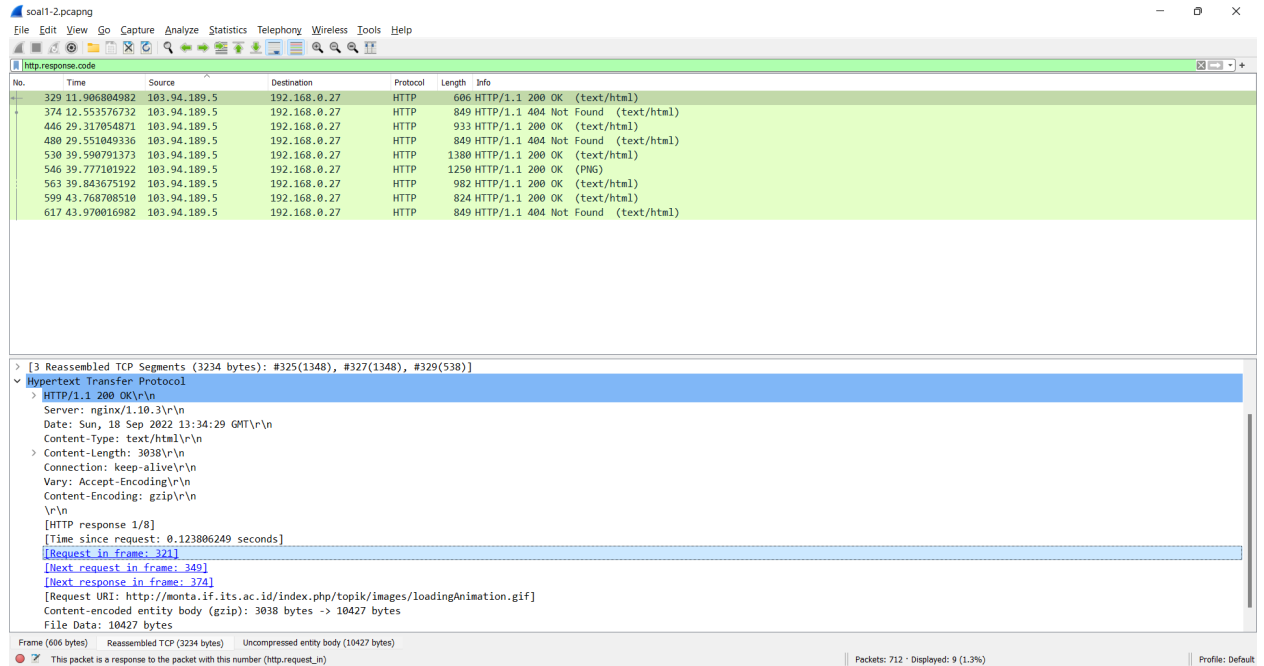


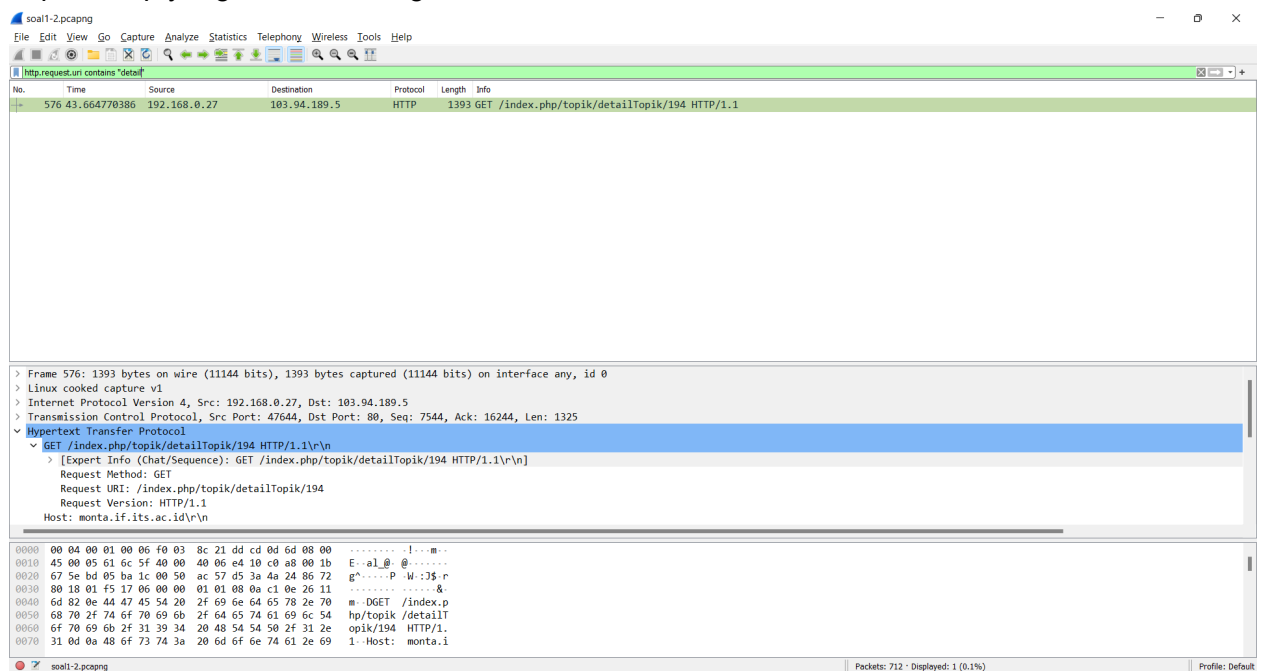
Kelompok ITA10
Hafizh Abid Wibowo 5027201011
Muhammad Farrel Abdillah 5027201057

