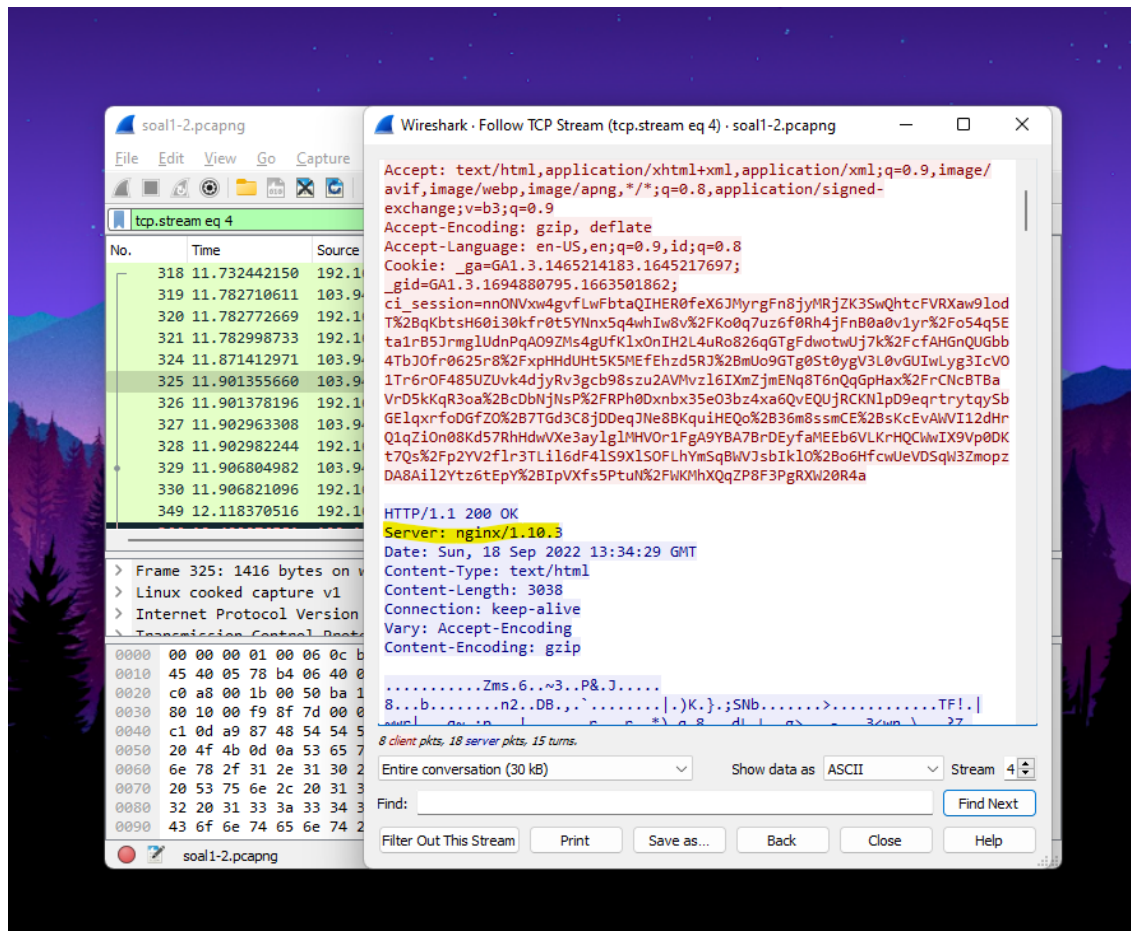


## Praktikum Modul 1 - Kelompok

### 1. Nginx

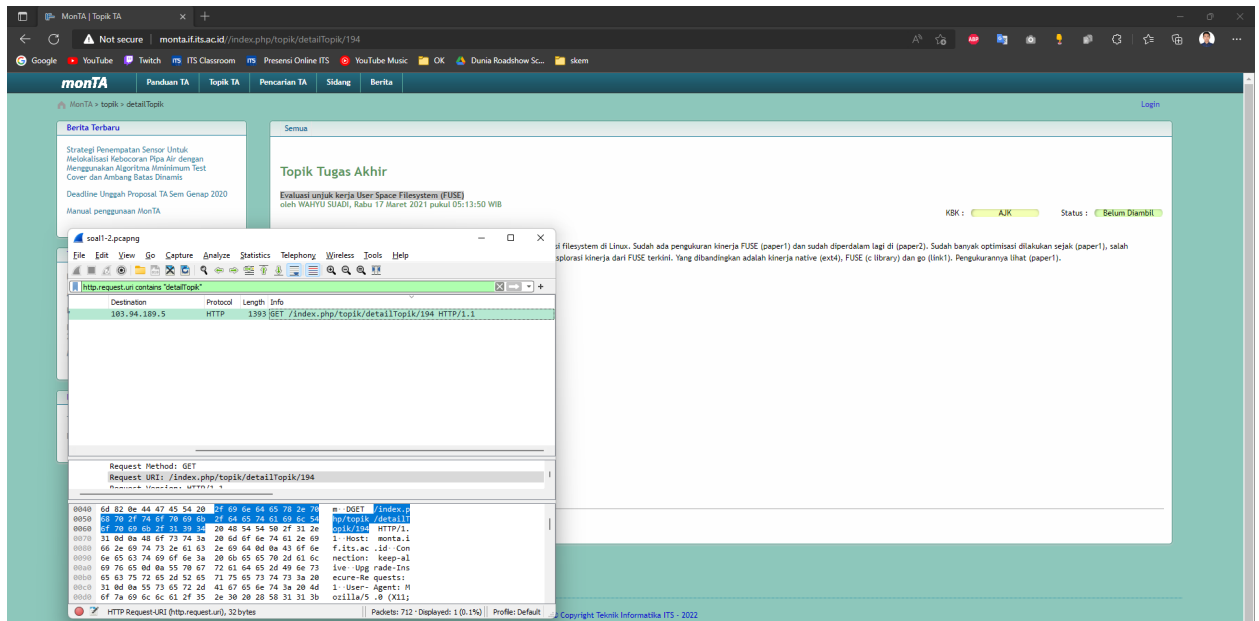


Informasi web server pada website [monta.if.its.ac.id](http://monta.if.its.ac.id) dapat diketahui dengan tahap sebagai berikut :

