

## Praktikum Modul 1 Jaringan Komputer (Kelompok E12)

1. Sebutkan web server yang digunakan pada "monta.if.its.ac.id"!

Diketahui ip address dari monta.if.its.ac.id adalah **103.94.189.5**.

**ping monta.if.its.ac.id**

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

C:\Users\lenovo>ping monta.if.its.ac.id

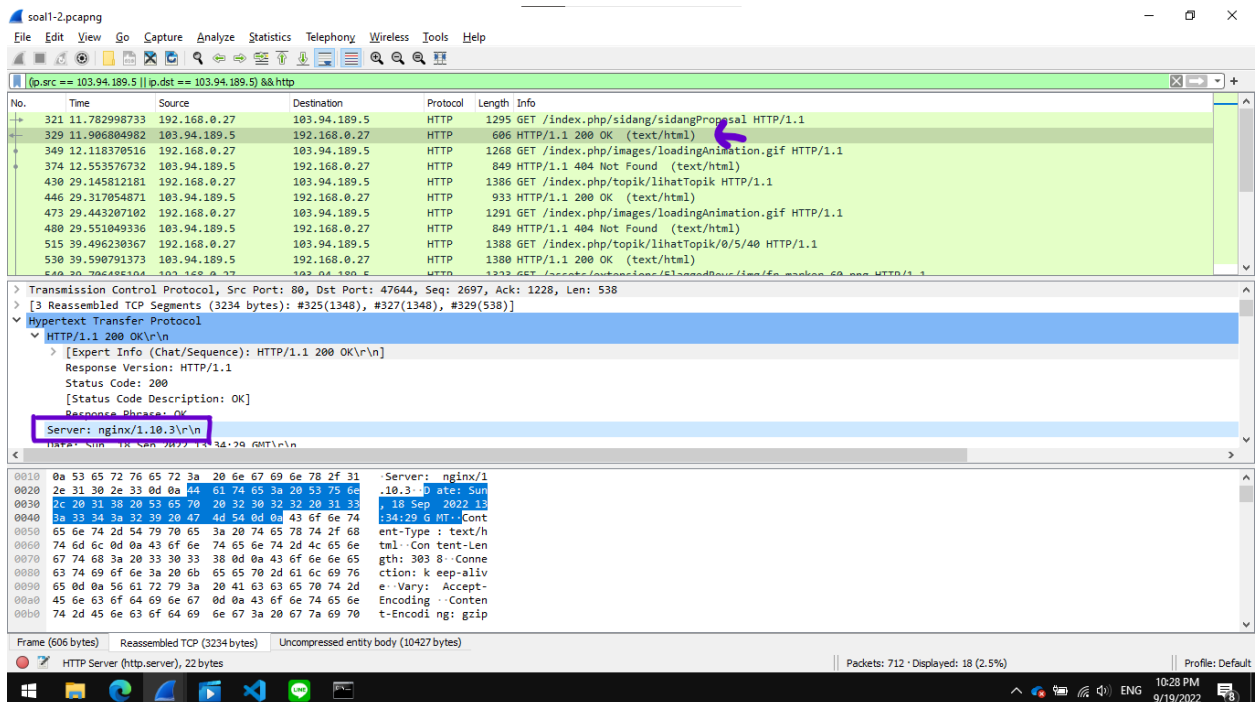
Pinging eclipse.if.its.ac.id [103.94.189.5] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 103.94.189.5:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