1. Dengan menggunakan display filter `http.response.code` kita bisa mendapatkan response dari protokol http kemudian terdapat beberapa informasi seperti Server dan HTTP response tersebut merupakan respons dari Request URL yang mana.



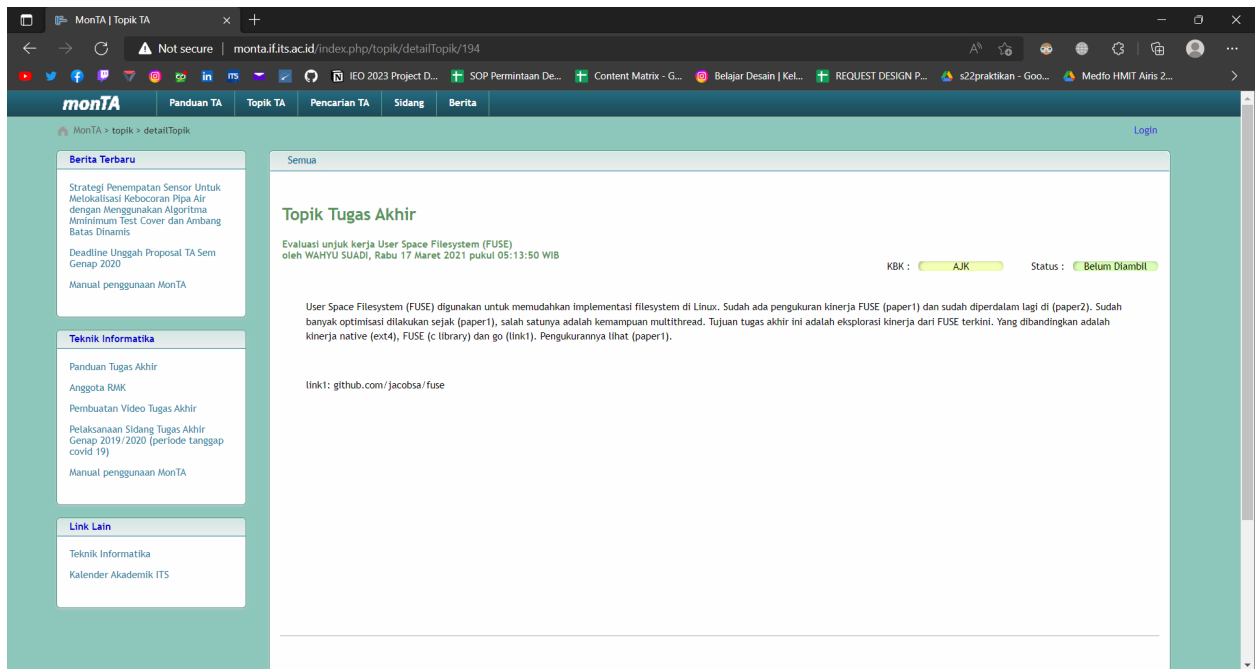
Dari response diatas dapat dilihat bahwa Web server dari monta merupakan: `nginx/1.10.3`

2. Menggunakan `http.request.uri contains "detail"`, dari filter tersebut kita bisa mendisplay request http yang memiliki string "detail".



