

Revisi Praktikum Modul 1
“Crimping dan Wireshark”



Disusun oleh Kelompok D-06 dengan Anggota:

Fian Awamiry Maulana (5025201035)

Rere Arga Dewanata (5025201078)

Muhamad Ridho Pratama (5025201186)

Jaringan Komputer D

Departemen Teknik Informatika

Fakultas Teknologi Elektro dan Informatika Cerdas

Institut Teknologi Sepuluh Nopember

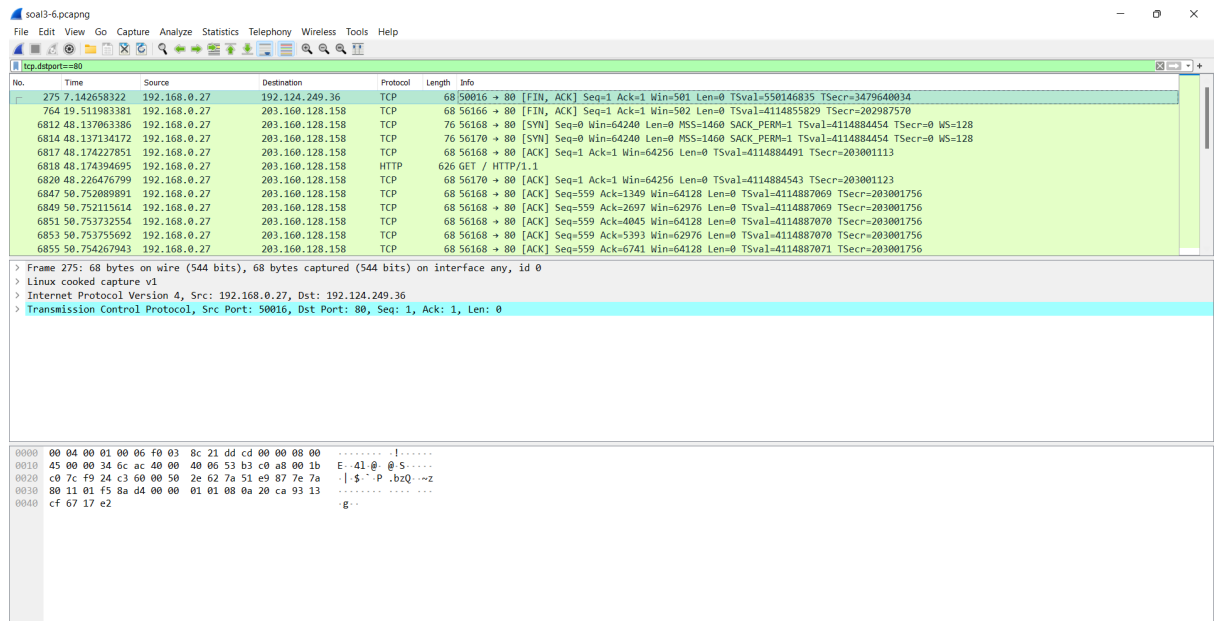
2022/2023

3. Filter sehingga wireshark hanya menampilkan paket yang menuju port 80!

Jawab:

Melakukan display filter pada file .pcapng yang sudah disediakan, terapkan:

tcp.dstport == 80

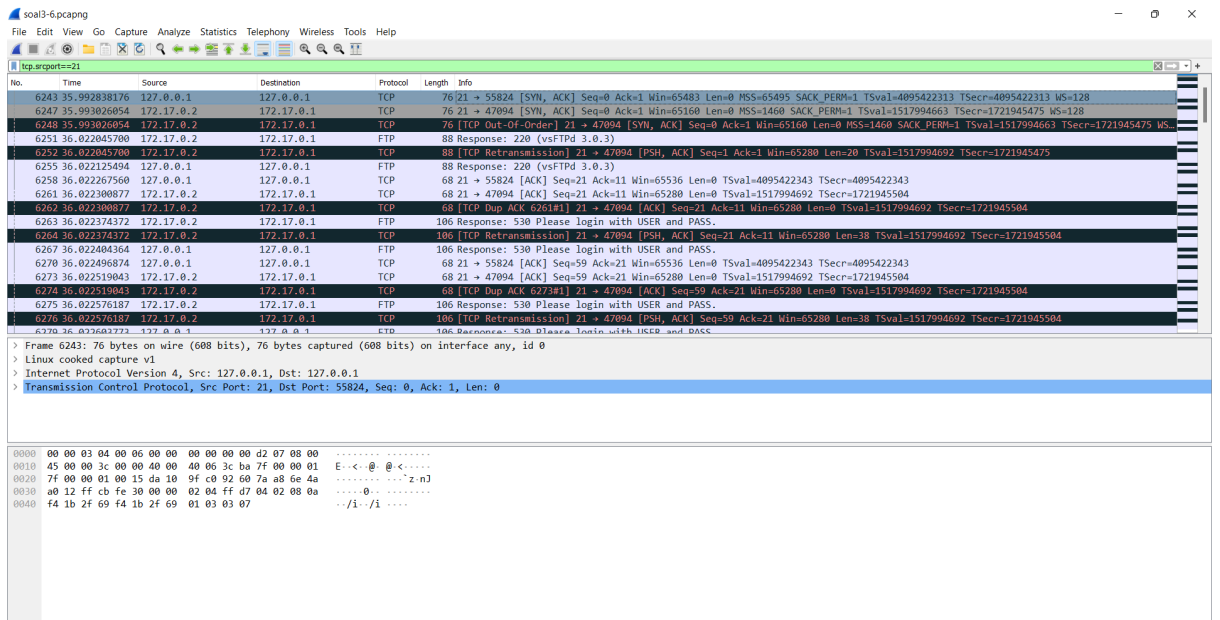


4. Filter sehingga wireshark hanya mengambil paket yang berasal dari port 21!

Jawab:

Melakukan display filter pada file .pcapng yang sudah disediakan, terapkan:

tcp.srcport==21



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

Jawab:

Melakukan display filter pada file .pcapng yang sudah disediakan, terapkan:

tcp.srcport==443

The image shows a Wireshark capture of a network traffic. The filter bar at the top is set to `tcp.srcport==443`. The packet list shows several packets, with the selected packet being a TCP Reset (RST) from 192.168.0.27 to 74.125.24.91. The packet details pane shows the Internet Protocol Version 4 and Transmission Control Protocol sections. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
6147	32.745251602	74.125.24.91	192.168.0.27	TCP	76	443 → 51870 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1360 SACK_PERM=1 TSval=651400817 TSecr=3380257171 WS=256
6150	32.823009983	74.125.24.91	192.168.0.27	TCP	68	443 → 51870 [ACK] Seq=1 Ack=518 Win=66816 Len=0 TSval=651400881 TSecr=3380257237
6151	32.823077877	74.125.24.91	192.168.0.27	TLSv1.3	1416	Server Hello, Change Cipher Spec
6153	32.823520916	74.125.24.91	192.168.0.27	TCP	1416	443 → 51870 [PSH, ACK] Seq=1349 Ack=518 Win=66816 Len=1348 TSval=651400882 TSecr=3380257237 [TCP segment of a reassembled PDU]
6155	32.824326201	74.125.24.91	192.168.0.27	TCP	1416	443 → 51870 [ACK] Seq=2697 Ack=518 Win=66816 Len=1348 TSval=651400882 TSecr=3380257237 [TCP segment of a reassembled PDU]
6157	32.826699680	74.125.24.91	192.168.0.27	TCP	1416	443 → 51870 [PSH, ACK] Seq=4045 Ack=518 Win=66816 Len=1348 TSval=651400882 TSecr=3380257237 [TCP segment of a reassembled PDU]
6159	32.826798278	74.125.24.91	192.168.0.27	TCP	1416	443 → 51870 [ACK] Seq=5393 Ack=518 Win=66816 Len=1348 TSval=651400882 TSecr=3380257237 [TCP segment of a reassembled PDU]
6161	32.828462129	74.125.24.91	192.168.0.27	TLSv1.3	133	Application Data
6166	32.937483406	74.125.24.91	192.168.0.27	TCP	68	443 → 51870 [ACK] Seq=6806 Ack=684 Win=67840 Len=0 TSval=651400978 TSecr=3380257324
6167	32.937502611	74.125.24.91	192.168.0.27	TLSv1.3	912	Application Data, Application Data
6170	32.938113625	74.125.24.91	192.168.0.27	TLSv1.3	99	Application Data
6172	32.939444329	74.125.24.91	192.168.0.27	TCP	80	443 → 51870 [ACK] Seq=6806 Ack=518 Win=67840 Len=0 TSval=651400978 TSecr=3380257320 SLE=592 SRE=684
6174	32.991952408	74.125.24.91	192.168.0.27	TCP	68	[TCP Previous segment not captured] 443 → 51870 [ACK] Seq=8756 Ack=1371 Win=69120 Len=0 TSval=651401074 TSecr=3380257429
6175	33.127610535	74.125.24.91	192.168.0.27	TCP	107	[TCP Retransmission] 443 → 51870 [PSH, ACK] Seq=8717 Ack=1371 Win=69120 Len=39 TSval=651401220 TSecr=3380257429
6182	33.404857352	74.125.24.91	192.168.0.27	TCP	1104	[TCP Retransmission] 443 → 51870 [PSH, ACK] Seq=7681 Ack=1371 Win=69120 Len=1036 TSval=651401492 TSecr=3380257619
6186	33.460599451	74.125.24.91	192.168.0.27	TCP	68	443 → 51870 [ACK] Seq=8756 Ack=1410 Win=69120 Len=0 TSval=651401544 TSecr=3380257897
6187	33.490209638	74.125.24.91	192.168.0.27	TCP	68	443 → 51870 [ACK] Seq=8756 Ack=1445 Win=69120 Len=0 TSval=651401544 TSecr=3380257902