1. Melakukan filter **capture** untuk semua paket yang berasal dan diterima oleh internet yang diakses perangkat
2. Membuka web [monta.if.its.ac.id](http://monta.if.its.ac.id) sehingga paket dari website tersebut dapat ditangkap oleh wireshark
3. Untuk mengetahui servernya, kita dapat memilih menu “Analyze” kemudian “Follow” dan memilih “TCP Stream”
4. Referensi :

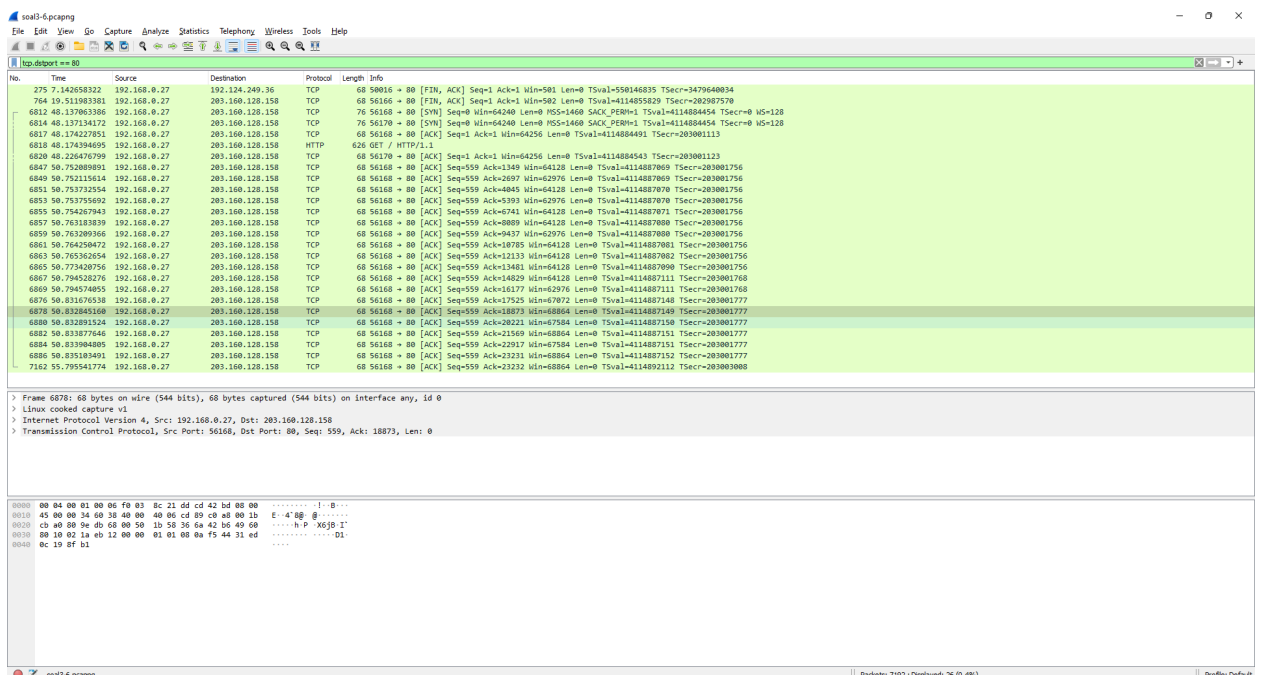
[https://www.wireshark.org/docs/wsug\\_html\\_chunked/ChAdvFollowStreamSection.html](https://www.wireshark.org/docs/wsug_html_chunked/ChAdvFollowStreamSection.html)

## 2. Evaluasi unjuk kerja User Space Filesystem (FUSE) Filter : http.request.uri contains "detailTopik"



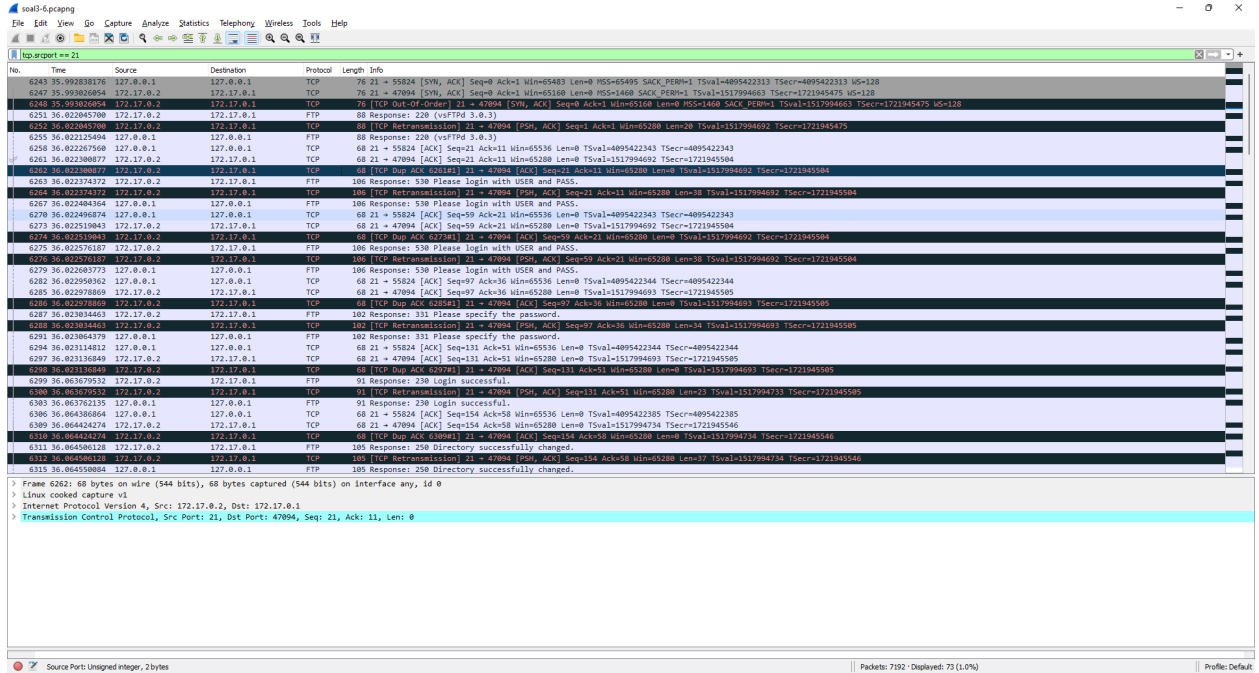
Untuk soal nomor 2, perlu menggunakan bantuan file dari folder *resource*. Ketika file tersebut dibuka, maka akan muncul paket-paket apa saja yang sudah *capture*. Setelah itu dilakukan filter yang hanya menampilkan string bernama **detailTopik** (http.request.uri contains "detailTopik"). Wireshark akan menampilkan alamat url http yang mengandung string “detailTopik”. Maka setelah itu, kita tinggal mengikuti alamat tersebut di peramban setelah alamat monta.if.its.ac.id