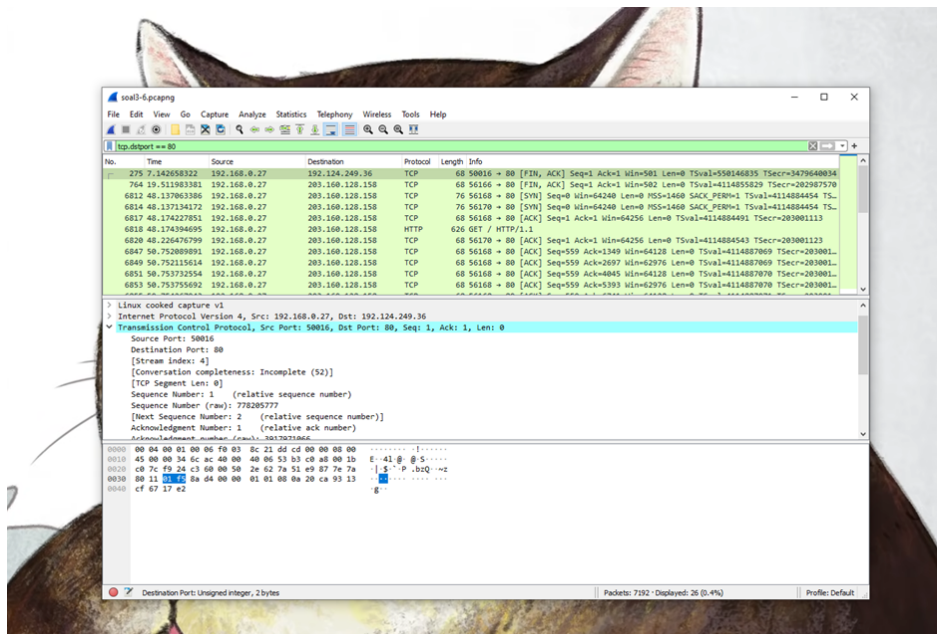
Kemudian buka full url di web browser

Kelompok ITA10
Hafizh Abid Wibowo 5027201011
Muhammad Farrel Abdillah 5027201057



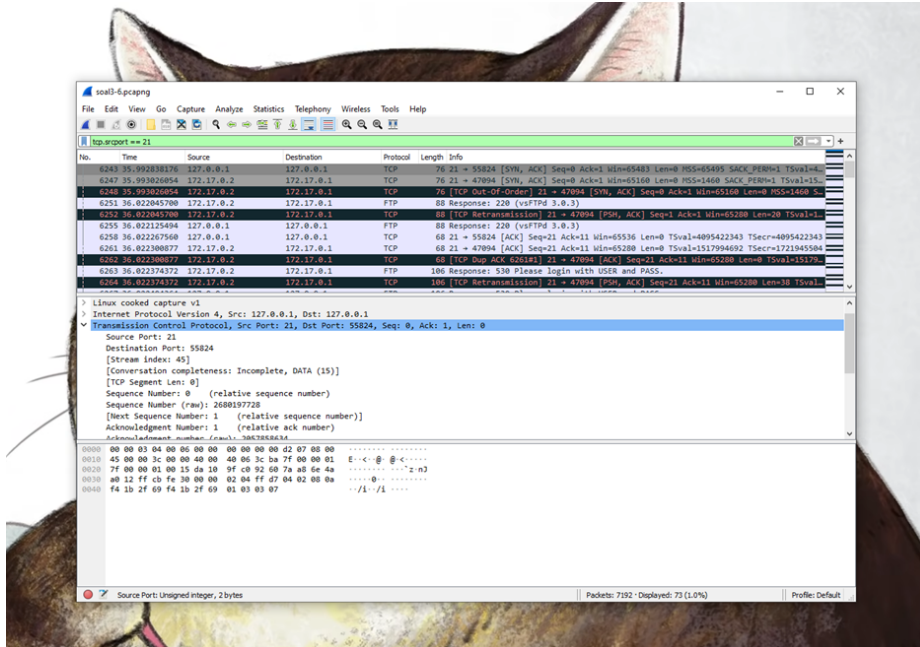
Maka didapat judul TA yang dibuka oleh Ishaq adalah
Evaluasi unjuk kerja User Space Filesystem (FUSE)

3. Dalam Soal 3-6, telah diberikan file dengan format .pcapng pada sebuah google drive. Untuk membukanya, harus memiliki wireshark yang telah terinstall pada pc. lalu hanya perlu open file saja pada wireshark nya Menggunakan tcp.dstport == 80, dari situ kita bisa mendisplay hasil filter paket dengan protokol tcp yang menuju port 80. Dengan penanda 'dst' sebagai destination yang berarti tujuan.

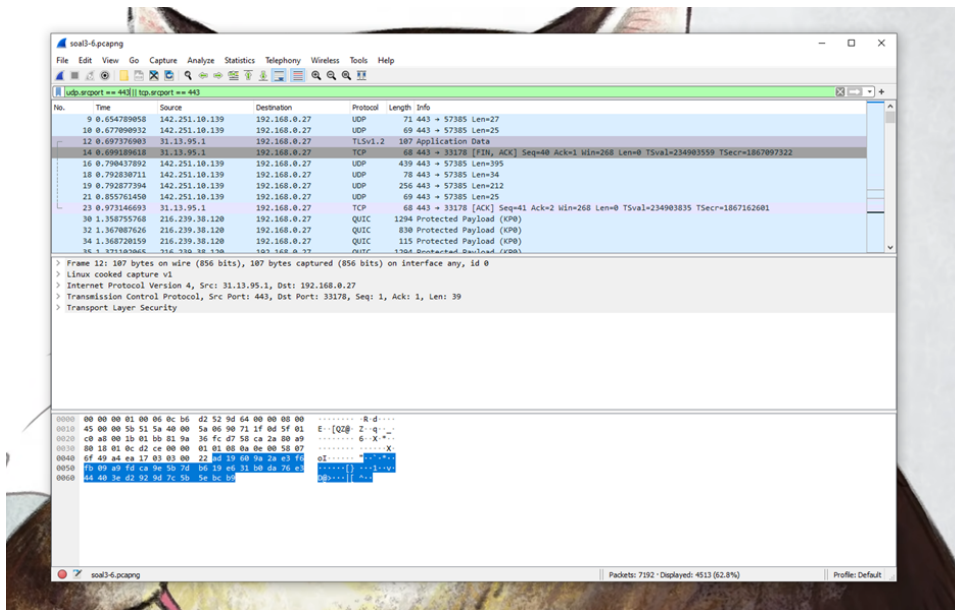


Kelompok ITA10
Hafizh Abid Wibowo 5027201011
Muhammad Farrel Abdillah 5027201057

4. Menggunakan tcp.srcport == 21. berbeda dengan nomor 3, 'src' mengambil dari source dari port tertentu.



5. Menggunakan udp.srcport == 443 dan tcp.srcport == 443, disini saya menggunakan kedua jenis protocol karena terdapat 2 jenis protocol yang tersedia dari source port yang sama yaitu 443.