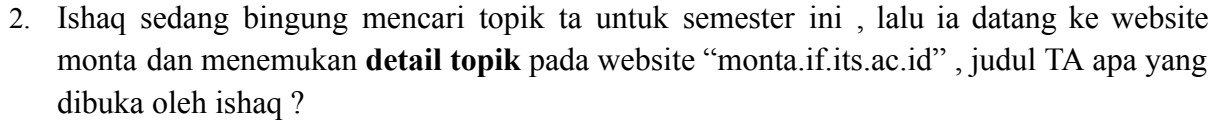
C:\Users\lenovo>
```

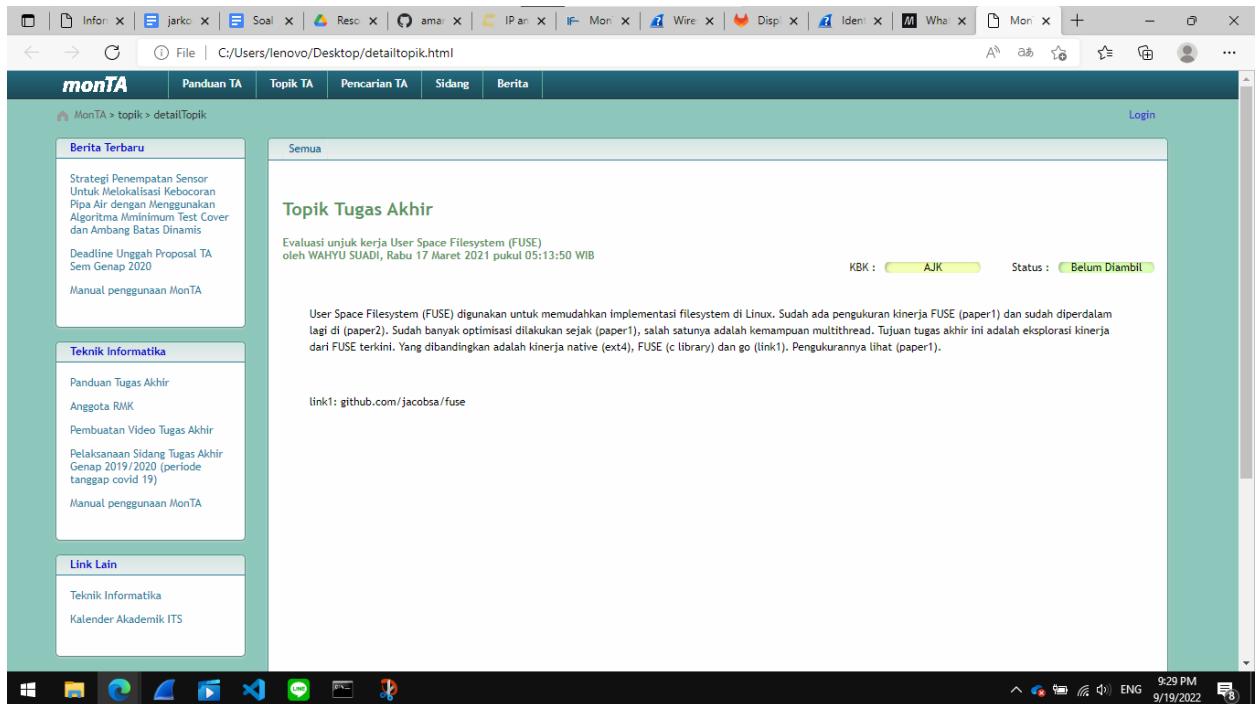
Berikut adalah ekspresi untuk mencari paket yang berasal dan menuju monta.if.its.ac.id dengan protokol http.

**(ip.src == 103.94.189.5 || ip.dst == 103.94.189.5) && http**



Dengan melihat detail salah satu paket, misal pada paket yang ditandai tanda panah, dapat diketahui bahwa web server yang digunakan adalah nginx/1.10.3.





Judul yang dibuka adalah **Evaluasi unjuk kerja User Space Filesystem (FUSE)**.

- Filter sehingga wireshark hanya menampilkan paket yang menuju port 80!

Yang harus dilakukan pertama adalah melihat semua paket yang menuju dan berasal dari port 80.

**tcp.port == 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=3479640034
287	7.234748634	192.124.249.36	192.168.0.27	TCP	56	80 → 50016 [RST] Seq=1 Win=0 Len=0
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=202987570
767	19.574566742	203.160.128.158	192.168.0.27	TCP	56	80 → 56166 [RST] Seq=1 Win=0 Len=0
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=4114884454 TSecr=0 WS=128
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=4114884454 TSecr=0 WS=128
6816	48.174183547	203.160.128.158	192.168.0.27	TCP	76	80 → 56168 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1360 SACK_PERM=1 TSval=203001113 TSecr=4114884454 WS=...
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=203001113
6818	48.174394695	192.168.0.27	203.160.128.158	HTTP	626	GET / HTTP/1.1
6819	48.226390170	203.160.128.158	192.168.0.27	TCP	76	80 → 56170 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1360 SACK_PERM=1 TSval=203001123 TSecr=4114884454 WS=...
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=203001123
6824	48.245117689	203.160.128.158	192.168.0.27	TCP	68	80 → 56168 [ACK] Seq=1 Ack=559 Win=30080 Len=0 TSval=203001127 TSecr=4114884491
6846	50.752065268	203.160.128.158	192.168.0.27	TCP	1416	80 → 56168 [ACK] Seq=1 Ack=559 Win=30080 Len=1348 TSval=203001756 TSecr=4114884491 [TCP segment of a reas...
6847	50.752089891	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=1349 Win=64128 Len=0 TSval=4114887069 TSecr=203001756
6848	50.752111201	203.160.128.158	192.168.0.27	TCP	1416	80 → 56168 [ACK] Seq=1349 Ack=559 Win=30080 Len=1348 TSval=203001756 TSecr=4114884491 [TCP segment of a rea...
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=203001756
6850	50.753158609	203.160.128.158	192.168.0.27	TCP	1416	80 → 56168 [ACK] Seq=2697 Ack=559 Win=30080 Len=1348 TSval=203001756 TSecr=4114884491 [TCP segment of a rea...
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=203001756
6852	50.753751823	203.160.128.158	192.168.0.27	TCP	1416	80 → 56168 [ACK] Seq=4045 Ack=559 Win=30080 Len=1348 TSval=203001756 TSecr=4114884491 [TCP segment of a rea...
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=203001756
6854	50.754259772	203.160.128.158	192.168.0.27	TCP	1416	80 → 56168 [ACK] Seq=5393 Ack=559 Win=30080 Len=1348 TSval=203001756 TSecr=4114884491 [TCP segment of a rea...

Diketahui bahwa ip address asal adalah 192.168.0.27, sehingga ekpresi sebelumnya berubah menjadi paket yang menuju/ berasal dari port 80 dan yang berasal dari ip 192.168.0.27.

**tcp.port == 80 && ip.src == 192.168.0.27**

No.	Time	Source	Destination	Protocol	Length	Info
275	7.142658322	192.168.0.27	192.124.249.36	TCP	68	58016 → 80 [FIN, ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=550146835 TSecr=3479640034
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=202987570
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=4114884454 TSecr=0 WS=128