## 3. display, tcp.dstport == 80



File pcapng sudah berisi paket paket yang dicapture, sehingga kita tidak perlu lagi melakukan capture lagi. Untuk mendapatkan paket yang menuju port 80, maka kita bisa menggunakan fitur **display** dengan sintaks **tcp.dstport == 80**

#### 4. Capture, tcp.srcport == 21

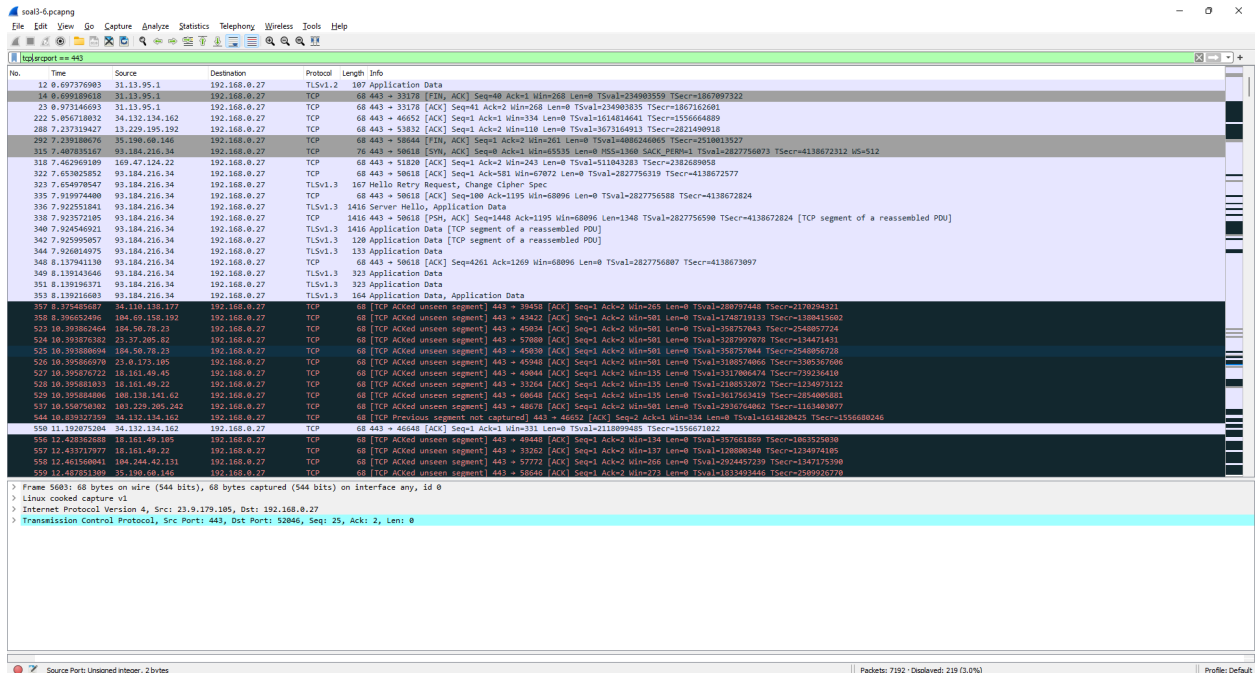


The image shows a Wireshark capture of a Telnet session. The filter bar at the top is set to 'tcp.srcport == 21'. The packet list shows several packets, including a SYN packet (6243) and a series of data packets (6255-6315) representing the Telnet session. The packet details pane shows the structure of the Telnet data, including the 'Telnet Option' field.

