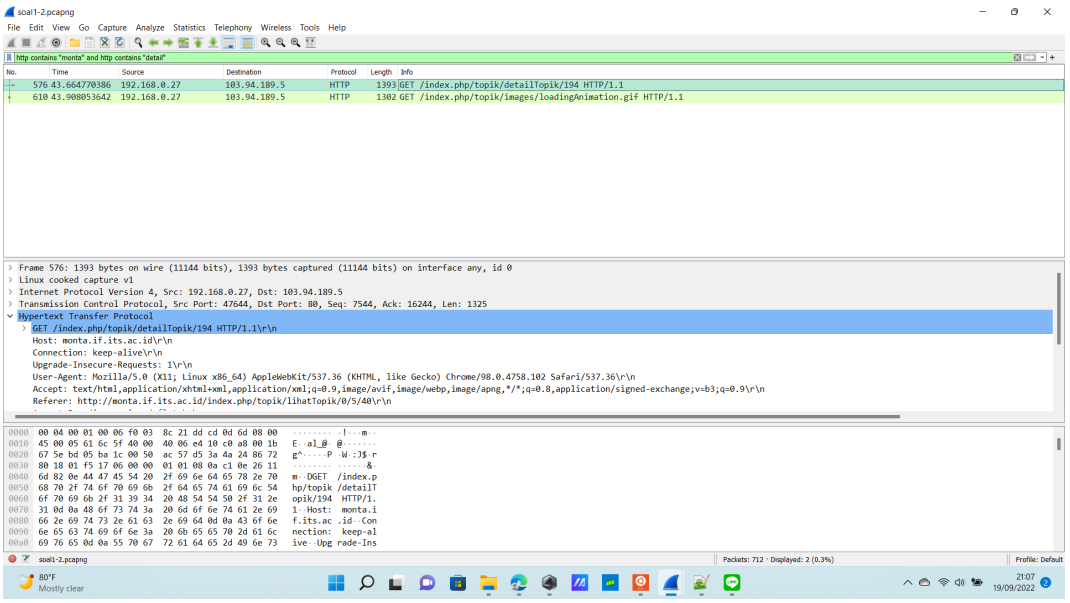
Jarkom E07
Modul 1

Arya Nur Razzaq	5025201102
Florentino Benedictus	5025201222
Muhammad Zufarrifqi Prakoso	5025201276

1.http.host == monta.if.its.ac.id
Follow tcp stream
Web Servernya adalah nginx/1.10.3

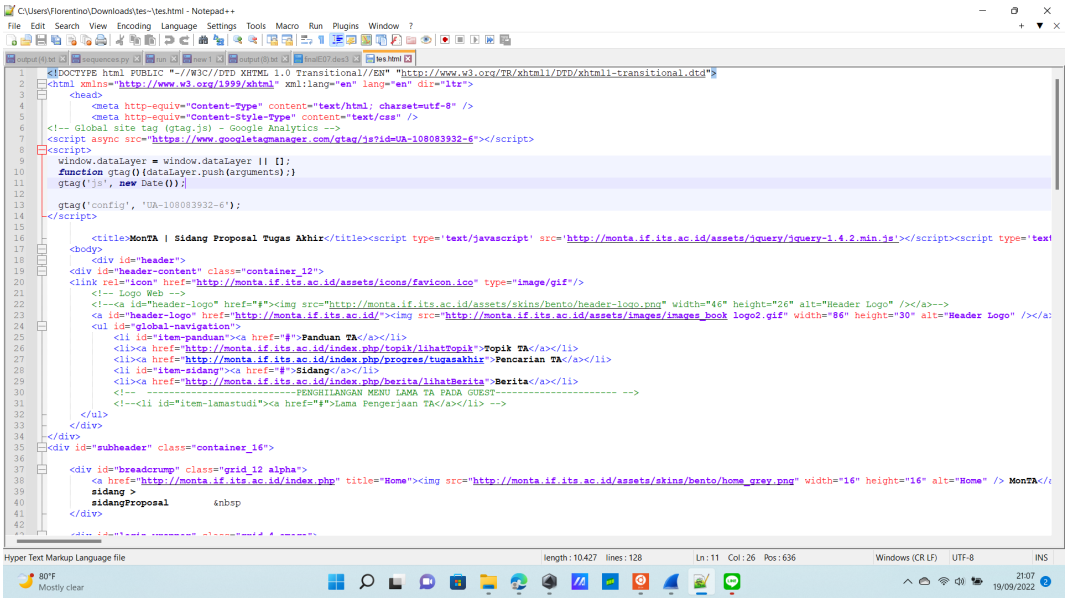
```
7TGd3C8jDDeqJNe8BKquiHEQo%2B36m8ssmCE%2BsK
VXfs5PtuN%2FWKMhXQqZP8F3PgRXW20R4a; _gat_gt

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
.
...
```