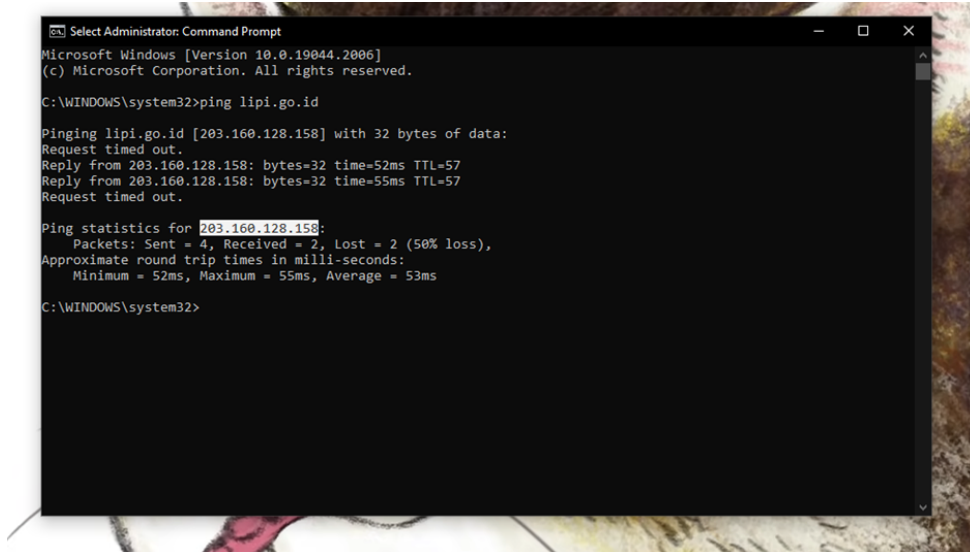


Kelompok ITA10

Hafizh Abid Wibowo 5027201011

Muhammad Farrel Abdillah 5027201057

- Untuk mencari ip dari lipi.go.id dibutuhkan untuk melakukan ping pada command prompt dengan "ping <nama domain>". Dibutuhkan beberapa saat dalam melakukan ping dan bahkan bisa timed out.



```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.19044.2006]
(c) Microsoft Corporation. All rights reserved.

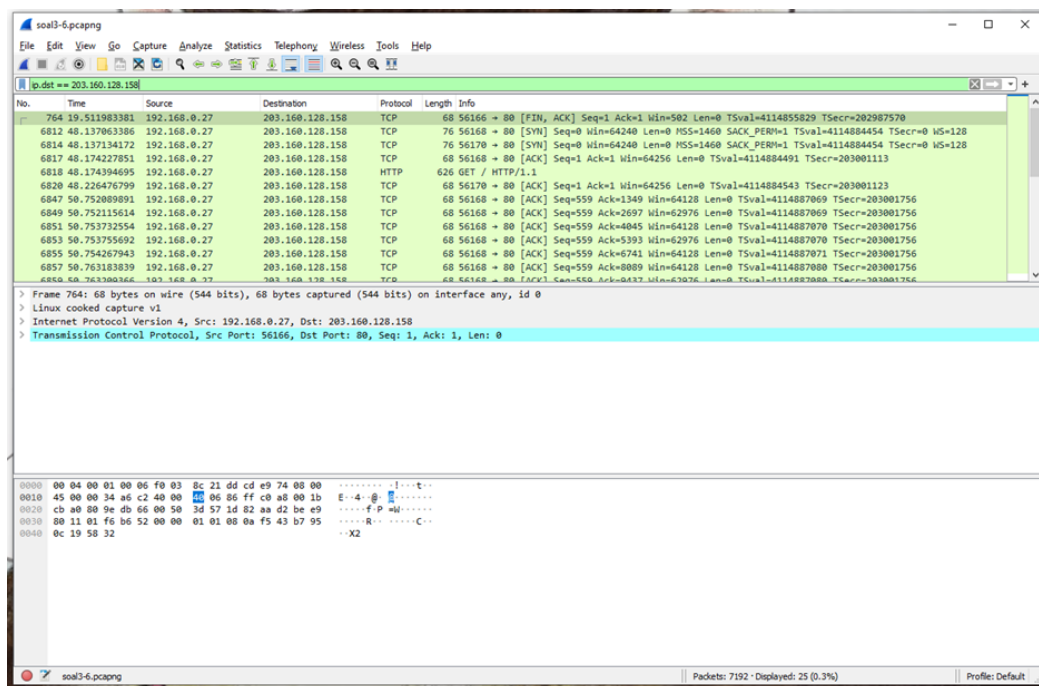
C:\WINDOWS\system32>ping lipi.go.id

Pinging lipi.go.id [203.160.128.158] with 32 bytes of data:
Request timed out.
Reply from 203.160.128.158: bytes=32 time=52ms TTL=57
Reply from 203.160.128.158: bytes=32 time=55ms TTL=57
Request timed out.

Ping statistics for 203.160.128.158:
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 52ms, Maximum = 55ms, Average = 53ms

C:\WINDOWS\system32>
```