No.	Time	Source	Destination	Protocol	Length	Info
6243	35.992838176	172.17.0.1	172.17.0.1	TCP	76	21 → 55824 [SYN, ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=65536 SACK_PERM=1 TSval=4895422313 TSecr=4895422313 US=128
6247	35.993026954	172.17.0.2	172.17.0.1	TCP	76	21 → 47894 [SYN, ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=65536 SACK_PERM=1 TSval=1517994663 TSecr=1721945475 US=128
6248	35.993026954	172.17.0.2	172.17.0.1	TCP	76	1700 → 47894 [ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=65536 SACK_PERM=1 TSval=1517994663 TSecr=1721945475 US=128
6251	36.022457800	172.17.0.2	172.17.0.1	FTP	88	Response: 220 (vsFTPd 3.0.3)
6252	36.022457800	172.17.0.2	172.17.0.1	FTP	68	1700 → 47894 [ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=65536 SACK_PERM=1 TSval=1517994663 TSecr=1721945475 US=128
6255	36.022525404	172.17.0.1	172.17.0.1	FTP	68	Response: 220 (vsFTPd 3.0.3)
6258	36.022575600	172.17.0.1	172.17.0.1	FTP	68	21 → 55824 [ACK] Seq=21 Ack=11 Win=65536 Len=0 TSval=4895422343 TSecr=4895422343
6261	36.022580877	172.17.0.2	172.17.0.1	TCP	68	21 → 47894 [ACK] Seq=21 Ack=11 Win=65536 Len=0 TSval=1517994663 TSecr=1721945475 US=128
6262	36.022580877	172.17.0.2	172.17.0.1	TCP	68	1700 → 47894 [ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=65536 SACK_PERM=1 TSval=1517994663 TSecr=1721945475 US=128
6263	36.022574372	172.17.0.2	172.17.0.1	FTP	106	Response: 530 Please login with USER and PASS.
6264	36.022574372	172.17.0.2	172.17.0.1	TCP	106	TCP Retransmission[21] = 47894 [PSH, ACK] Seq=59 Ack=1 Win=65280 Len=36 TSval=1517994663 TSecr=1721945475 US=128
6267	36.02246874	172.17.0.1	172.17.0.1	FTP	106	Response: 530 Please login with USER and PASS.
6270	36.02246874	172.17.0.1	172.17.0.1	TCP	68	21 → 55824 [ACK] Seq=59 Ack=21 Win=65536 Len=0 TSval=4895422344 TSecr=4895422344
6273	36.022519843	172.17.0.2	172.17.0.1	TCP	68	21 → 47894 [ACK] Seq=59 Ack=21 Win=65536 Len=0 TSval=1517994663 TSecr=1721945475 US=128
6274	36.022519843	172.17.0.2	172.17.0.1	TCP	68	1700 → 47894 [ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=65536 SACK_PERM=1 TSval=1517994663 TSecr=1721945475 US=128
6275	36.022576187	172.17.0.2	172.17.0.1	FTP	106	Response: 530 Please login with USER and PASS.
6276	36.022576187	172.17.0.2	172.17.0.1	TCP	106	TCP Retransmission[21] = 47894 [PSH, ACK] Seq=59 Ack=21 Win=65280 Len=36 TSval=1517994663 TSecr=1721945475 US=128
6279	36.022603773	172.17.0.1	172.17.0.1	FTP	106	Response: 530 Please login with USER and PASS.
6282	36.022604062	172.17.0.1	172.17.0.1	TCP	68	21 → 55824 [ACK] Seq=131 Ack=51 Win=65536 Len=0 TSval=4895422344 TSecr=4895422344
6285	36.022978869	172.17.0.2	172.17.0.1	TCP	68	21 → 47894 [ACK] Seq=87 Ack=36 Win=65536 Len=0 TSval=1517994663 TSecr=1721945475 US=128
6289	36.022978869	172.17.0.2	172.17.0.1	TCP	68	1700 → 47894 [ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=65536 SACK_PERM=1 TSval=1517994663 TSecr=1721945475 US=128
6292	36.023014463	172.17.0.2	172.17.0.1	TCP	68	1700 → 47894 [ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=65536 SACK_PERM=1 TSval=1517994663 TSecr=1721945475 US=128
6298	36.023044463	172.17.0.2	172.17.0.1	TCP	102	TCP Retransmission[21] = 47894 [PSH, ACK] Seq=97 Ack=36 Win=65280 Len=34 TSval=1517994663 TSecr=1721945475 US=128
6291	36.023064379	172.17.0.1	172.17.0.1	FTP	102	Response: 331 Please specify the password.
6294	36.023114812	172.17.0.1	172.17.0.1	TCP	68	21 → 55824 [ACK] Seq=131 Ack=51 Win=65536 Len=0 TSval=4895422344 TSecr=4895422344
6297	36.023136849	172.17.0.2	172.17.0.1	TCP	68	21 → 47894 [ACK] Seq=131 Ack=51 Win=65280 Len=0 TSval=1517994663 TSecr=1721945475 US=128
6298	36.023136849	172.17.0.2	172.17.0.1	TCP	68	TCP Dup ACK 6297[21] = 47894 [ACK] Seq=131 Ack=51 Win=65280 Len=0 TSval=1517994663 TSecr=1721945475 US=128
6299	36.023079512	172.17.0.2	172.17.0.1	FTP	91	Response: 330 Login successful.
6300	36.023079512	172.17.0.2	172.17.0.1	TCP	91	TCP Retransmission[21] = 47894 [PSH, ACK] Seq=131 Ack=51 Win=65280 Len=23 TSval=1517994733 TSecr=1721945475 US=128
6303	36.063762135	172.17.0.1	172.17.0.1	FTP	91	Response: 230 Login successful.
6306	36.063806804	172.17.0.1	172.17.0.1	TCP	68	21 → 55824 [ACK] Seq=154 Ack=58 Win=65536 Len=0 TSval=4895422385 TSecr=4895422385
6309	36.064424274	172.17.0.2	172.17.0.1	TCP	68	21 → 47894 [ACK] Seq=154 Ack=58 Win=65280 Len=0 TSval=1517994734 TSecr=1721945475 US=128
6310	36.064424274	172.17.0.2	172.17.0.1	TCP	68	1700 → 47894 [ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=65536 SACK_PERM=1 TSval=1517994734 TSecr=1721945475 US=128
6311	36.06446128	172.17.0.2	172.17.0.1	FTP	105	Response: 250 Directory successfully changed.
6312	36.06446128	172.17.0.2	172.17.0.1	TCP	105	TCP Retransmission[21] = 47894 [PSH, ACK] Seq=154 Ack=58 Win=65280 Len=37 TSval=1517994734 TSecr=1721945475 US=128
6315	36.064550884	172.17.0.1	172.17.0.1	FTP	105	Response: 250 Directory successfully changed.