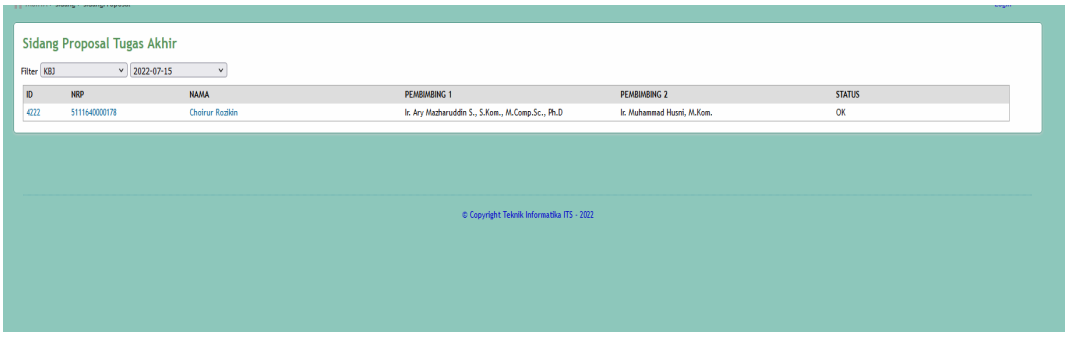
2. http.host == "monta.if.its.ac.id"
Judul TAnya adalah Perancangan Sistem Pengendali Panas Otomatis pada Mesin Sangrai Kopi dengan Logika Fuzzy