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=4114884454 TSecr=0 WS=128
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=203001113
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	56176 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4114884543 TSecr=203001123
6847	50.752089891	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=1349 Win=64128 Len=0 TSval=4114887069 TSecr=203001756
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=203001756
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=203001756
6853	50.753755092	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=5393 Win=62976 Len=0 TSval=4114887070 TSecr=203001756
6855	50.754267943	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=6741 Win=64128 Len=0 TSval=4114887071 TSecr=203001756
6857	50.763183839	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=8089 Win=64128 Len=0 TSval=4114887080 TSecr=203001756
6859	50.763209366	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=9437 Win=62976 Len=0 TSval=4114887080 TSecr=203001756
6861	50.764250472	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=10785 Win=64128 Len=0 TSval=4114887081 TSecr=203001756
6863	50.765362654	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=12133 Win=64128 Len=0 TSval=4114887082 TSecr=203001756
6865	50.773420756	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=13481 Win=64128 Len=0 TSval=4114887090 TSecr=203001756
6867	50.794528276	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=14829 Win=64128 Len=0 TSval=4114887111 TSecr=203001768
6869	50.794574055	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=16177 Win=62976 Len=0 TSval=4114887111 TSecr=203001768
6876	50.831676538	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=17525 Win=67072 Len=0 TSval=4114887148 TSecr=203001777
6878	50.832845160	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=18873 Win=68864 Len=0 TSval=4114887149 TSecr=203001777

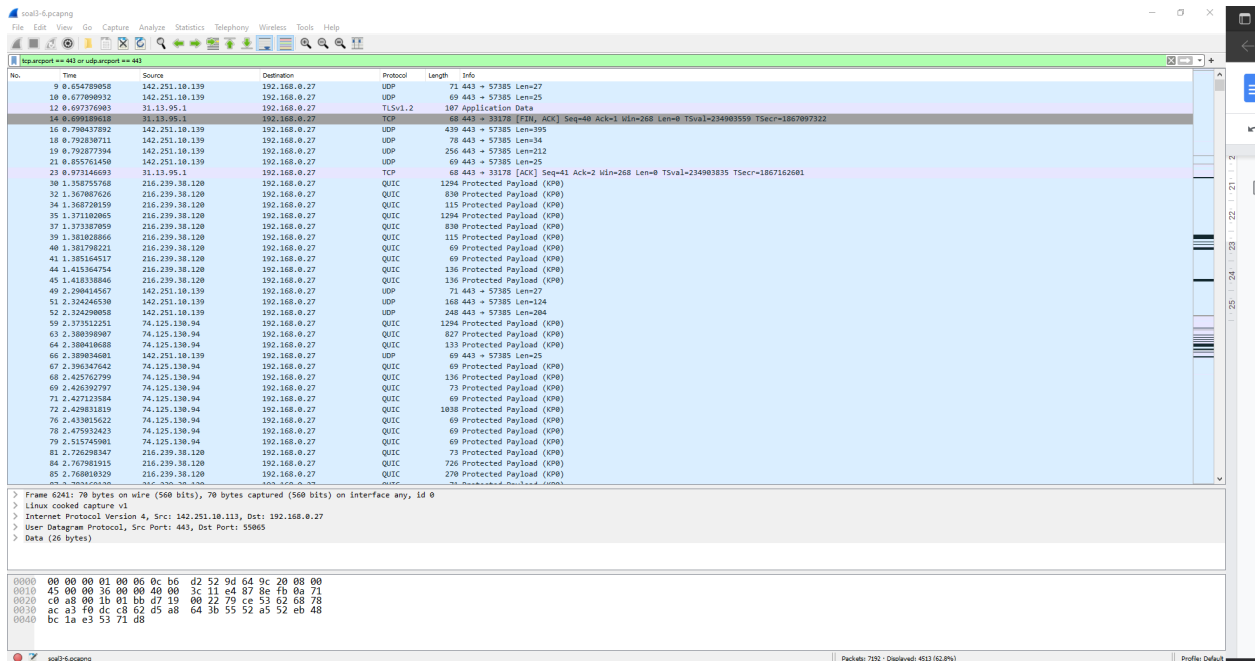
#### 4. Filter sehingga wireshark hanya mengambil paket yang berasal dari port 21!

Yang harus dilakukan adalah kita tinggal melakukan capture filter di port 21, yakni dengan menggunakan **tcp.srport == 21 or udp.srport == 21** untuk mengambil semua paket dengan protokol TCP atau UDP yang berasal dari port 21.

No.	Time	Source	Destination	Protocol	Length	Info
6243	35.992618176	127.0.0.1	127.0.0.1	TCP	76	21 → 55824 [SYN, ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=1460 SACK_PERM=1 TSval=4095422313 TSecr=4095422313 WS=128
6247	35.993626854	127.0.0.1	127.0.0.1	TCP	76	21 → 47094 [SYN, ACK] Seq=0 Ack=1 Win=65536 Len=0 MSS=1460 SACK_PERM=1 TSval=4117994603 TSecr=1721945475 WS=128
6248	36.000000000	127.0.0.1	127.0.0.1	TCP	76	47094 → 21 [ACK] Seq=559 Ack=1 Win=65536 Len=0 TSval=4117994603 TSecr=1721945475 WS=128
6251	36.020457800	127.0.0.1	127.0.0.1	FTP	88	Response: 220 (vsFTPd 3.0.3)
6252	36.020457800	127.0.0.1	127.0.0.1	TCP	68	[TCP Retransmission] 21 → 47094 [PSH, ACK] Seq=4 Ack=1 Win=65280 Len=0 TSval=4117994602 TSecr=1721945475
6255	36.021125484	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=4095422343
6261	36.023208877	127.0.0.1	127.0.0.1	TCP	68	21 → 47094 [ACK] Seq=21 Ack=11 Win=65280 Len=0 TSval=4117994602 TSecr=1721945504
6262	36.023208877	127.0.0.1	127.0.0.1	TCP	68	[TCP Dup ACK 6258] 21 → 47094 [ACK] Seq=559 Ack=21 Win=65280 Len=0 TSval=4117994602 TSecr=1721945504
6263	36.023274372	127.0.0.1	127.0.0.1	FTP	100	Response: 530 Please login with USER and PASS.
6264	36.023274372	127.0.0.1	127.0.0.1	TCP	100	[TCP Retransmission] 21 → 47094 [PSH, ACK] Seq=21 Ack=11 Win=65280 Len=0 TSval=4117994602 TSecr=1721945504