Setelah itu, untuk mendisplay packet yang menuju lipi.go.id dapat dilakukan: ip.dst == 203.160.128.158 yang berarti display paket menuju ke ip tersebut, yaitu ip milik lipi.go.id

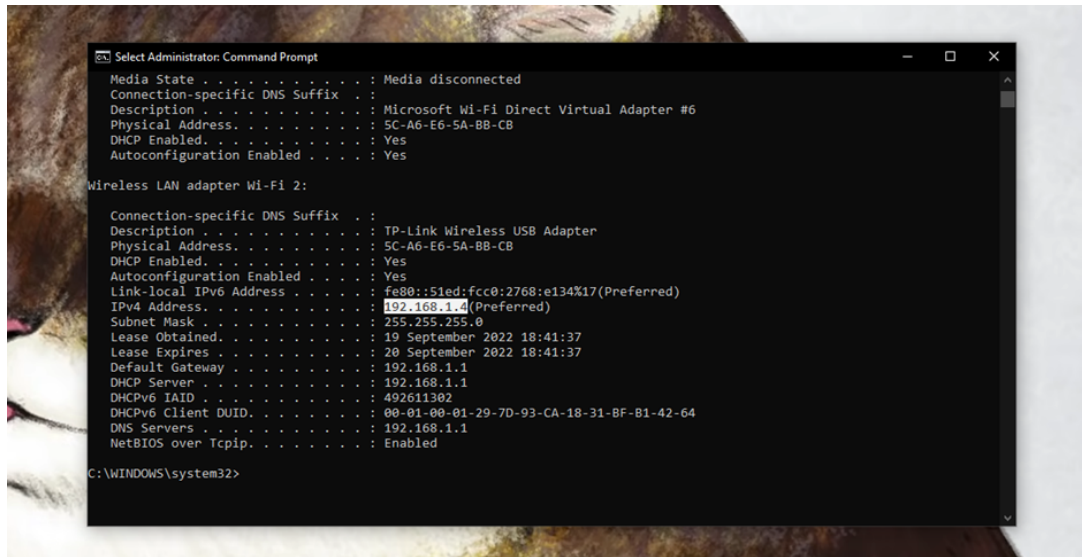


Kelompok ITA10

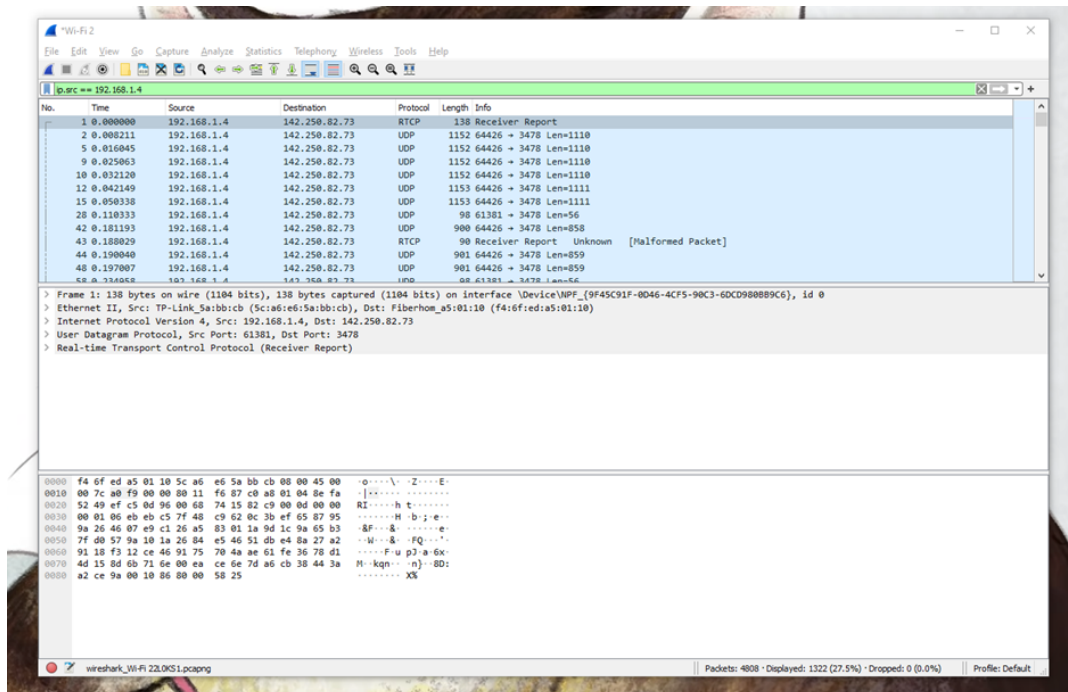
Hafizh Abid Wibowo 5027201011

Muhammad Farrel Abdillah 5027201057

- Untuk mencari ip sendiri dapat dilihat dengan menggunakan ipconfig pada command prompt dan mencari IPv4 Address pada wifi, disini saya telah menemukan bahwa ip dari wifi saya adalah 192.168.1.4

