

Jarkom E07
Modul 1

Arya Nur Razzaq	5025201102
Florentino Benedictus	5025201222
Muhammad Zufarriqi Prakoso	5025201276



1. http.host == monta.if.its.ac.id

Follow tcp stream

Web Servernya adalah [nginx/1.10.3](#)

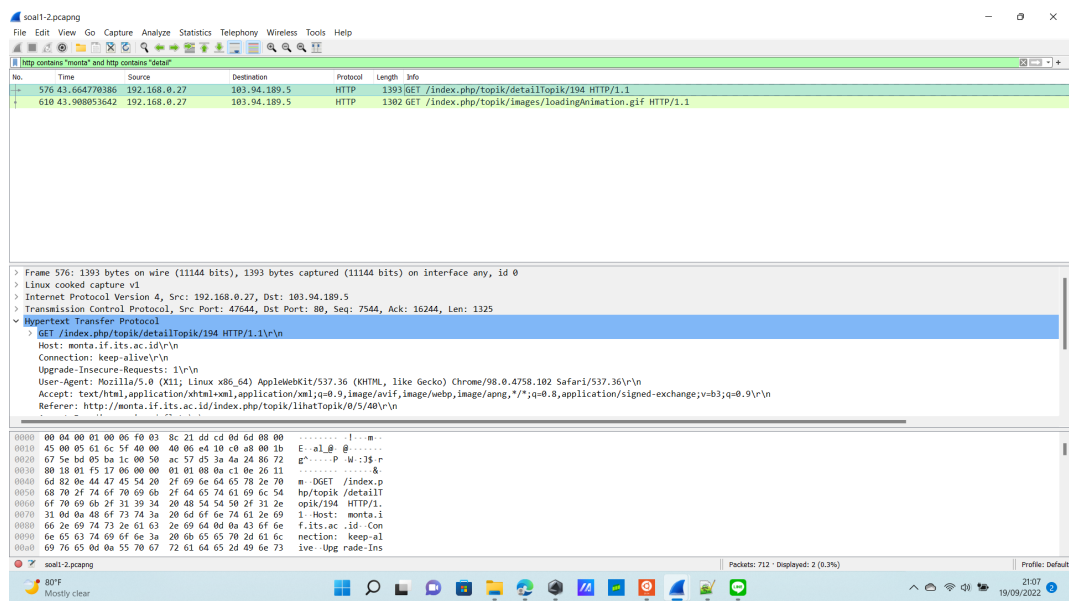
```
7TGd3C8jDDeqJNe8BKquiHEQo%2B36m8ssmCE%2BsK
VXfs5PtUN%2FWKMHXQqZP8F3PgRXW20R4a; _gat_gt

HTTP/1.1 200 OK
Server: nginx/1.10.3
Date: Sun, 18 Sep 2022 13:34:57 GMT
Content-Type: image/png
Content-Length: 939
Connection: keep-alive
Last-Modified: Sat, 18 Oct 2014 16:36:16 GMT
ETag: "3ab-505b51493c000"
Accept-Ranges: bytes

.PNG
*
***
```