6267	36.02404354	127.0.0.1	127.0.0.1	FTP	100	Response: 530 Please login with USER and PASS.
6270	36.024606574	127.0.0.1	127.0.0.1	TCP	68	21 → 55824 [ACK] Seq=59 Ack=21 Win=65536 Len=0 TSval=4095422343 TSecr=4095422343
6273	36.02519043	127.0.0.1	127.0.0.1	TCP	68	21 → 47094 [ACK] Seq=59 Ack=21 Win=65280 Len=0 TSval=4117994602 TSecr=1721945504
6274	36.02519043	127.0.0.1	127.0.0.1	TCP	68	[TCP Dup ACK 6273] 21 → 47094 [ACK] Seq=59 Ack=21 Win=65280 Len=0 TSval=4117994602 TSecr=1721945504
6275	36.025376177	127.0.0.1	127.0.0.1	FTP	100	Response: 530 Please login with USER and PASS.
6276	36.025761877	127.0.0.1	127.0.0.1	TCP	100	[TCP Retransmission] 21 → 47094 [PSH, ACK] Seq=9 Ack=21 Win=65280 Len=0 TSval=4117994602 TSecr=1721945504
6279	36.02603773	127.0.0.1	127.0.0.1	FTP	100	Response: 530 Please login with USER and PASS.
6282	36.026998862	127.0.0.1	127.0.0.1	TCP	68	21 → 55824 [ACK] Seq=97 Ack=36 Win=65536 Len=0 TSval=4095422344 TSecr=4095422344
6285	36.02798860	127.0.0.1	127.0.0.1	TCP	68	21 → 47094 [ACK] Seq=97 Ack=36 Win=65280 Len=0 TSval=4117994603 TSecr=1721945505
6286	36.02798860	127.0.0.1	127.0.0.1	TCP	68	[TCP Dup ACK 6285] 21 → 47094 [ACK] Seq=97 Ack=36 Win=65280 Len=0 TSval=4117994603 TSecr=1721945505
6287	36.028034463	127.0.0.1	127.0.0.1	FTP	100	Response: 331 Please specify the password.
6288	36.02834463	127.0.0.1	127.0.0.1	TCP	100	[TCP Retransmission] 21 → 47094 [PSH, ACK] Seq=97 Ack=36 Win=65280 Len=0 TSval=4117994603 TSecr=1721945505
6291	36.02864379	127.0.0.1	127.0.0.1	FTP	100	Response: 331 Please specify the password.
6294	36.023114812	127.0.0.1	127.0.0.1	TCP	68	21 → 55824 [ACK] Seq=131 Ack=51 Win=65536 Len=0 TSval=4095422344 TSecr=4095422344
6297	36.023115849	127.0.0.1	127.0.0.1	TCP	68	21 → 47094 [ACK] Seq=131 Ack=51 Win=65280 Len=0 TSval=4117994603 TSecr=1721945505
6298	36.023115849	127.0.0.1	127.0.0.1	TCP	68	[TCP Dup ACK 6297] 21 → 47094 [ACK] Seq=131 Ack=51 Win=65280 Len=0 TSval=4117994603 TSecr=1721945505
6299	36.063679332	127.0.0.1	127.0.0.1	FTP	93	Response: 230 Login successful.
6300	36.063679332	127.0.0.1	127.0.0.1	TCP	76	[TCP Retransmission] 21 → 47094 [PSH, ACK] Seq=331 Ack=51 Win=65280 Len=0 TSval=4117994713 TSecr=1721945505
6303	36.063762135	127.0.0.1	127.0.0.1	FTP	93	Response: 230 Login successful.
6306	36.064304864	127.0.0.1	127.0.0.1	TCP	68	21 → 55824 [ACK] Seq=154 Ack=58 Win=65536 Len=0 TSval=4095422385 TSecr=4095422385
6309	36.064434374	127.0.0.1	127.0.0.1	TCP	68	21 → 47094 [ACK] Seq=154 Ack=58 Win=65280 Len=0 TSval=4117994734 TSecr=1721945546
6310	36.064434374	127.0.0.1	127.0.0.1	TCP	68	[TCP Dup ACK 6309] 21 → 47094 [ACK] Seq=154 Ack=58 Win=65280 Len=0 TSval=4117994734 TSecr=1721945546
6311	36.064506128	127.0.0.1	127.0.0.1	FTP	105	Response: 250 Directory successfully changed.
6312	36.064506128	127.0.0.1	127.0.0.1	TCP	100	[TCP Retransmission] 21 → 47094 [PSH, ACK] Seq=154 Ack=58 Win=65280 Len=0 TSval=4117994734 TSecr=1721945546

#### 5. Filter sehingga wireshark hanya mengambil paket yang berasal dari port 443!

Yang harus dilakukan adalah kita tinggal melakukan capture filter di port 443, yakni dengan menggunakan **tcp.srport == 443 or udp.srport == 443** untuk mengambil semua paket dengan protokol TCP atau UDP yang berasal dari port 443.



## 6. Filter sehingga wireshark hanya menampilkan paket yang menuju ke lipi.go.id!

Diketahui web address yang diminta adalah ping.lipi.id, maka dari itu yang perlu dilakukan adalah mencari ip address nya dengan cara membuka cmd dan enter command ping.lipi.go.id

### ping lipi.go.id