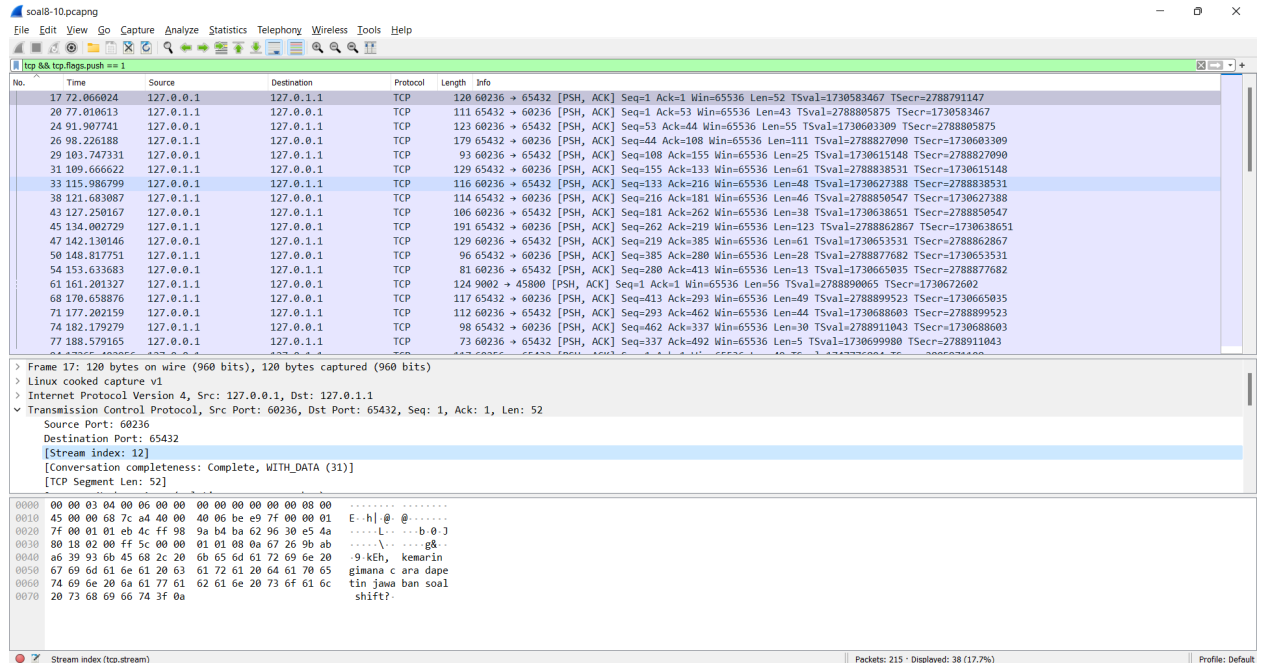


Setelah itu untuk mengambil paket dari ip sendiri, dapat membuka wireshark Wi-Fi 2 dan langsung menggunakan ip.src == 192.168.1.4

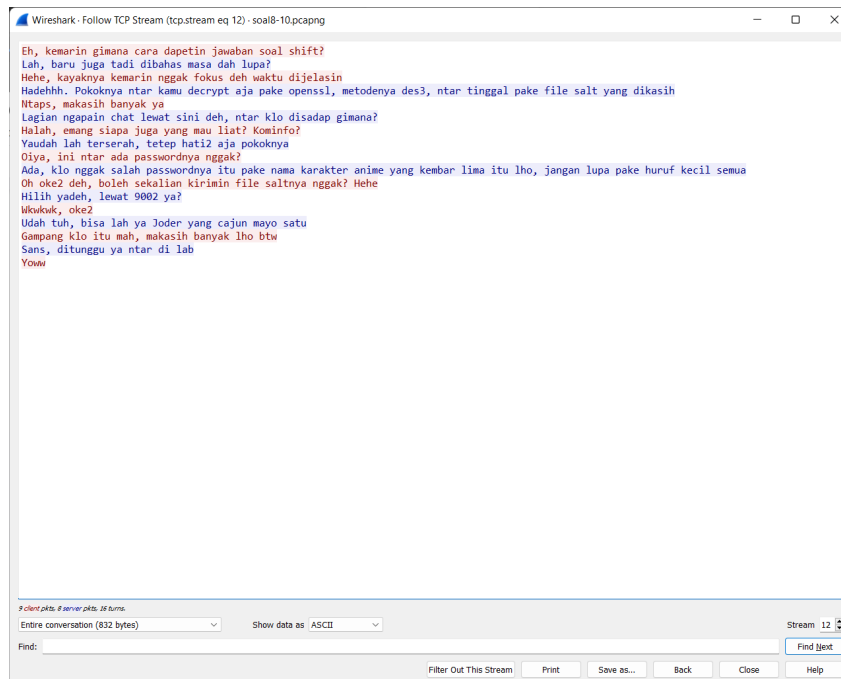


Kelompok ITA10
Hafizh Abid Wibowo 5027201011
Muhammad Farrel Abdillah 5027201057

8. Pertama-tama melakukan analisis paket dan protokol yang digunakan pada resource file, kemudian didapati informasi bahwa chat berlangsung pada protokol tcp dan flags [PSH, ACK]. Kemudian dilakukan filtering tcp && tcp.flags.push == 1