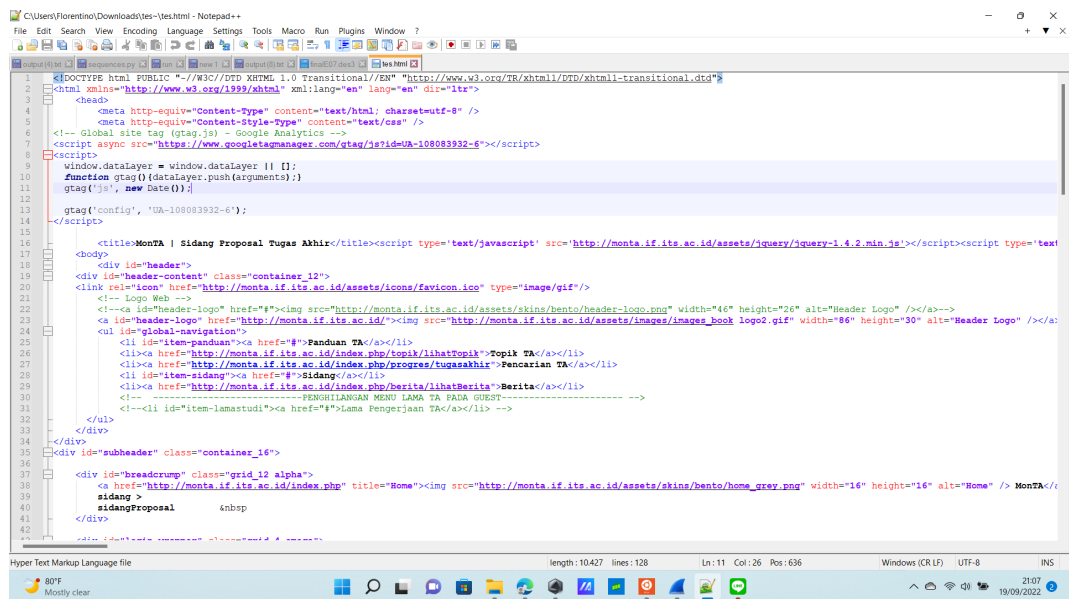
2. http.host == "monta.if.its.ac.id"

Judul TANYA adalah Perancangan Sistem Pengendali Panas Otomatis pada Mesin Sangrai Kopi dengan Logika Fuzzy



Follow tcp->save raw as .zip

Waktu unzip ada file tidak berextension tapi formatnya html



3. tcp.dstport eq 80

```
soal3-6.pcapng
tcp.dstport eq 80
No.    Time           Source            Destination       Protocol Length Info
275    7.142658322    192.168.0.27      192.124.249.36    TCP           68 50016 → 80 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=550146835 TSecr=
764    19.511983381    192.168.0.27      203.160.128.158   TCP           68 56166 → 80 [FIN, ACK] Seq=1 Ack=1 Win=502 Len=0 TSval=4114855829 TSecr=
6812   48.137063386    192.168.0.27      203.160.128.158   TCP           76 56168 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4114855829 TSecr=
6814   48.137134172    192.168.0.27      203.160.128.158   TCP           76 56170 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4114855829 TSecr=
6817   48.174227851    192.168.0.27      203.160.128.158   TCP           68 56168 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4114884491 TSecr=
6818   48.174394695    192.168.0.27      203.160.128.158   HTTP          626 GET / HTTP/1.1
6820   48.226476799    192.168.0.27      203.160.128.158   TCP           68 56170 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4114884543 TSecr=
6847   50.752809891    192.168.0.27      203.160.128.158   TCP           68 56168 → 80 [ACK] Seq=559 Ack=1349 Win=64128 Len=0 TSval=4114887069 TSecr=
6849   50.752115614    192.168.0.27      203.160.128.158   TCP           68 56168 → 80 [ACK] Seq=559 Ack=2697 Win=62976 Len=0 TSval=4114887069 TSecr=
6851   50.753732554    192.168.0.27      203.160.128.158   TCP           68 56168 → 80 [ACK] Seq=559 Ack=4045 Win=64128 Len=0 TSval=4114887070 TSecr=
6853   50.753755692    192.168.0.27      203.160.128.158   TCP           68 56168 → 80 [ACK] Seq=559 Ack=5393 Win=62976 Len=0 TSval=4114887070 TSecr=

> Frame 275: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.0.27, Dst: 192.124.249.36
> Transmission Control Protocol, Src Port: 50016, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

0000  00 04 00 01 00 06 f0 03 8c 21 dd cd 00 00 08 00  .....!.....
0010  45 00 00 34 6c ac 40 00 40 06 53 b3 c0 a8 00 1b  E..4l@.@S.....
0020  c0 7c f9 24 c3 60 00 50 2e 62 7a 51 e9 87 7e 7a  .|.$.P.bzQ...z
0030  80 11 01 f5 8a d4 00 00 01 01 08 0a 20 ca 93 13  g.....
0040  cf 67 17 e2                                     g..
```