```
C:\Users\User>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=47ms TTL=54
Reply from 203.160.128.158: bytes=32 time=36ms TTL=54
Reply from 203.160.128.158: bytes=32 time=34ms TTL=54
Reply from 203.160.128.158: bytes=32 time=61ms TTL=54

Ping statistics for 203.160.128.158:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 34ms, Maximum = 61ms, Average = 44ms
```

Setelah mendapatkan ip address nya, kita mengambil paket yang berasal dari ip address tersebut dengan cara mengenter display filter ip.dst == 203.160.128.158

### ip.dst == 203.160.128.158

soal3-6.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.dst == 203.160.128.158

No.	Time	Source	Destination	Protocol	Length	Info
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 T
6812	48.137063386	192.168.0.27	203.160.128.158	TCP	76	56168 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
6814	48.137134172	192.168.0.27	203.160.128.158	TCP	76	56170 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S
6817	48.174227851	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSva
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 TSva
6847	50.752089891	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=1349 Win=64128 Len=0
6849	50.752115614	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=2697 Win=62976 Len=0
6851	50.753732554	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=4045 Win=64128 Len=0
6853	50.753755692	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=5393 Win=62976 Len=0
6855	50.754267943	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=6741 Win=64128 Len=0
6857	50.763183839	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=8089 Win=64128 Len=0
6859	50.763209366	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=9437 Win=62976 Len=0
6861	50.764250472	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=10785 Win=64128 Len=
6863	50.765362654	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=12133 Win=64128 Len=
6865	50.773420756	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=13481 Win=64128 Len=
6867	50.794528276	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=14829 Win=64128 Len=
6869	50.794574055	192.168.0.27	203.160.128.158	TCP	68	56168 → 80 [ACK] Seq=559 Ack=16177 Win=62976 Len=

## 7. Filter sehingga wireshark hanya mengambil paket yang berasal dari ip kalian!

Kita perlu menampilkan paket yang berasal ip kita sendiri maka dari itu kita membuka capture wifi

### Capture

...using this filter:  All interfaces shown ▾

Local Area Connection\* 7

Wi-Fi

Local Area Connection\* 10

Kemudian kita perlu mengambil ip address kita sendiri melalui cmd dengan enter command ipconfig dan mengambil ip address yang tertulis di sebelah IPV4 Address

### ipconfig