File pcapng sudah berisi paket paket yang dicapture, sehingga kita tidak perlu lagi melakukan capture lagi. Untuk mengambil paket yang berasal dari port 21, maka kita bisa menggunakan fitur **capture** dengan sintaks **tcp.srcport == 21**

#### 5. Capture, tcp.srcport == 443

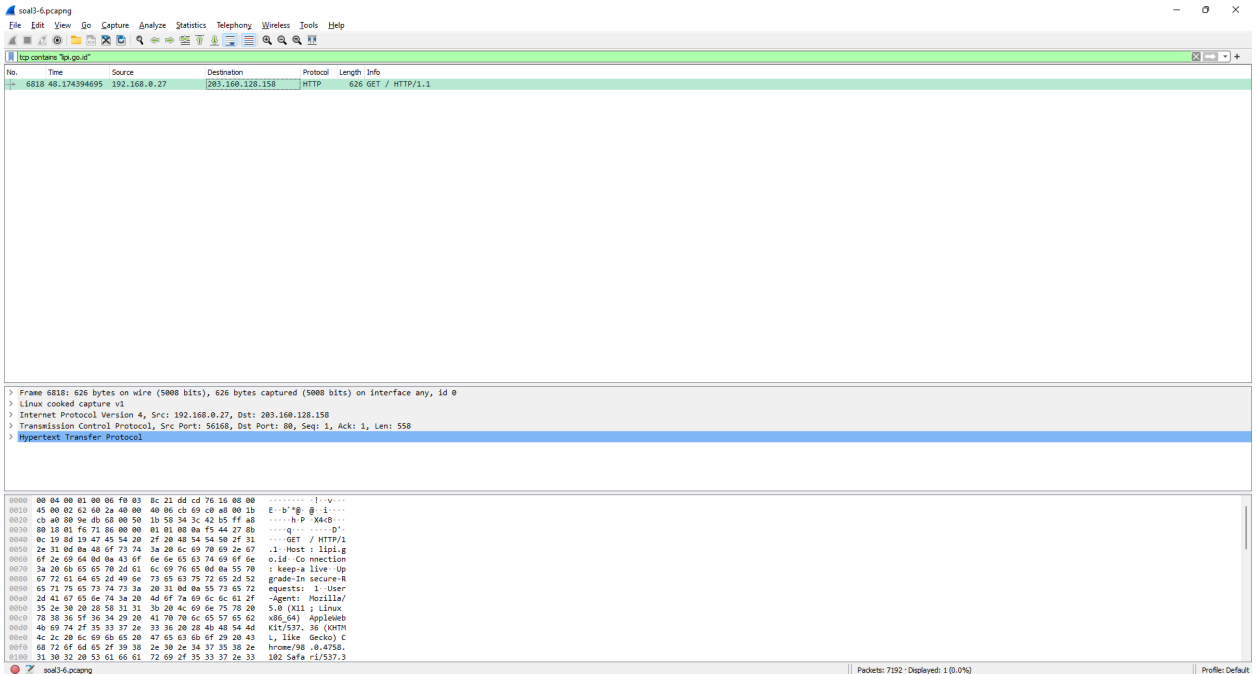


The image shows a Wireshark capture of an HTTPS session. The filter bar at the top is set to 'tcp.srcport == 443'. The packet list shows several packets, including a SYN packet (12) and a series of data packets (13-100) representing the HTTPS session. The packet details pane shows the structure of the data, including the 'Application Data' field.