4. tcp.srcport eq 21

```
soal3-6.pcapng
tcp.srcport eq 21
No.    Time           Source            Destination       Protocol Length Info
6243   35.992838176    127.0.0.1         127.0.0.1         TCP           76 21 → 55824 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=4095422343 TSecr=
6247   35.993026054    172.17.0.2        172.17.0.1        TCP           76 21 → 47094 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=4095422343 TSecr=
6248   35.993026054    172.17.0.2        172.17.0.1        TCP           76 [TCP Out-Of-Order] 21 → 47094 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=4095422343 TSecr=
6251   36.022045700    172.17.0.2        172.17.0.1        FTP           88 Response: 220 (vsFTPd 3.0.3)
6252   36.022045700    172.17.0.2        172.17.0.1        TCP           88 [TCP Retransmission] 21 → 47094 [PSH, ACK] Seq=1 Ack=1 Win=65280 Len=0 MSS=1460 SACK_PERM=1 TSval=4095422343 TSecr=
6255   36.022125494    127.0.0.1         127.0.0.1         FTP           88 Response: 220 (vsFTPd 3.0.3)
6258   36.022267560    127.0.0.1         127.0.0.1         TCP           68 21 → 55824 [ACK] Seq=21 Ack=11 Win=65536 Len=0 TSval=4095422343 TSecr=
6261   36.022308877    172.17.0.2        172.17.0.1        TCP           68 21 → 47094 [ACK] Seq=21 Ack=11 Win=65280 Len=0 MSS=1460 SACK_PERM=1 TSval=4095422343 TSecr=
6262   36.022308877    172.17.0.2        172.17.0.1        TCP           68 [TCP Dup ACK 6261#1] 21 → 47094 [ACK] Seq=21 Ack=11 Win=65280 Len=0 MSS=1460 SACK_PERM=1 TSval=4095422343 TSecr=
6263   36.022374372    172.17.0.2        172.17.0.1        FTP           106 Response: 530 Please login with USER and PASS.
6264   36.022374372    172.17.0.2        172.17.0.1        TCP           106 [TCP Retransmission] 21 → 47094 [PSH, ACK] Seq=21 Ack=11 Win=65280 Len=0 MSS=1460 SACK_PERM=1 TSval=4095422343 TSecr=

> Frame 6243: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Transmission Control Protocol, Src Port: 21, Dst Port: 55824, Seq: 0, Ack: 1, Len: 0

0000  00 00 03 04 00 06 00 00 00 00 00 00 d2 07 08 00  .....
0010  45 00 00 3c 00 00 40 00 40 06 3c ba 7f 00 00 01  E..<.@.@.....
0020  7f 00 00 01 00 15 da 10 9f c0 92 60 7a a8 6e 4a  .f.....z.nJ
0030  a0 12 ff cb fe 30 00 00 02 04 ff d7 04 02 08 0a  ..0.....
0040  f4 1b 2f 69 f4 1b 2f 69 01 03 03 07             ..i./i.....
```