```

Select C:\Windows\system32\cmd.exe
C:\Users\User>ipconfig

Windows IP Configuration

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::2d4f:7335:3e53:37d%10
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Wireless LAN adapter Local Area Connection* 1:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Local Area Connection* 10:

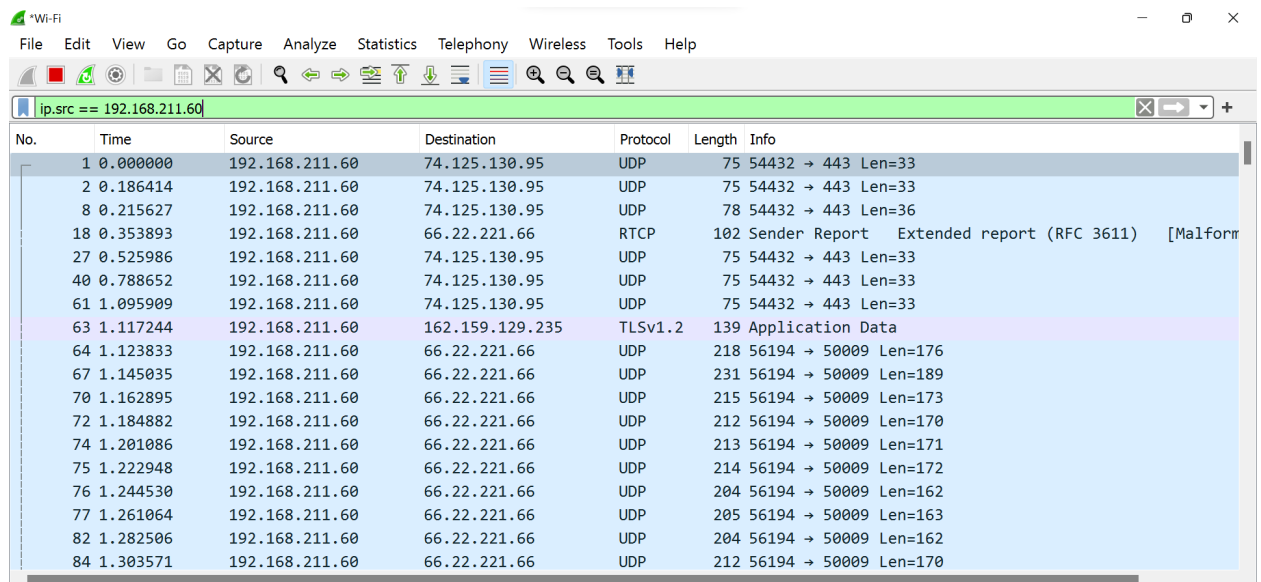
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::1113:ac09:fee4:c335%15
    IPv4 Address. . . . . : 192.168.211.60
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.211.164
  
```

Setelah didapatkannya ip address, ambil paket yang berasal dari ip address kita dengan menggunakan ip.src == 192.168.211.60

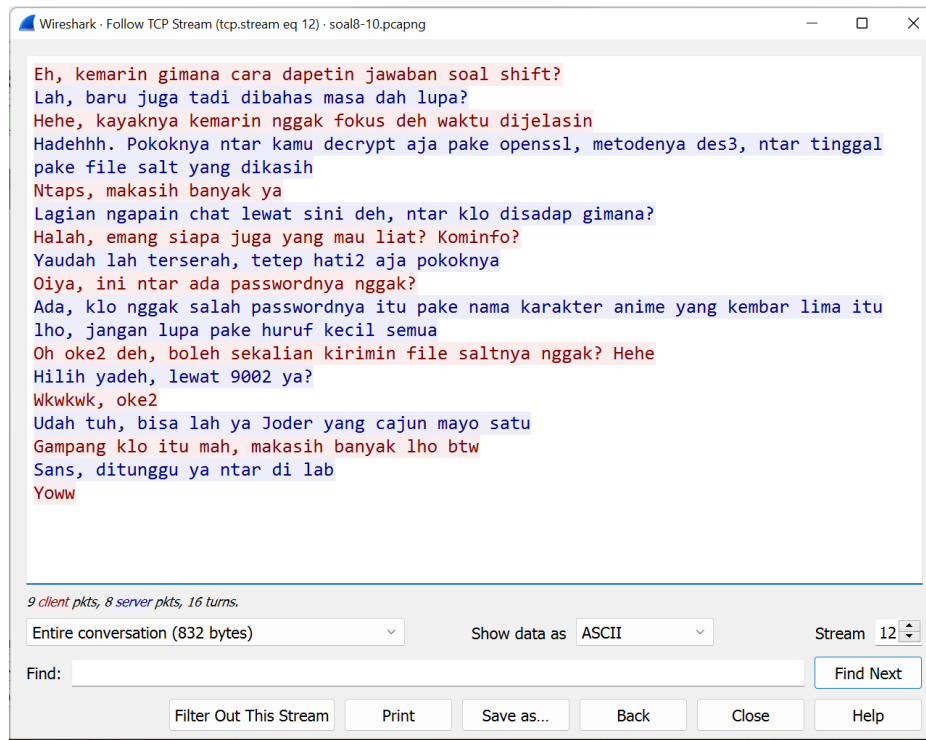
**ip.src == 192.168.211.60**



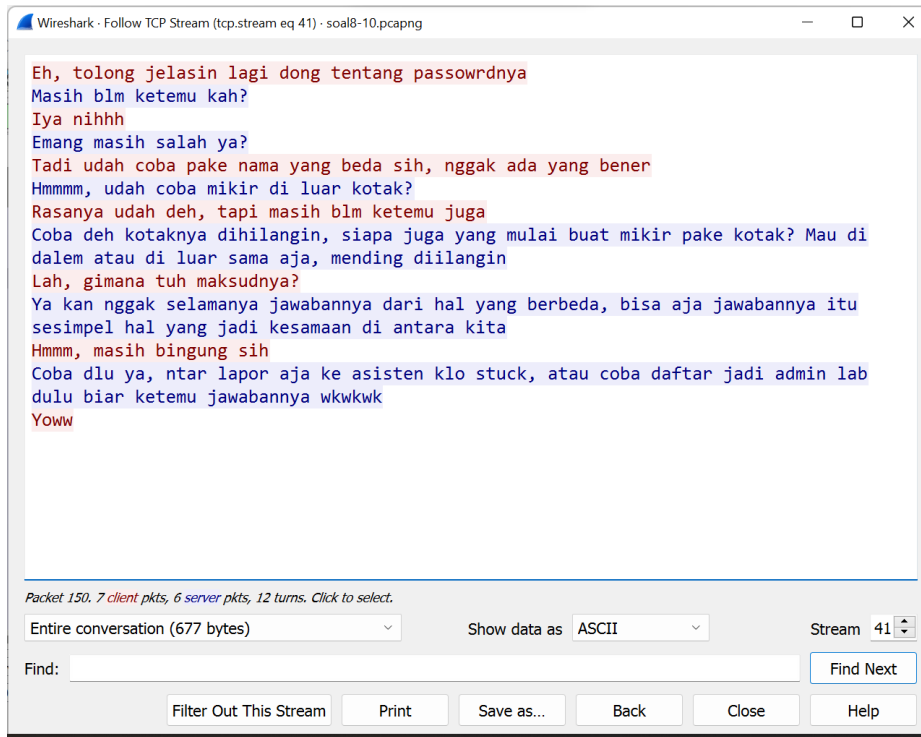
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.211.60	74.125.130.95	UDP	75	54432 → 443 Len=33
2	0.186414	192.168.211.60	74.125.130.95	UDP	75	54432 → 443 Len=33
8	0.215627	192.168.211.60	74.125.130.95	UDP	78	54432 → 443 Len=36
18	0.353893	192.168.211.60	66.22.221.66	RTCP	102	Sender Report Extended report (RFC 3611) [Malform
27	0.525986	192.168.211.60	74.125.130.95	UDP	75	54432 → 443 Len=33
40	0.788652	192.168.211.60	74.125.130.95	UDP	75	54432 → 443 Len=33