No.	Time	Source	Destination	Protocol	Length	Info
12	0.007376980	31.13.95.1	192.168.0.27	TLSv1.2	107	Application Data
14	0.009180610	31.13.95.1	192.168.0.27	TCP	68	443 → 33178 [FIN, ACK] Seq=40 Ack=1 Win=260 Len=0 TSval=234903559 TSecr=1867707322
23	0.973146693	31.13.95.1	192.168.0.27	TCP	68	443 → 33178 [ACK] Seq=41 Ack=2 Win=260 Len=0 TSval=234903835 TSecr=1867162601
222	5.050710832	34.132.134.162	192.168.0.27	TCP	68	443 → 44652 [ACK] Seq=1 Ack=1 Win=354 Len=0 TSval=1614014641 TSecr=1556684809
288	7.237131427	33.229.195.192	192.168.0.27	TCP	68	443 → 44652 [ACK] Seq=1 Ack=1 Win=110 Len=0 TSval=1607164913 TSecr=1821480918
292	7.239180676	35.130.60.146	192.168.0.27	TCP	68	443 → 58644 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0 TSval=4486624065 TSecr=2518013527
315	7.407893517	93.184.216.34	192.168.0.27	TCP	76	443 → 58618 [SYN, ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=65536 SACK_PERM=1 TSval=2827756873 TSecr=4138672312 US=512
318	7.402960189	109.148.124.22	192.168.0.27	TCP	68	443 → 51828 [ACK] Seq=1 Ack=2 Win=261 Len=0 TSval=4118421283 TSecr=2382609858
322	7.453825852	93.184.216.34	192.168.0.27	TCP	68	443 → 58618 [ACK] Seq=1 Ack=81 Win=6792 Len=0 TSval=2827756319 TSecr=4138672577
323	7.454078547	93.184.216.34	192.168.0.27	TLSv1.3	167	Hello Retry Request, Change Cipher Spec
325	7.503974009	93.184.216.34	192.168.0.27	TCP	68	443 → 58618 [ACK] Seq=100 Ack=195 Win=68096 Len=0 TSval=2827756580 TSecr=4138672824
336	7.922551841	93.184.216.34	192.168.0.27	TLSv1.3	1416	Server Hello, Application Data
338	7.923721205	93.184.216.34	192.168.0.27	TCP	1416	443 → 58618 [PSH, ACK] Seq=1448 Ack=195 Win=68096 Len=1348 TSval=2827756590 TSecr=4138672824 [TCP segment of a reassembled PDU]
340	7.924546921	93.184.216.34	192.168.0.27	TLSv1.3	1416	Application Data [TCP segment of a reassembled PDU]
342	7.925995957	93.184.216.34	192.168.0.27	TLSv1.3	120	Application Data [TCP segment of a reassembled PDU]
344	7.926814975	93.184.216.34	192.168.0.27	TLSv1.3	133	Application Data
348	8.137941130	93.184.216.34	192.168.0.27	TCP	68	443 → 58618 [ACK] Seq=4261 Ack=1209 Win=68096 Len=0 TSval=2827756807 TSecr=4138673097
349	8.139143646	93.184.216.34	192.168.0.27	TLSv1.3	323	Application Data
351	8.139196371	93.184.216.34	192.168.0.27	TLSv1.3	323	Application Data
353	8.139216683	93.184.216.34	192.168.0.27	TLSv1.3	364	Application Data, Application Data
354	8.139245651	194.187.183.177	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 33178 [ACK] Seq=1 Ack=2 Win=260 Len=0 TSval=280777448 TSecr=2178294321
358	8.396652496	104.69.158.192	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 44652 [ACK] Seq=1 Ack=2 Win=583 Len=0 TSval=1748719133 TSecr=1380415682
523	10.393824264	184.58.78.23	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 44652 [ACK] Seq=1 Ack=2 Win=583 Len=0 TSval=1358757043 TSecr=2548057724
524	10.393826162	23.27.205.82	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 57800 [ACK] Seq=1 Ack=2 Win=592 Len=0 TSval=1827970707 TSecr=134471421
525	10.393880604	184.58.78.23	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 44652 [ACK] Seq=1 Ack=2 Win=583 Len=0 TSval=1358757044 TSecr=2548057728
526	10.395866970	23.0.173.105	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 44652 [ACK] Seq=1 Ack=2 Win=583 Len=0 TSval=1318574866 TSecr=3365367896
527	10.395870722	10.161.40.22	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 40844 [ACK] Seq=1 Ack=2 Win=125 Len=0 TSval=1337806674 TSecr=739225618
528	10.395881833	10.161.40.22	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 33264 [ACK] Seq=1 Ack=2 Win=135 Len=0 TSval=12188532072 TSecr=1234973122
529	10.395884806	108.138.143.62	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 60848 [ACK] Seq=1 Ack=2 Win=135 Len=0 TSval=13617656419 TSecr=2854085881
537	10.530756382	183.229.205.242	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 48070 [ACK] Seq=1 Ack=2 Win=583 Len=0 TSval=18263676482 TSecr=1163483877
544	10.639272359	35.132.134.162	192.168.0.27	TCP	68	TCP Previous segment not captured 443 → 44652 [ACK] Seq=2 Ack=1 Win=134 Len=0 TSval=1614014641 TSecr=1556682340
550	11.329292304	34.132.134.162	192.168.0.27	TCP	68	443 → 44648 [ACK] Seq=1 Ack=1 Win=331 Len=0 TSval=2118099485 TSecr=1556671822
556	12.42812688	10.161.40.105	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 49448 [ACK] Seq=1 Ack=2 Win=134 Len=0 TSval=1576018189 TSecr=1803575838
557	12.43717877	10.161.40.22	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 33162 [ACK] Seq=1 Ack=2 Win=137 Len=0 TSval=1288081048 TSecr=1234974185
558	12.461500841	104.244.42.131	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 57772 [ACK] Seq=1 Ack=2 Win=266 Len=0 TSval=19244557239 TSecr=1347175398
559	12.487851309	35.130.60.146	192.168.0.27	TCP	68	TCP ACKed unsent segment 443 → 58646 [ACK] Seq=1 Ack=2 Win=273 Len=0 TSval=1613491446 TSecr=2509526778

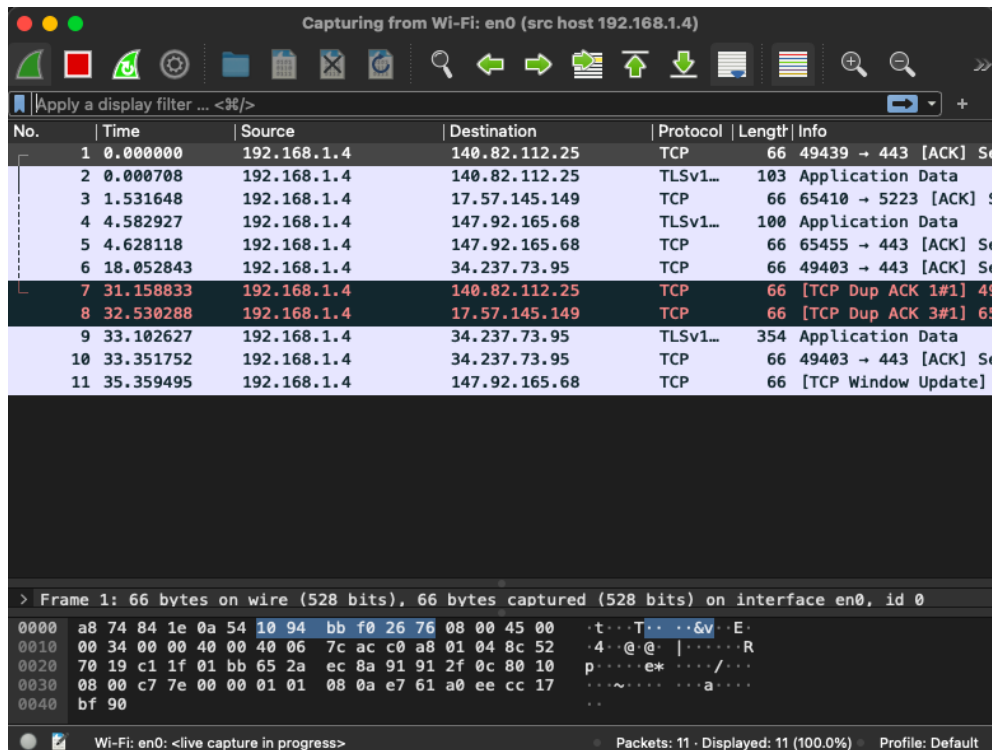
File pcapng sudah berisi paket paket yang dicapture, sehingga kita tidak perlu lagi melakukan capture lagi. Untuk mengambil paket yang berasal dari port 443, maka kita bisa menggunakan fitur **capture** dengan sintaks **tcp.srcport == 443**