5.tcp.srcport eq 443

No.	Time	Source	Destination	Protocol	Length	Info
12	0.697376903	31.13.95.1	192.168.0.27	TLSv1...	107	Application Data
14	0.699189618	31.13.95.1	192.168.0.27	TCP	68	443 → 33178 [FIN, ACK] Seq=40 Ack=1 Win=268 Len=0 TSval=234903559 TS...
23	0.973146693	31.13.95.1	192.168.0.27	TCP	68	443 → 33178 [ACK] Seq=41 Ack=2 Win=268 Len=0 TSval=234903835 TSecr=1...
222	5.056718032	34.132.134.162	192.168.0.27	TCP	68	443 → 46652 [ACK] Seq=1 Ack=1 Win=334 Len=0 TSval=1614814641 TSecr=2...
288	7.237319427	13.229.195.192	192.168.0.27	TCP	68	443 → 53832 [ACK] Seq=1 Ack=2 Win=110 Len=0 TSval=3673164913 TSecr=2...
292	7.239180676	35.190.60.146	192.168.0.27	TCP	68	443 → 58644 [FIN, ACK] Seq=1 Ack=2 Win=261 Len=0 TSval=4086246065 TS...
315	7.407835167	93.184.216.34	192.168.0.27	TCP	76	443 → 50618 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PER...
318	7.462969109	169.47.124.22	192.168.0.27	TCP	68	443 → 51820 [ACK] Seq=1 Ack=2 Win=243 Len=0 TSval=511043283 TSecr=23...
322	7.653025852	93.184.216.34	192.168.0.27	TCP	68	443 → 50618 [ACK] Seq=1 Ack=581 Win=67072 Len=0 TSval=2827756319 TSe...
323	7.654970547	93.184.216.34	192.168.0.27	TLSv1...	167	Hello Retry Request, Change Cipher Spec
335	7.919974400	93.184.216.34	192.168.0.27	TCP	68	443 → 50618 [ACK] Seq=100 Ack=1195 Win=68096 Len=0 TSval=2827756588...

> Frame 222: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0

> Linux cooked capture v1

> Internet Protocol Version 4, Src: 34.132.134.162, Dst: 192.168.0.27

> Transmission Control Protocol, Src Port: 443, Dst Port: 46652, Seq: 1, Ack: 1, Len: 0

```

0000  00 00 00 01 00 06 0c b6 d2 52 9d 64 00 00 08 00  ..... R d ....
0010  45 00 00 34 53 df 40 00 3b 06 81 fb 22 84 86 a2  E..4S.@;.....
0020  c0 a8 00 1b 01 bb b6 3c 7c 94 ee d4 ba 06 cd eb  .....<|.....
0030  80 10 01 4e b3 3e 00 00 01 01 08 0a 60 40 1d b1  ...N>.....@..
0040  5c c8 d2 39  \..9

