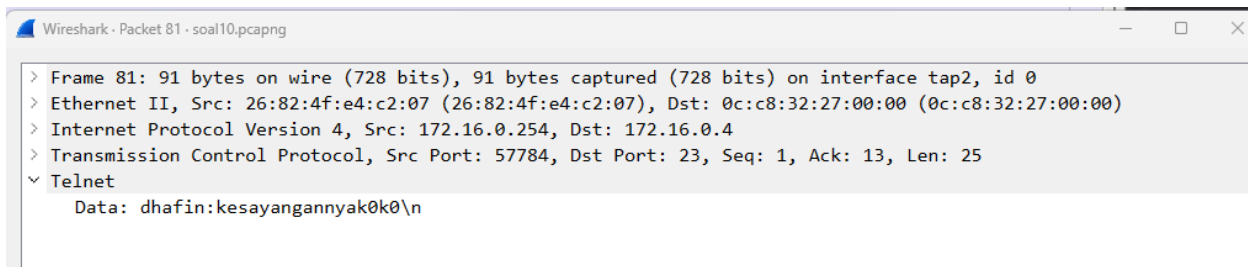
9. ip.src == 10.51.40.1 && ip.dst != 10.39.55.34



The image shows a Wireshark window with the filter `ip.src == 10.51.40.1 && ip.dst != 10.39.55.34` applied. Below it, a terminal window displays the following text:

```
C:\Users\Nadya Permata>ncat 10.21.78.111 7272
Berikan kueri filter sehingga wireshark hanya mengambil paket yang berasal dari alamat 10.51.40.1 tetapi tidak menuju ke
alamat 10.39.55.34!
Your answer: ip.src == 10.51.40.1 && ip.dst != 10.39.55.34
Correct answer!
Here is your flag: Jarkom2023{y3s_its_QiPhNlNiNjQ_qu3ry1ng}
```

## 10. dhafin:kesayangannyak0k0



```
C:\Users\Nadya Permata>ncat 10.21.78.111 7373
Sebutkan kredensial yang benar ketika user mencoba login menggunakan Telnet, format [username]:[password]!
Your answer: dhafin:kesayangannyak0k0
Correct answer!
Here is your flag: Jarkom2023{t3lnet_is_8z62A30ABz3xyAxBc_N0tSecu2e}
```