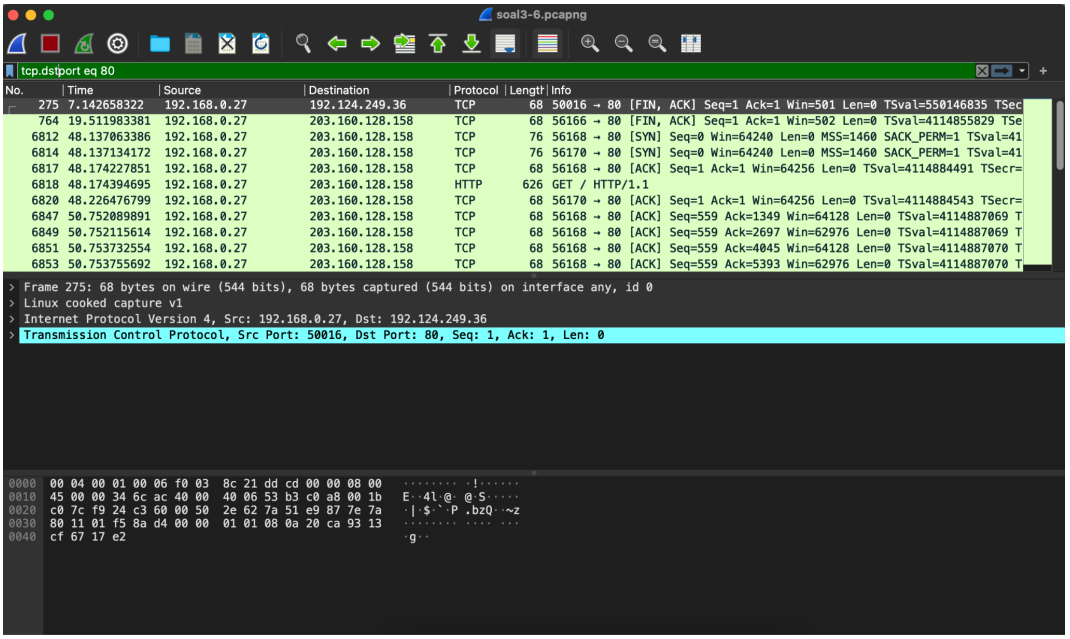
Follow tcp->save raw as .zip

Waktu unzip ada file tidak berextension tapi formatnya html

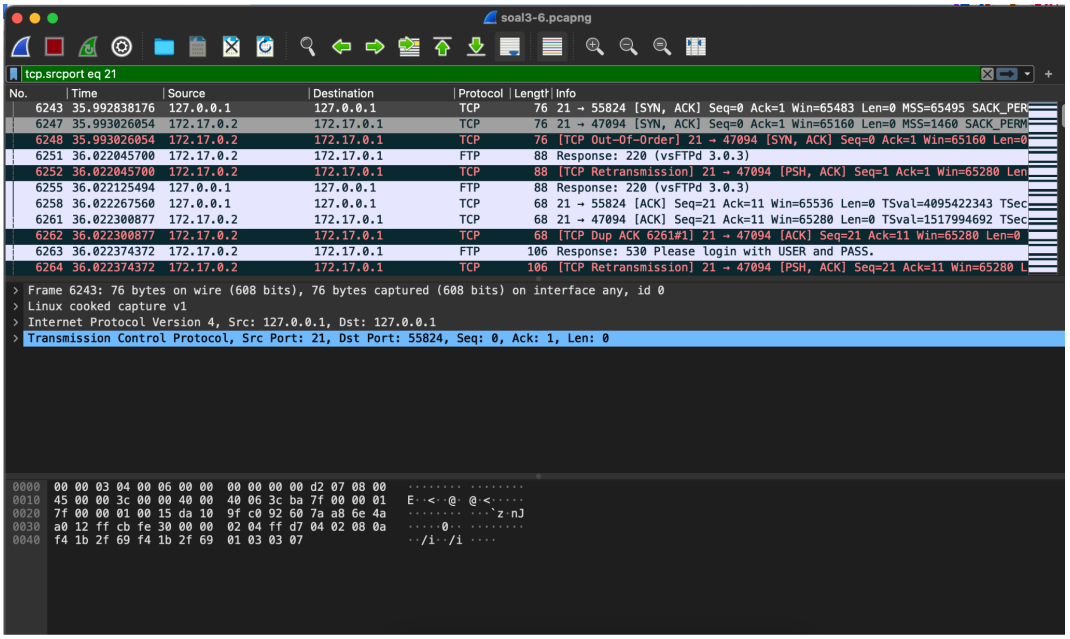




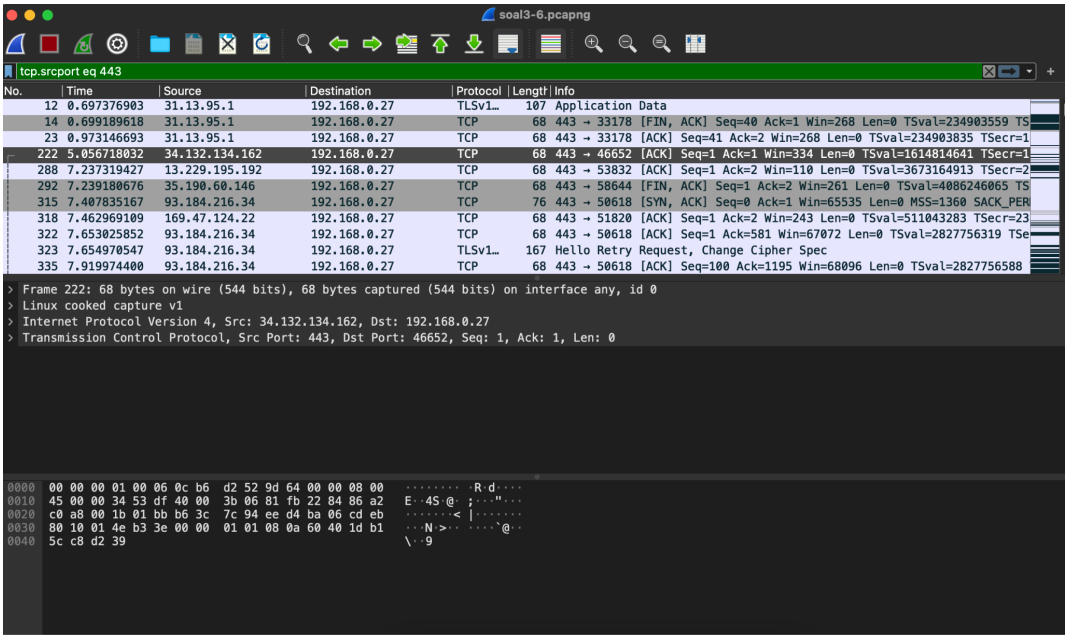
3. tcp.dstport eq 80



4.tcp.srcport eq 21



5.tcp.srcport eq 443