```

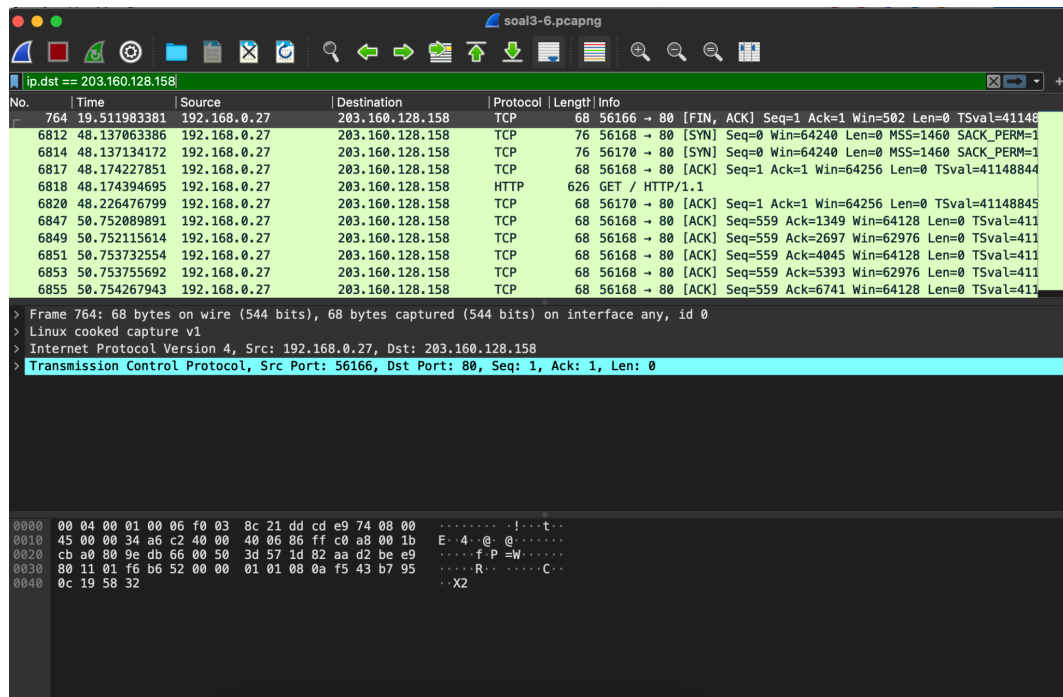
6. ping lipi.go.id->

Pinging lipi.go.id [203.160.128.158] with 32 bytes of data:
 Reply from 203.160.128.158: bytes=32 time=103ms TTL=57
 Reply from 203.160.128.158: bytes=32 time=114ms TTL=57
 Reply from 203.160.128.158: bytes=32 time=115ms TTL=57
 Reply from 203.160.128.158: bytes=32 time=119ms TTL=57

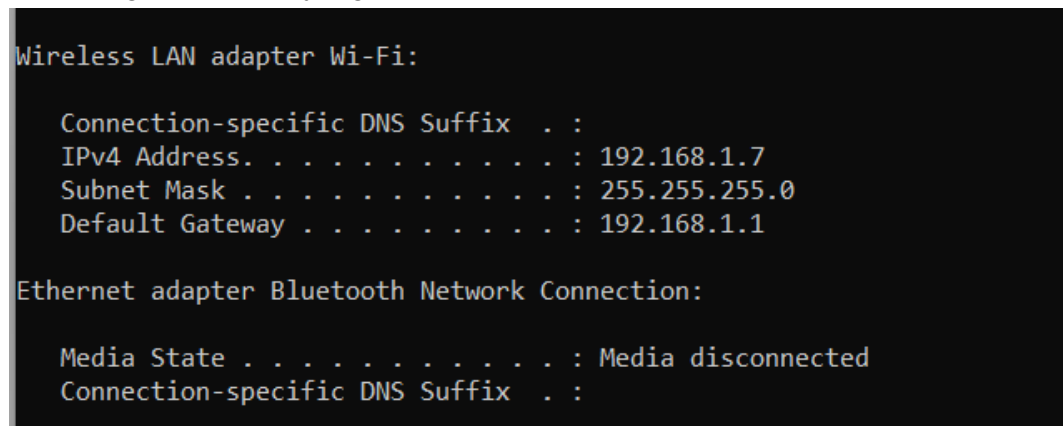
Ping statistics for 203.160.128.158:
 Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
 Approximate round trip times in milli-seconds:
 Minimum = 103ms, Maximum = 119ms, Average = 112ms