Frame 6150: 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: 74.125.24.91, Dst: 192.168.0.27
> Transmission Control Protocol, Src Port: 443, Dst Port: 51870, Seq: 1, Ack: 518, Len: 0

0000 00 00 00 01 00 06 0c b6 d2 52 9d 64 c7 04 08 00R.d....
0010 45 00 00 34 e2 a4 00 00 7a 06 3a 84 4a 7d 18 5b E-4...z:-J)-[
0020 c0 a8 00 1b 01 bb ca 9e 7b dc 7a 30 34 eb 90 a5(-z04....
0030 80 10 01 05 a1 50 00 00 01 01 08 0a 26 d3 96 b1P.....&...
0040 c9 7a a1 d5z... ..

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

Jawab:

Pertama, nyalakan “Resolve Network Addresses” terlebih dahulu pada **View -> Name Resolution -> Resolve Network Addresses**, agar IP-nya berbentuk alamat yang sudah di-resolve, bukan plain IP address.

Lalu, lakukan display filter pada file .pcapng yang sudah disediakan, terapkan:

ip.dst_host contains “lipi.go.id”

The image shows a Wireshark capture of a network traffic. The filter bar at the top is set to `ip.dst_host contains "lipi.go.id"`. The packet list shows several packets, with the selected packet being a TCP Reset (RST) from 192.168.0.27 to ppid.lipi.go.id. The packet details pane shows the Internet Protocol Version 4 and Transmission Control Protocol sections. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
764	19.511983...	192.168.0.27	ppid.lipi.go.id	TCP	68	56166 → 80 [FIN, ACK] Seq=1 Ack=1 Win=502 Len=0 TSval=4114855829 TSecr=202987570
6812	48.137063...	192.168.0.27	ppid.lipi.go.id	TCP	76	56168 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4114884454 TSecr=0 WS=128
6814	48.137134...	192.168.0.27	ppid.lipi.go.id	TCP	76	56170 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=4114884454 TSecr=0 WS=128
6817	48.174227...	192.168.0.27	ppid.lipi.go.id	TCP	68	56168 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4114884491 TSecr=203001113
6818	48.174394...	192.168.0.27	ppid.lipi.go.id	HTTP	626	GET / HTTP/1.1
6820	48.226476...	192.168.0.27	ppid.lipi.go.id	TCP	68	56170 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4114884543 TSecr=203001123
6847	50.752089...	192.168.0.27	ppid.lipi.go.id	TCP	68	56168 → 80 [ACK] Seq=559 Ack=1349 Win=64128 Len=0 TSval=4114887069 TSecr=203001756
6849	50.752115...	192.168.0.27	ppid.lipi.go.id	TCP	68	56168 → 80 [ACK] Seq=559 Ack=2697 Win=62976 Len=0 TSval=4114887069 TSecr=203001756
6851	50.753732...	192.168.0.27	ppid.lipi.go.id	TCP	68	56168 → 80 [ACK] Seq=559 Ack=4045 Win=64128 Len=0 TSval=4114887070 TSecr=203001756