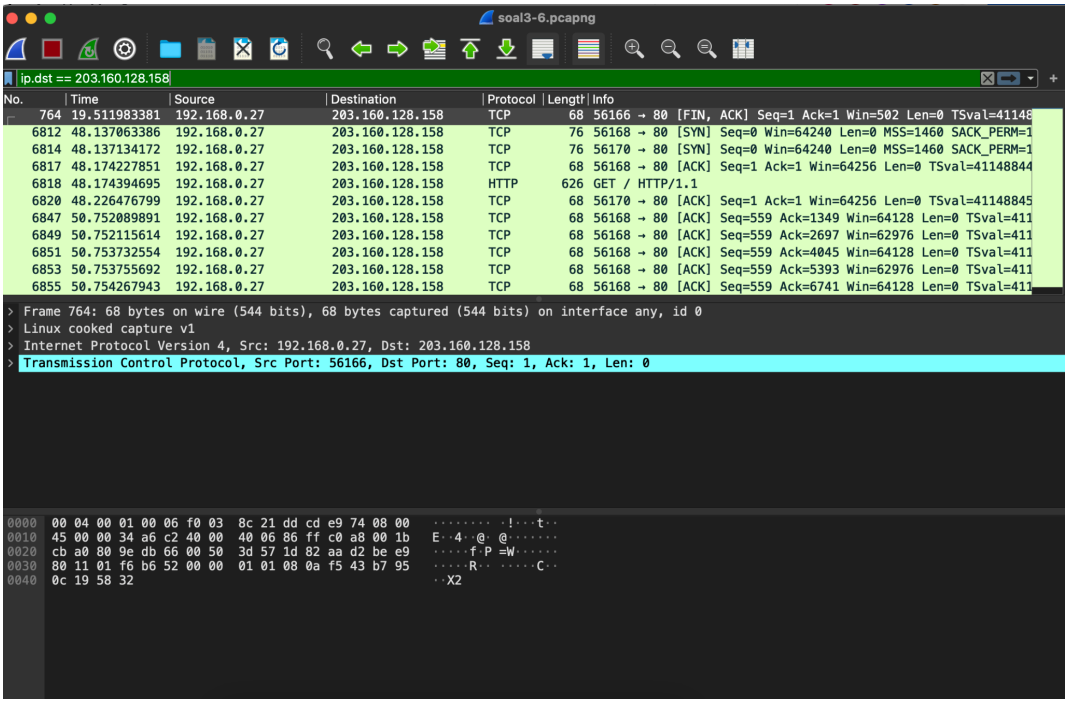
6. ping lipi.go.id->

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

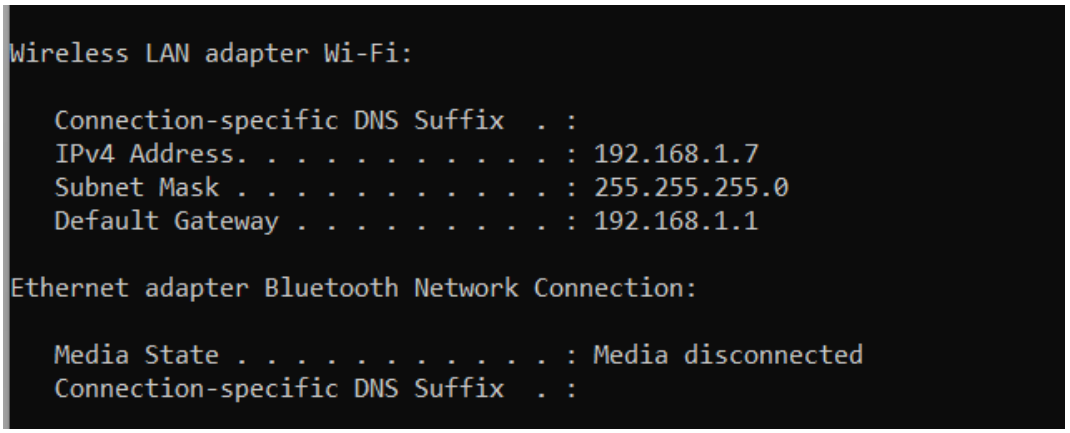
Ping statistics for 203.160.128.158:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 103ms, Maximum = 119ms, Average = 112ms