Didapat ping lipi

ip.dst == 203.160.128.158



7. Ipconfig->didapat ip yang dimiliki



src host 192.168.1.7

No.	Time	Source	Destination	Protocol	Length	Info
150	11.984473	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=331 Ack=331 Win=511 Len=0
980	16.874320	192.168.1.7	192.168.1.6	TCP	164	55829 → 8009 [PSH, ACK] Seq=331 Ack=331 Win=511 Len=110 [TCP segment of a reassembled PDU]
913	17.845557	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=441 Ack=441 Win=511 Len=0
1253	22.805268	192.168.1.7	192.168.1.6	TCP	164	55829 → 8009 [PSH, ACK] Seq=441 Ack=441 Win=511 Len=110 [TCP segment of a reassembled PDU]
1255	22.852293	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=551 Ack=551 Win=510 Len=0
1386	27.018580	192.168.1.7	192.168.1.6	TCP	164	55829 → 8009 [PSH, ACK] Seq=551 Ack=551 Win=510 Len=110 [TCP segment of a reassembled PDU]
1389	27.065406	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=661 Ack=661 Win=510 Len=0
2678	32.838405	192.168.1.7	192.168.1.6	TCP	164	55829 → 8009 [PSH, ACK] Seq=661 Ack=661 Win=510 Len=110 [TCP segment of a reassembled PDU]
2681	32.127549	192.168.1.7	192.168.1.6	APPL	164	APPL Error! [TCP segment of a reassembled PDU]
2684	32.151865	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=881 Ack=881 Win=509 Len=0
3853	37.141742	192.168.1.7	192.168.1.6	TCP	164	55829 → 8009 [PSH, ACK] Seq=881 Ack=881 Win=509 Len=110 [TCP segment of a reassembled PDU]
3855	37.187481	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=991 Ack=991 Win=508 Len=0
3977	42.160538	192.168.1.7	192.168.1.6	TCP	164	55829 → 8009 [PSH, ACK] Seq=991 Ack=991 Win=508 Len=110 [TCP segment of a reassembled PDU]
3979	42.207534	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=1101 Ack=1101 Win=508 Len=0
4087	47.167040	192.168.1.7	192.168.1.6	TCP	164	55829 → 8009 [PSH, ACK] Seq=1101 Ack=1101 Win=508 Len=110 [TCP segment of a reassembled PDU]
4010	47.242746	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=1211 Ack=1211 Win=508 Len=0
4062	52.203696	192.168.1.7	192.168.1.6	TCP	164	55829 → 8009 [PSH, ACK] Seq=1211 Ack=1211 Win=508 Len=110 [TCP segment of a reassembled PDU]
4065	52.250480	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=1321 Ack=1321 Win=507 Len=0
4114	57.215201	192.168.1.7	192.168.1.6	TCP	164	55829 → 8009 [PSH, ACK] Seq=1321 Ack=1321 Win=507 Len=110 [TCP segment of a reassembled PDU]
4117	57.259871	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=1431 Ack=1431 Win=513 Len=0
4153	62.230043	192.168.1.7	192.168.1.6	TCP	164	55829 → 8009 [PSH, ACK] Seq=1431 Ack=1431 Win=513 Len=110 [TCP segment of a reassembled PDU]
4156	62.305811	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=1541 Ack=1541 Win=512 Len=0
4270	67.269550	192.168.1.7	192.168.1.6	TCP	164	55829 → 8009 [PSH, ACK] Seq=1541 Ack=1541 Win=512 Len=110 [TCP segment of a reassembled PDU]
4276	67.422169	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=1651 Ack=1651 Win=512 Len=0
4286	72.388635	192.168.1.7	192.168.1.6	TCP	164	55829 → 8009 [PSH, ACK] Seq=1651 Ack=1651 Win=512 Len=110 [TCP segment of a reassembled PDU]
4288	72.433375	192.168.1.7	192.168.1.6	TCP	54	55829 → 8009 [ACK] Seq=1761 Ack=1761 Win=511 Len=0