## 6. Display, tcp contains "lipi.go.id"

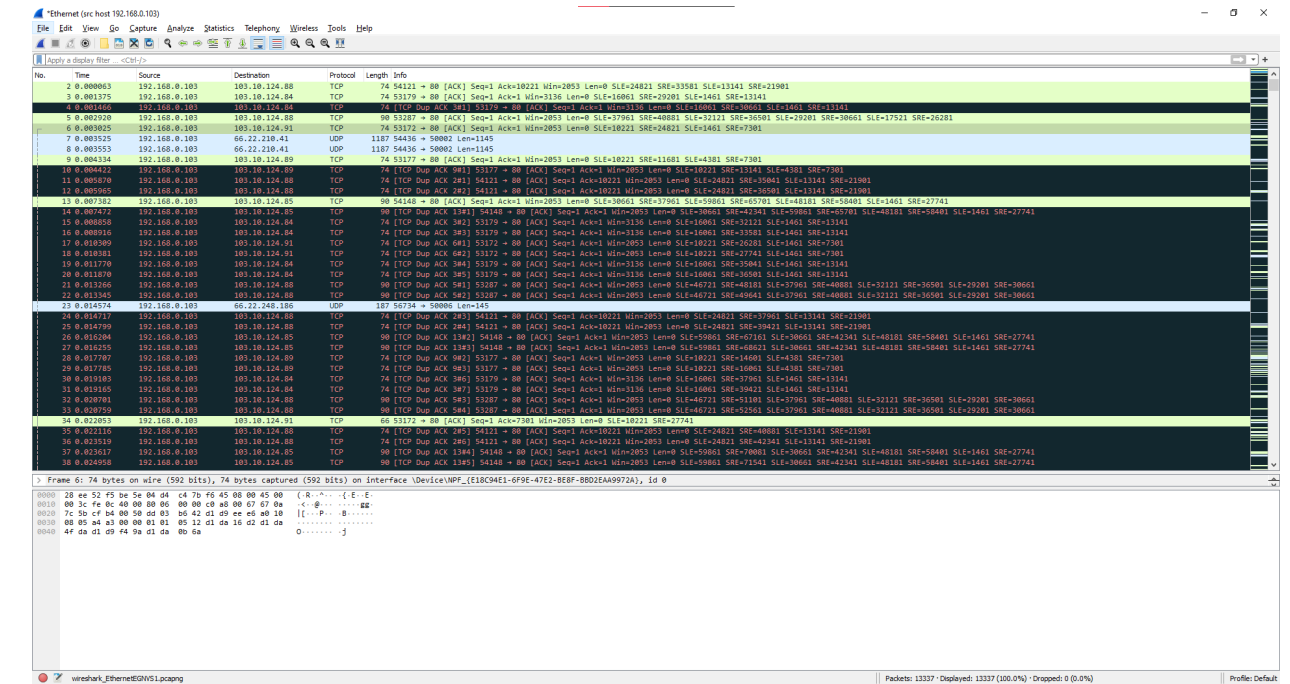


File pcapng sudah berisi paket paket yang dicapture, sehingga kita tidak perlu lagi melakukan capture lagi. Untuk mendapatkan paket yang berasal dari website lipi.go.id, maka kita bisa menggunakan fitur **display** dengan sintaks **tcp contains "lipi.go.id"**

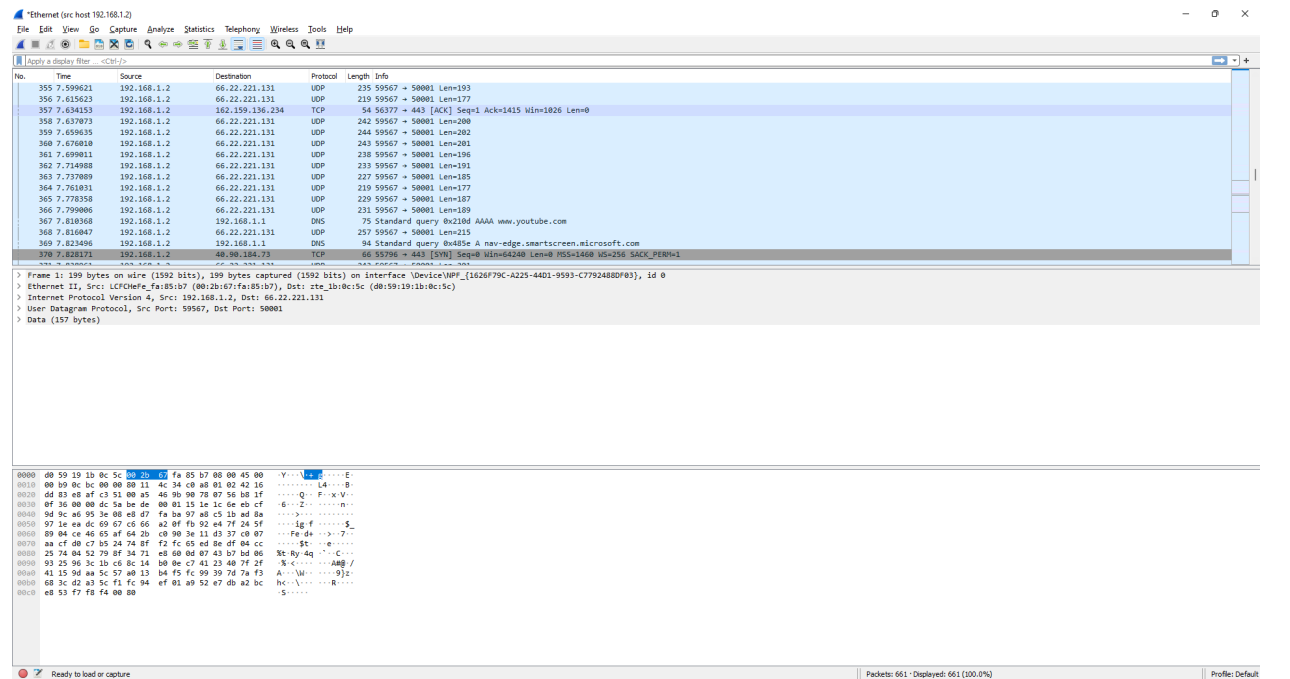
## 7. 1. src host 192.168.1.4 (Angela Oryza)



## 2. src host 192.168.0.103 (Naufal Fabian W)



## 3. src host 192.168.1.2 (Helmi Taqiyudin)



Untuk mengambil paket yang berasal dari IP Address kita, kita perlu mencari tahu IP Address dari koneksi masing-masing terlebih dahulu. Setelah mendapatkannya, maka kita tinggal menggunakan fitur **capture** dari wireshark untuk mengambil paket-paket yang hanya berasal dari IP Address kita dengan sintaks **src host IP Address**

8. .