Didapat ping lipi

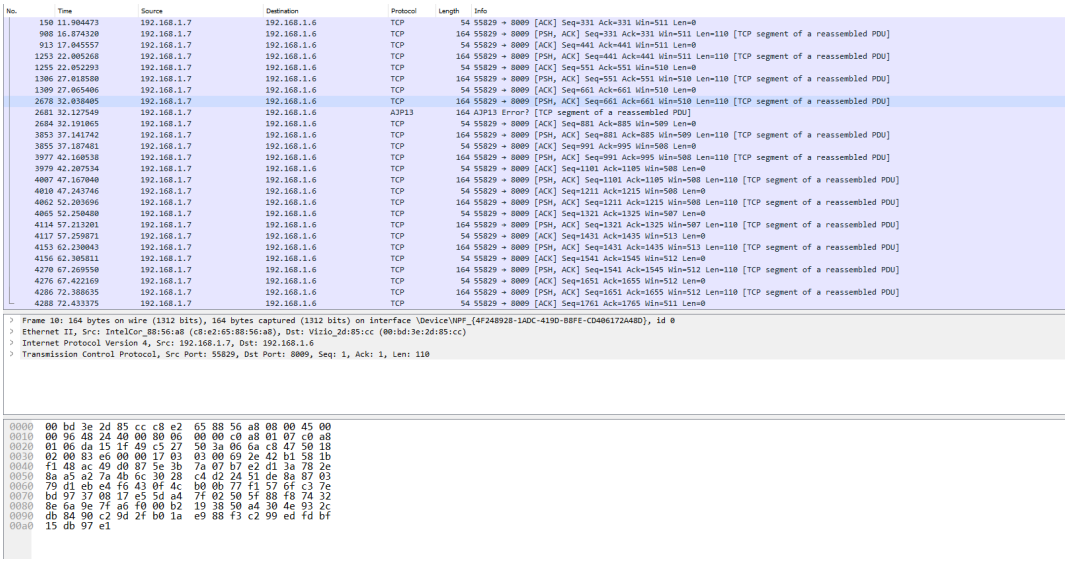
Ip.dst == 203.160.128.158



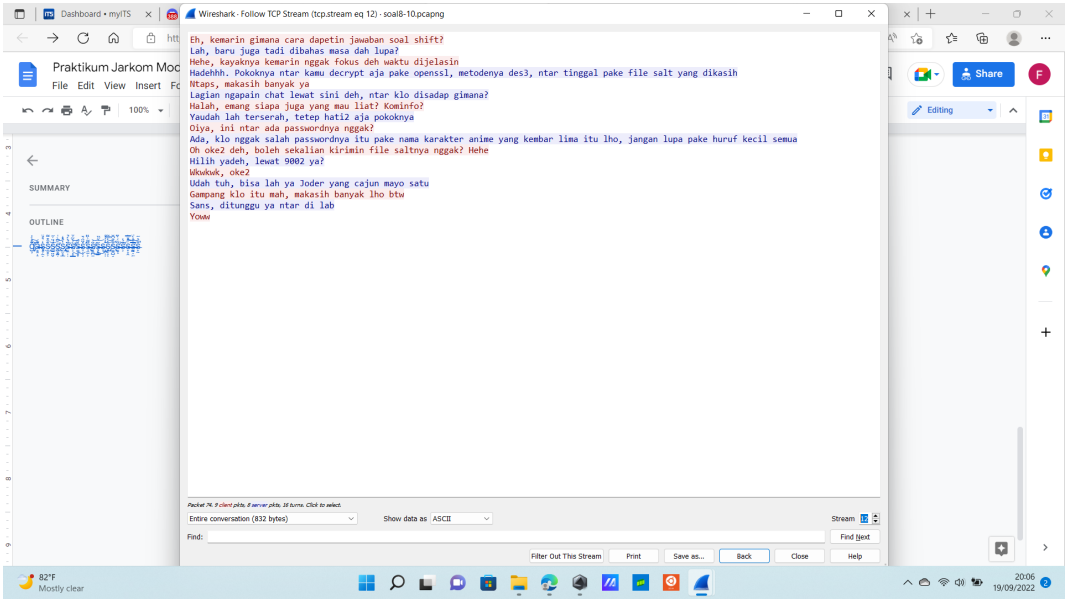