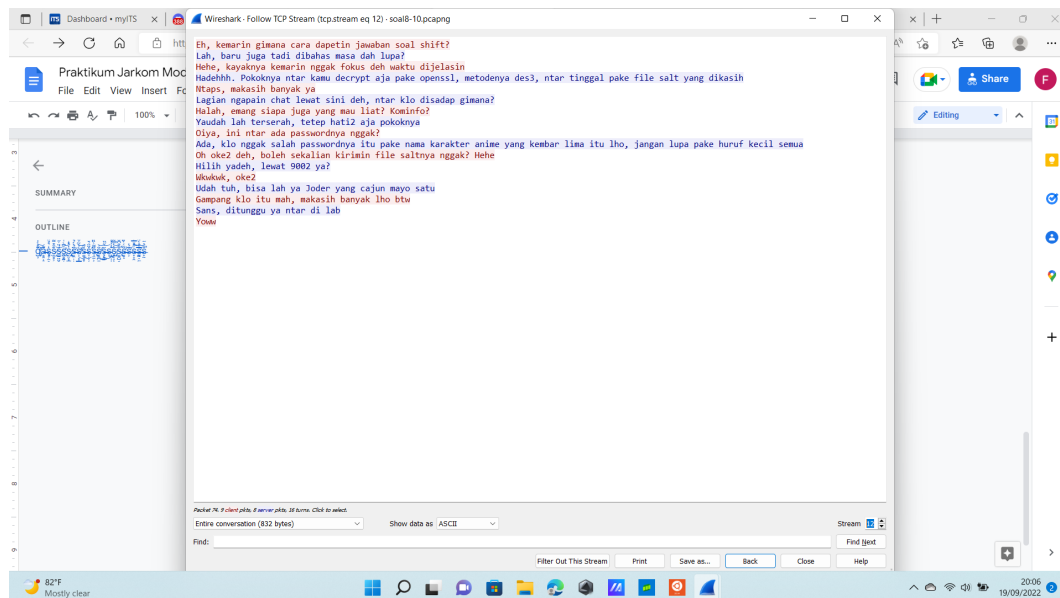
Frame 180: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface \Device\NPF...{4F248928-1ADC-419D-B0FE-CD486172A48D}, id 0
Ethernet II, Src: IntelCor_B81561a8 (c8:e2:65:88:15:61a8), Dst: Vizio_2d:85:cc (08:bd:3e:2d:85:cc)
Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.1.6
Transmission Control Protocol, Src Port: 55829, Dst Port: 8009, Seq: 1, Ack: 1, Len: 110

```

0000  00 bd 3e 2d 85 cc c8 e2 65 88 56 a8 08 00 45 00
0010  00 96 48 24 40 00 00 06 00 00 c0 a8 01 07 c0 a8
0020  01 86 da 15 1f 49 c5 27 50 3a 00 6a c8 17 50 19
0030  02 00 83 ec 00 00 17 03 03 00 69 2e 42 b1 58 1b
0040  f1 48 ac 49 00 87 5e 3b 7a 07 b7 e2 d1 3a 78 2e
0050  8a a5 a2 7a 4b 6c 30 28 c4 02 24 51 de 5a 87 03
0060  79 d1 eb e4 f6 43 0f 4c b0 0b 77 f1 57 0f c3 7e
0070  bd 97 37 00 17 e5 5d a4 7f 02 50 5f 08 19 74 32
0080  8e 6a 9e 7f a6 f0 00 b2 19 38 50 a4 30 4e 93 2c
0090  db 84 90 c2 9d 2f b0 1a e9 88 f3 c2 99 ed fd bf
00a0  15 db 97 e1

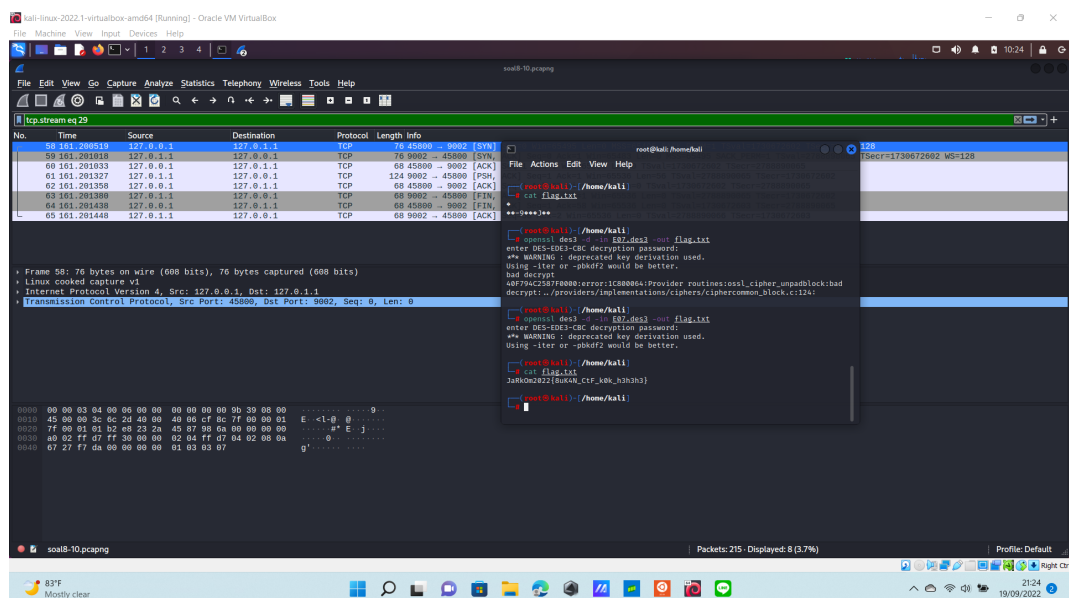