The screenshot displays the Wireshark interface with a packet capture of a file named 'soal8-10.pcapng'. The main pane shows a list of network packets. Packet 45 is selected, and the 'Follow TCP Stream' window is open, displaying the raw data of the selected stream. The data is a text-based chat conversation in Indonesian. The status bar at the bottom indicates that 215 packets were captured, and 40 (18.6%) are currently displayed. The profile is set to 'Default'.

No.	Time	Source
13	62.283148	127.0.0.1
14	62.283159	127.0.1.1
15	62.283166	127.0.0.1
17	72.066024	127.0.0.1
18	72.066051	127.0.1.1
20	77.010613	127.0.1.1
21	77.010642	127.0.0.1
24	91.907741	127.0.0.1
25	91.907769	127.0.1.1
26	98.226188	127.0.1.1
27	98.226216	127.0.0.1
29	103.747331	127.0.0.1
30	103.747357	127.0.1.1
31	109.666622	127.0.1.1
32	109.666653	127.0.0.1
33	115.986799	127.0.0.1
34	115.986826	127.0.1.1
38	121.683087	127.0.1.1
39	121.683111	127.0.0.1
43	127.250167	127.0.0.1
44	127.250199	127.0.1.1
45	134.002729	127.0.1.1
46	134.002774	127.0.0.1
47	142.130146	127.0.0.1
48	142.130173	127.0.1.1
50	148.817751	127.0.1.1
51	148.817795	127.0.0.1
54	153.633683	127.0.0.1
55	153.633714	127.0.1.1

Frame 45: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits) on interface 0

9 client pkts, 8 server pkts, 16 turns.

Entire conversation (832 bytes) Show data as ASCII Stream 12

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

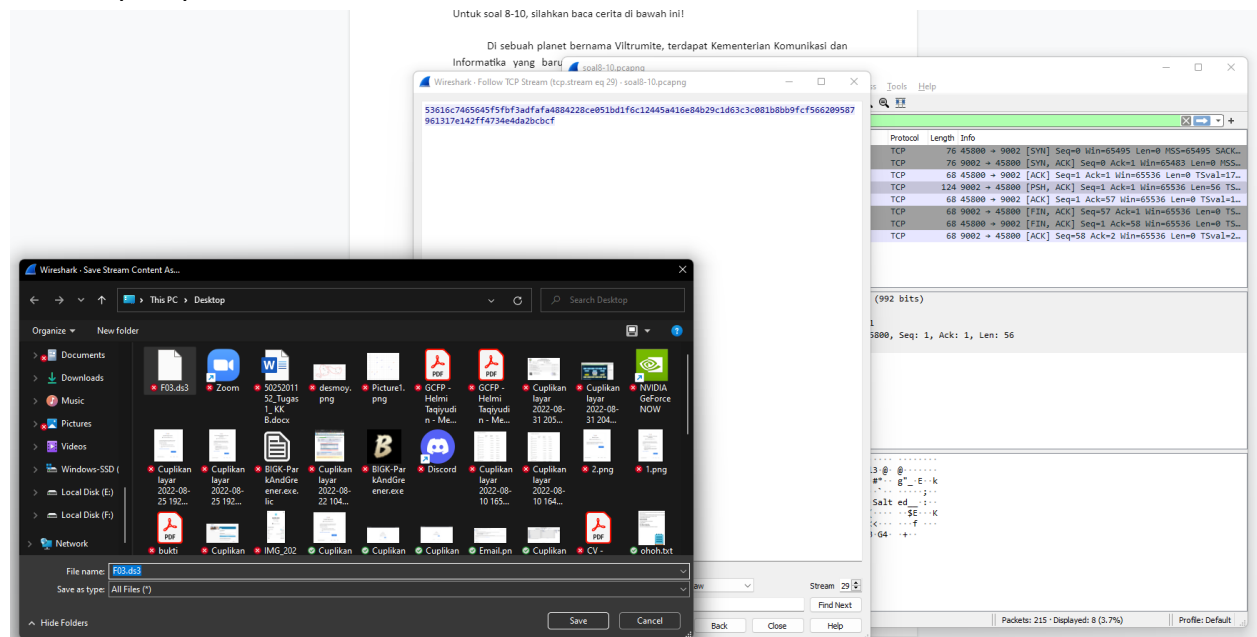
Packets: 215 · Displayed: 40 (18.6%) Profile: Default

Karena protokol dengan keandalan yang tinggi adalah TCP, maka paket yang perlu kita filter adalah paket dengan protokol TCP. Setelah itu, kita tinggal menggunakan menu Analyze -> Follow -> TCP Stream dan mencari percakapan sebagai bukti contekan



9.

Filter : tcp.srcport==9002



Untuk menyimpan file yang dijadikan contekan, kita perlu menggunakan filter dengan sintaks **tcp.srcport==9002**. Setelah menemukan paket-paket yang berasal dari port 9002, kita membaca salah satu paket dengan mengubahnya ke RAW karena file tersebut sudah sempat diencode ke salted. Setelah itu disimpan dengan nama **F03.des3**.

Untuk mengubahnya ke file flag.txt, maka digunakan CLI dengan command **openssl des3 -d salt -in F03.des3 -out flag.txt -k nakano**. Password nakano didapatkan dari clue di percakapan rahasia mereka

10.

Pass : nakano