61	1.095909	192.168.211.60	74.125.130.95	UDP	75	54432 → 443 Len=33
63	1.117244	192.168.211.60	162.159.129.235	TLSv1.2	139	Application Data
64	1.123833	192.168.211.60	66.22.221.66	UDP	218	56194 → 50009 Len=176
67	1.145035	192.168.211.60	66.22.221.66	UDP	231	56194 → 50009 Len=189
70	1.162895	192.168.211.60	66.22.221.66	UDP	215	56194 → 50009 Len=173
72	1.184882	192.168.211.60	66.22.221.66	UDP	212	56194 → 50009 Len=170
74	1.201086	192.168.211.60	66.22.221.66	UDP	213	56194 → 50009 Len=171
75	1.222948	192.168.211.60	66.22.221.66	UDP	214	56194 → 50009 Len=172
76	1.244530	192.168.211.60	66.22.221.66	UDP	204	56194 → 50009 Len=162
77	1.261064	192.168.211.60	66.22.221.66	UDP	205	56194 → 50009 Len=163
82	1.282506	192.168.211.60	66.22.221.66	UDP	204	56194 → 50009 Len=162
84	1.303571	192.168.211.60	66.22.221.66	UDP	212	56194 → 50009 Len=170

8. Telusuri aliran paket dalam file .pcap yang diberikan, cari informasi berguna berupa percakapan antara dua mahasiswa terkait tindakan kecurangan pada kegiatan praktikum. Percakapan tersebut dilaporkan menggunakan protokol jaringan dengan tingkat keandalan yang tinggi dalam pertukaran datanya sehingga kalian perlu menerapkan filter dengan protokol yang tersebut.

Caranya adalah dengan melakukan **tcp.stream**