Kemudian didapatkan stream index: 12. Kemudian dilakukan follow tcp stream yang stream indexnya 12.



9. Didapatkan indikasi bahwa pertukaran file diadakan di TCP port 9002, dilakukan filtering tcp.port == 9002 dan didapatkan display berikut

Kelompok ITA10
Hafizh Abid Wibowo 5027201011
Muhammad Farrel Abdillah 5027201057

soal8-10.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 9002

No.	Time	Source	Destination	Protocol	Length	Info
58	161.200519	127.0.0.1	127.0.0.1	TCP	76	45800 → 9002 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1730672602 TSecr=0 WS=128
59	161.201018	127.0.0.1	127.0.0.1	TCP	76	9002 → 45800 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=2788890065 TSecr=1730672602 WS=128
60	161.201033	127.0.0.1	127.0.0.1	TCP	68	45800 → 9002 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1730672602 TSecr=2788890065
61	161.201327	127.0.0.1	127.0.0.1	TCP	124	9002 → 45800 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=56 TSval=2788890065 TSecr=1730672602
62	161.201358	127.0.0.1	127.0.0.1	TCP	68	45800 → 9002 [ACK] Seq=1 Ack=57 Win=65536 Len=0 TSval=1730672602 TSecr=2788890065
63	161.201380	127.0.0.1	127.0.0.1	TCP	68	9002 → 45800 [FIN, ACK] Seq=57 Ack=1 Win=65536 Len=0 TSval=2788890065 TSecr=1730672602
64	161.201438	127.0.0.1	127.0.0.1	TCP	68	45800 → 9002 [FIN, ACK] Seq=1 Ack=58 Win=65536 Len=0 TSval=1730672603 TSecr=2788890065
65	161.201448	127.0.0.1	127.0.0.1	TCP	68	9002 → 45800 [ACK] Seq=58 Ack=2 Win=65536 Len=0 TSval=2788890066 TSecr=1730672603
200	18511.728346	127.0.0.1	127.0.0.1	TCP	76	45822 → 9002 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1749023129 TSecr=0 WS=128
201	18511.728442	127.0.0.1	127.0.0.1	TCP	76	9002 → 45822 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=2807240593 TSecr=1749023129 WS=128
202	18511.728467	127.0.0.1	127.0.0.1	TCP	68	45822 → 9002 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=1749023130 TSecr=2807240593
203	18511.728647	127.0.0.1	127.0.0.1	TCP	124	9002 → 45822 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=56 TSval=2807240593 TSecr=1749023130
204	18511.728667	127.0.0.1	127.0.0.1	TCP	68	45822 → 9002 [ACK] Seq=1 Ack=57 Win=65536 Len=0 TSval=1749023130 TSecr=2807240593
205	18511.728681	127.0.0.1	127.0.0.1	TCP	68	9002 → 45822 [FIN, ACK] Seq=57 Ack=1 Win=65536 Len=0 TSval=2807240593 TSecr=1749023130
206	18511.728779	127.0.0.1	127.0.0.1	TCP	68	45822 → 9002 [FIN, ACK] Seq=1 Ack=58 Win=65536 Len=0 TSval=1749023130 TSecr=2807240593
207	18511.728784	127.0.0.1	127.0.0.1	TCP	68	9002 → 45822 [ACK] Seq=58 Ack=2 Win=65536 Len=0 TSval=2807240593 TSecr=1749023130
208	18640.272718	127.0.0.1	127.0.0.1	TCP	76	45824 → 9002 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=1749151674 TSecr=0 WS=128
209	18640.272738	127.0.0.1	127.0.0.1	TCP	76	9002 → 45824 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=2807369137 TSecr=1749151674 WS=128

> Frame 61: 124 bytes on wire (992 bits), 124 bytes captured (992 bits)

> Linux cooked capture v1

> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

> Transmission Control Protocol, Src Port: 9002, Dst Port: 45800, Seq: 1, Ack: 1, Len: 56

Source Port: 9002

Destination Port: 45800

[Stream Index: 29]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 56]

0000 00 00 03 04 00 06 00 00 00 00 00 00 00 00 00
0010 45 00 00 0c 33 fb 40 00 40 06 07 8f 7f 00 01 01 E..13 @
0020 7f 00 00 01 23 2a b2 e8 67 22 5f 92 45 87 98 6b ...B*...E..k
0030 80 18 02 00 ff 60 00 00 01 01 08 0a a6 3b 15 d1
0040 67 27 f7 da 53 61 6c 7a 65 64 5f 5f bf 3a df af g..Salt.ed....
0050 a4 88 42 28 ce 05 1b d1 f6 c1 24 45 a4 16 e8 4b ..B(....\$E...K
0060 29 c1 d6 3c 08 1b 8b b9 fc f5 66 20 95 87 96)...<....f...
0070 13 17 e1 42 ff 47 3d e4 da 26 cb cf ...B-G...+..