7. Ipconfig->didapat ip yang dimiliki



src host 192.168.1.7

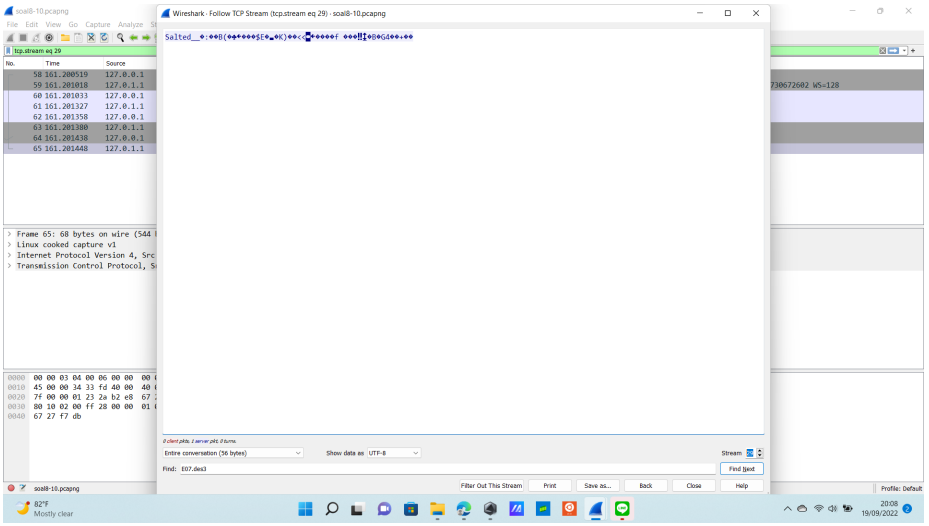


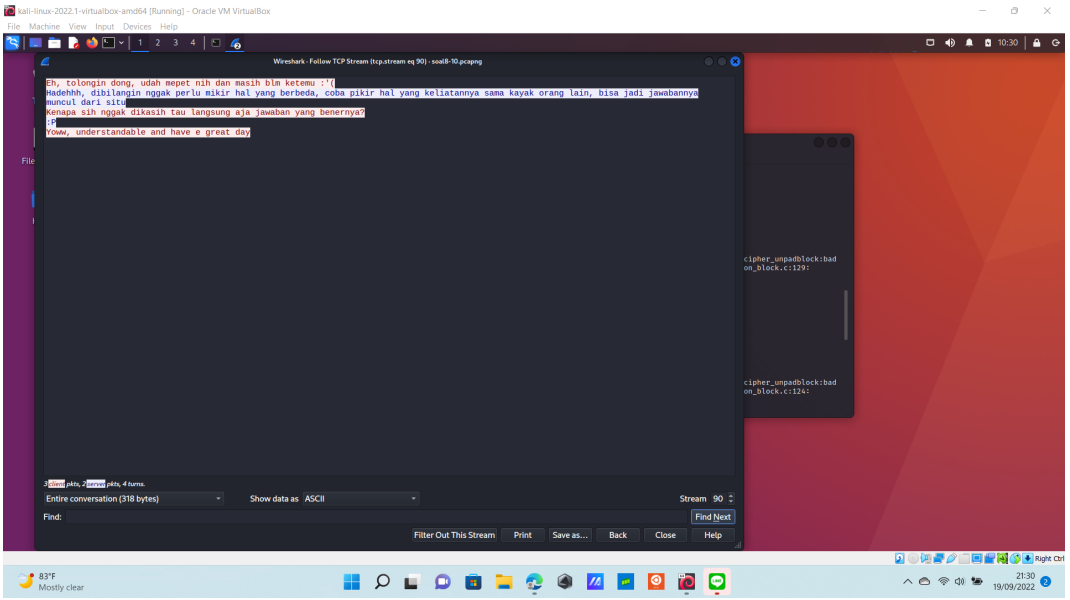
8-10.