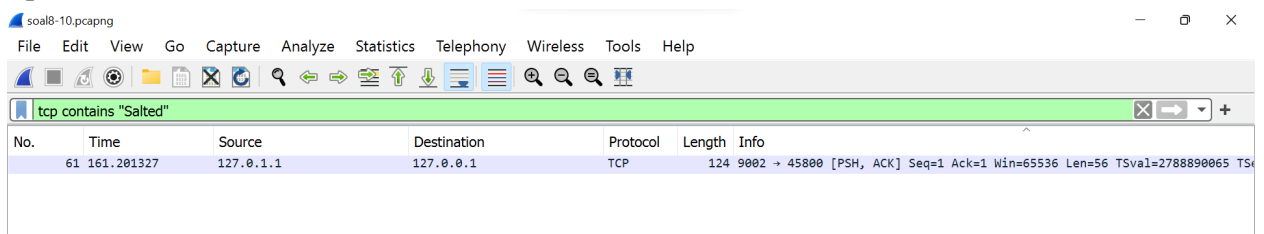


9. Terdapat laporan adanya pertukaran file yang dilakukan oleh kedua mahasiswa dalam percakapan yang diperoleh, carilah file yang dimaksud! Untuk memudahkan laporan kepada atasan, beri nama file yang ditemukan dengan format [nama\_kelompok].des3 dan simpan output file dengan nama “flag.txt”

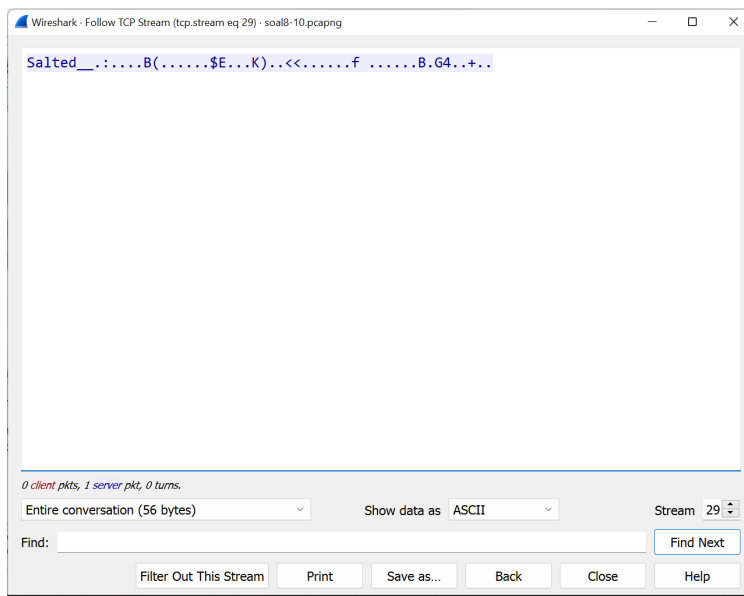


Dari percakapan pada nomor 8, dapat diketahui bahwa kedua mahasiswa tersebut sedang bertukar file salt, maka dari itu kita dapat melakukan display filter dengan keyword “salt”

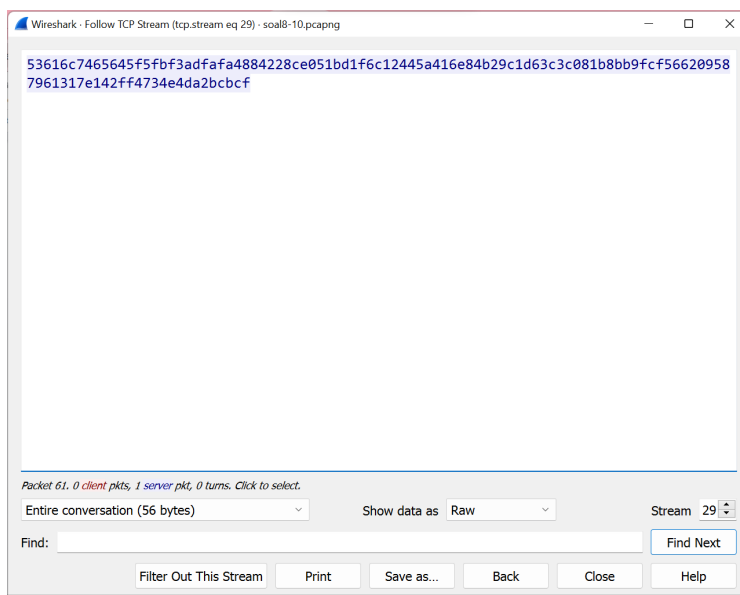
**tcp contains “Salted”**



Ditemukan pada paket no. 61

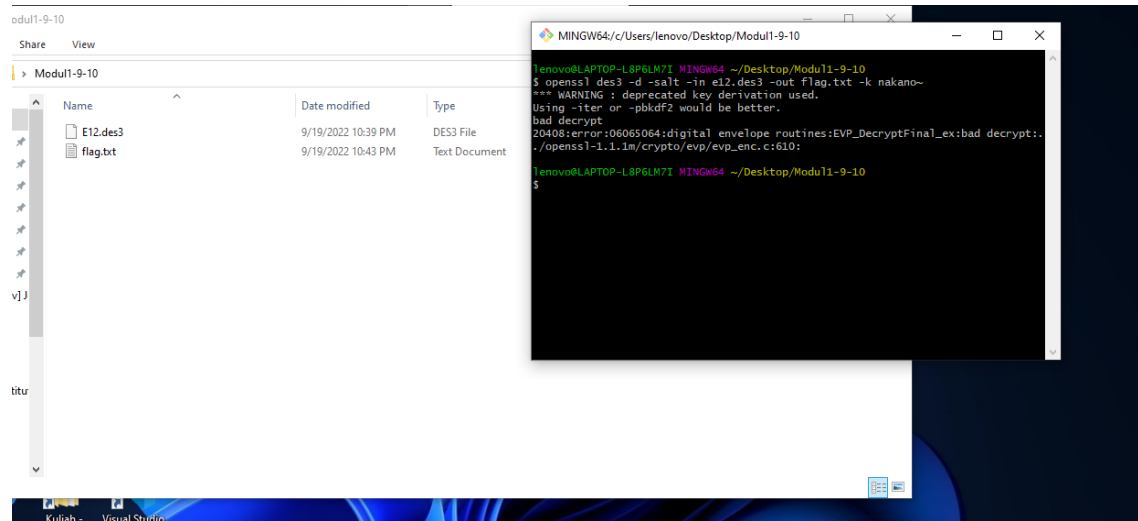


Kemudian, kita show data as raw dan save as E12.des3

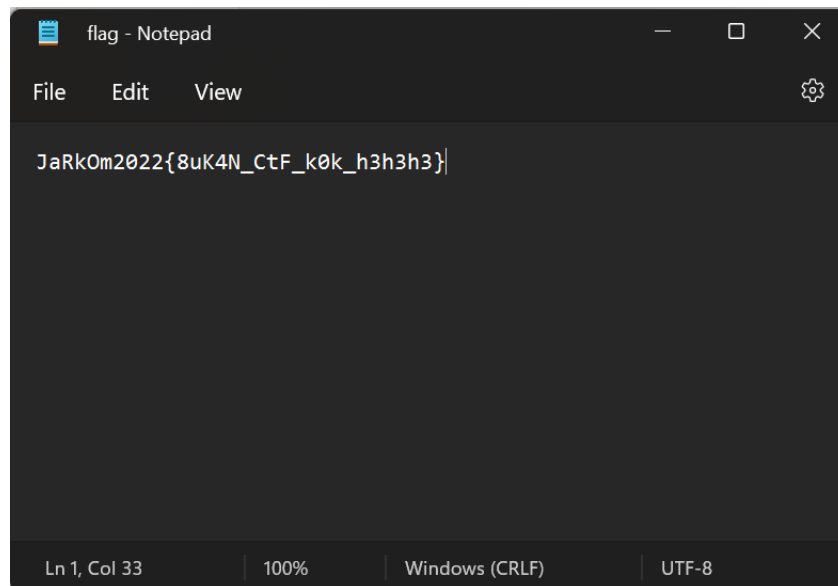


Pada folder yang terdapat file .des3 tersebut, kita melakukan git bash dengan command **openssl des3 -d -salt -in e12.des3 -out flag.txt -k nakano**

Password nakano didapatkan dari percakapan yang ditampilkan pada nomor 8



Kemudian akan muncul output flag.txt yakni:



10. Temukan password rahasia (flag) dari organisasi bawah tanah yang disebutkan di atas!  
Isi flag.txt : **JaRkOm2022{8uK4N\_CtF\_k0k\_h3h3h3}**  
Password untuk openssl : **nakano**