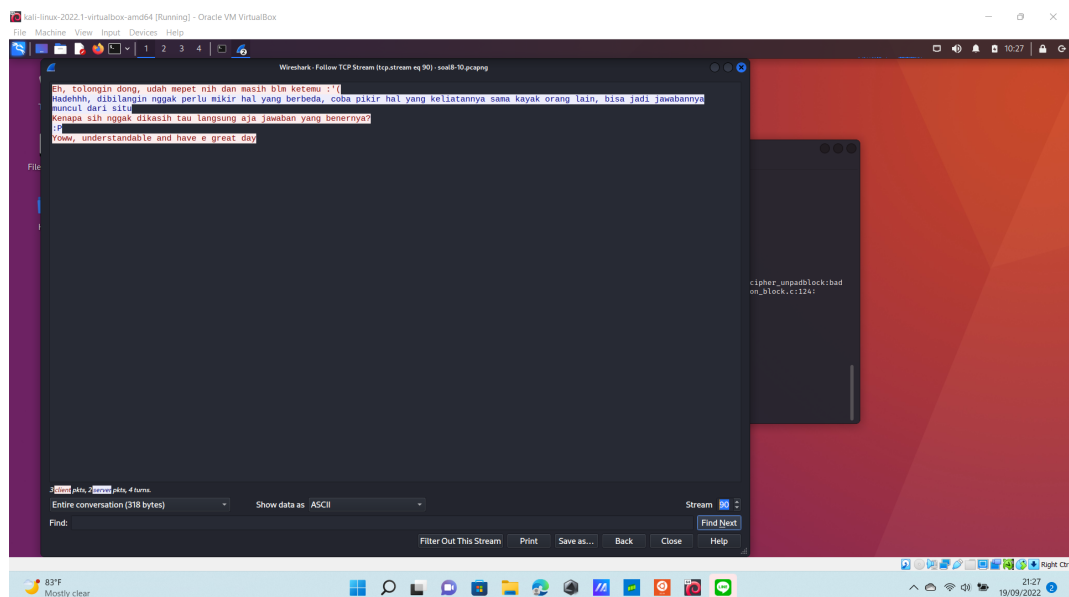
```

8-10.



Pertama-tama tcp stream paket, lalu ganti angka stream pada kanan bawah ternyata banyak pesan, lalu ada paket yang memberi pesan enkripsinya (stream 12)des3 dan pakai salted, lalu setelah streamnya dinaikkan, ada file salted, tapi harus di save as raw karena jika ascii akan ada data yang hilang, lalu 9002 juga setelah dicari di google ternyata TCP/UDP (jawaban no. 8, protokol yang digunakan), save data salted sebagai E07.des3 (jawaban no.9 part 1)

Lalu untuk command opensslnya kelompok kami menggunakan `openssl des3 -d -in E07.des3 -out flag.txt` (output flag.txt sebagai jawaban no.9 part 2, referensinya [Encrypt & Decrypt Files from the Command Line with OpenSSL \(osxdaily.com\)](#))
Ternyata diminta password, setelah dicari di internet tentang karakter kembar 5 ditemukan https://myanimelist.net/anime/38101/5-Toubun_no_Hanayome/



Akhirnya didapat flag.txt yang berisi
JaRkOm2022{8uK4N_CtF_k0k_h3h3h3} (jawaban no. 10)