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)

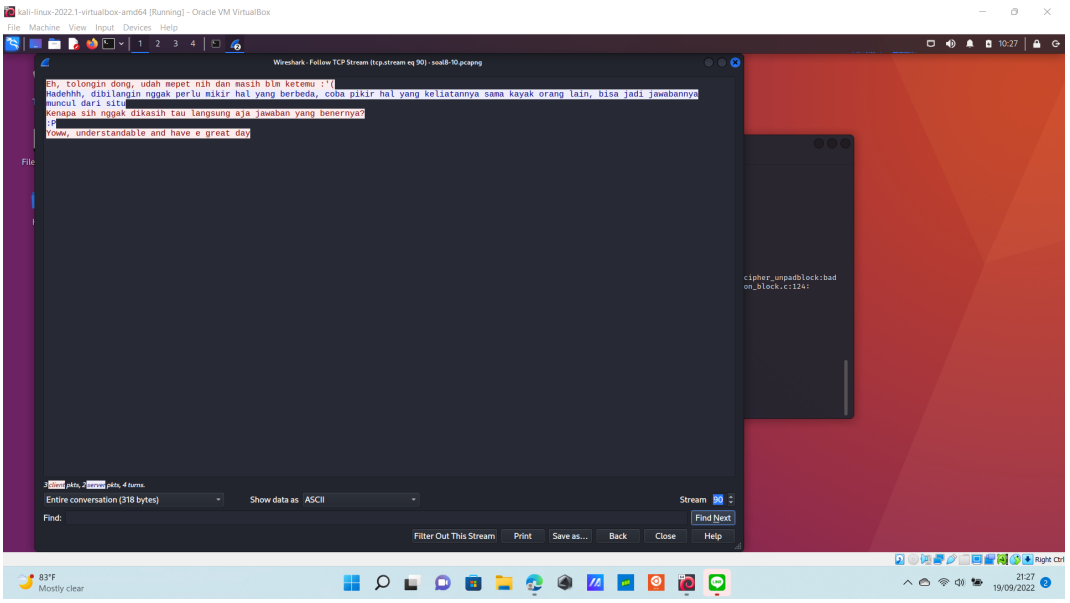
Lalu untuk command opensslnya kelompok kami menggunakan `openssl des3 -d -in E07.des3 -out flag.txt` (output flag.txt sebagai jawaban no.9 part 2, referensinya [Encrypt & Decrypt Files from the Command Line with OpenSSL (osxdaily.com)]())
Ternyata diminta password, setelah dicari di internet tentang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

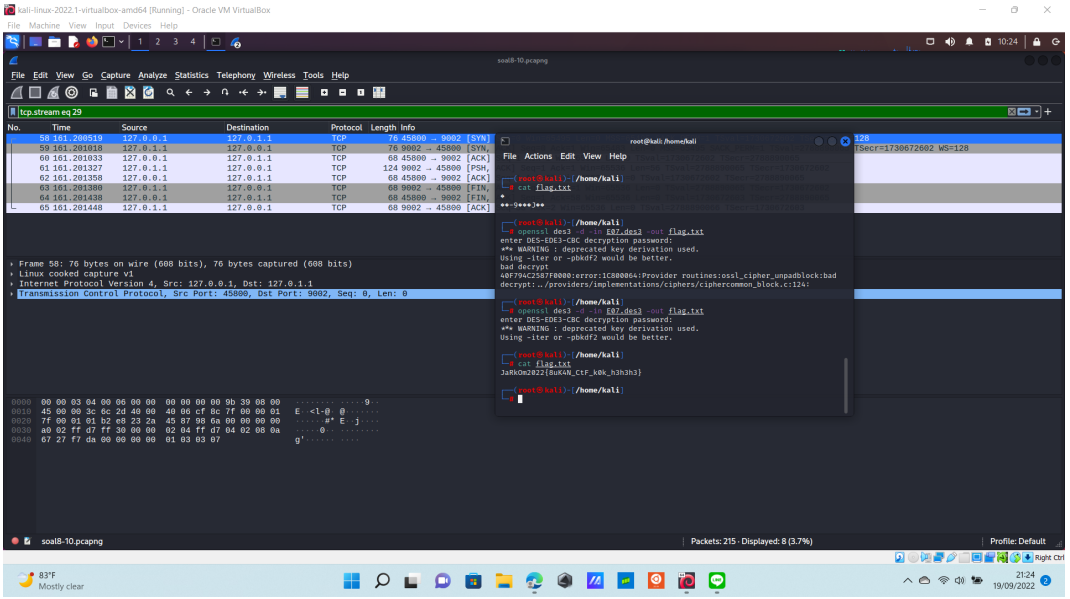




Setelah dicoba nama belakang semua karakter yang muncul ternyata salah (indikasi password salah -> terdapat “bad decrypt”), dan ternyata pada salah satu stream(stream 90) terdapat clue di atas

Maka dicoba iseng-iseng “nakano” karena dari 5 karakter yang ada pada film tersebut hal yang umum adalah nama keluarganya





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