Bytes 68-123: Data (data.data) Packets: 215 · Displayed: 24 (11.2%) Profile: Default

Kemudian dilakukan tcp follow stream untuk mengesave file as raw

Wireshark · Follow TCP Stream (tcp.stream eq 29) · soal8-10.pcapng

53616c7465645f5fbf3adafafa4884228ce051bd1f6c12445a416e84b29c1d63c3c081b8bb9fcf566209587961317e142ff4734e4da2bcbcf

0 client pkts, 1 server pkts, 0 bytes.

Entire conversation (56 bytes) Show data as Raw Stream 29

Find: Find Next

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

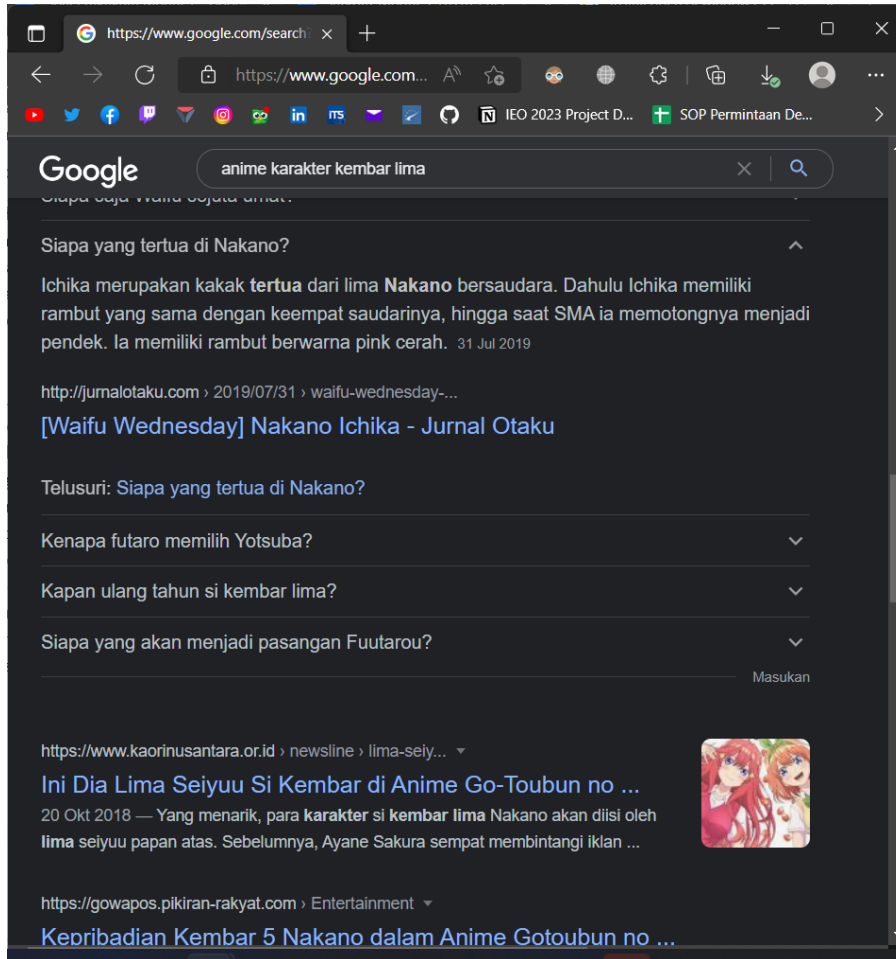
Kelompok ITA10

Hafizh Abid Wibowo 5027201011

Muhammad Farrel Abdillah 5027201057

10. Dengan menggunakan openssl, dapat dimasukkan password lalu akan muncul flag yang tersedia pada file yang telah disave.

Password ditemukan dengan social engineering:



Flag akan segera terlihat setelah memasukkan password, Flagnya adalah JaRkOm2022{8uK4N_CtF_K0k_h3h3h3}

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22000.978]
(c) Microsoft Corporation. All rights reserved.

C:\Users\hfzh\Downloads>openssl des3 -d -in ITA10.des3 -out flag.txt -k nakano
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.

C:\Users\hfzh\Downloads>cat flag.txt
JaRkOm2022{8uK4N_CtF_K0k_h3h3h3}
C:\Users\hfzh\Downloads>
```


Kelompok ITA10

Hafizh Abid Wibowo 5027201011

Muhammad Farrel Abdillah 5027201057

KESULITAN YANG DIALAMI:

- Kesulitan mencari command yang tepat pada wireshark untuk membedakan paket yang menuju dari - dan paket yang datang dari -. Kesulitan dapat diatasi dengan searching.
- Kesulitan mencari password untuk membuka flag