Frame 764: 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 (192.168.0.27), Dst: ppid.lipi.go.id (203.160.160.160)
> Transmission Control Protocol, Src Port: 56166, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

0000 00 04 00 01 00 06 f0 03 8c 21 dd cd e9 74 08 00!-t-
0010 45 00 00 34 a6 c2 40 00 40 06 86 ff c0 a8 00 1b E-4:@@.....
0020 cb a0 80 9e db 66 00 50 3d 57 1d 82 aa d2 be e9 f P=W.....
0030 80 11 01 f6 b6 52 00 00 01 01 08 0a f5 43 b7 95R.....C-
0040 0c 19 58 32X2

Untuk soal 8-10, silahkan baca cerita di bawah ini!

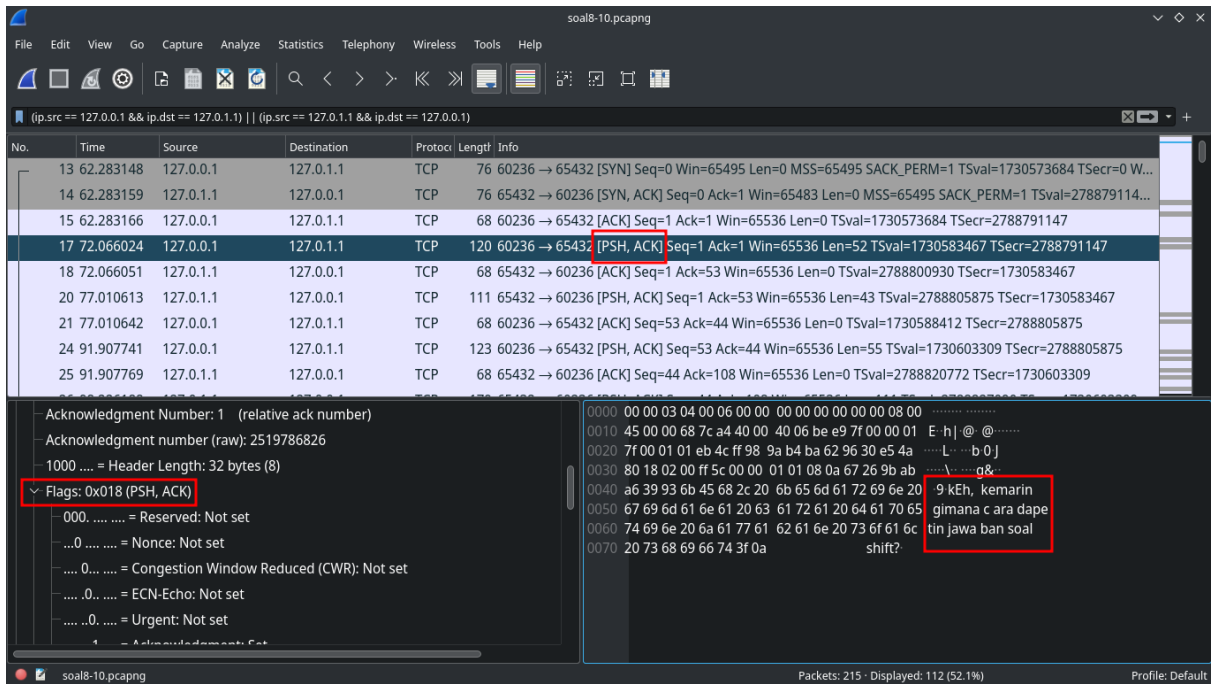
Di sebuah planet bernama Viltrumite, terdapat Kementerian Komunikasi dan Informatika yang baru saja menetapkan kebijakan baru. Dalam kebijakan baru tersebut, pemerintah dapat mengakses data pribadi masyarakat secara bebas jika memang dibutuhkan, baik dengan maupun tanpa persetujuan pihak yang bersangkutan. Sebagai mahasiswa yang sedang melaksanakan program magang di kementerian tersebut, kalian mendapat tugas berupa penyadapan percakapan mahasiswa yang diduga melakukan tindak kecurangan dalam kegiatan Praktikum Komunikasi Data dan Jaringan Komputer 2022. Selain itu, terdapat sebuah password rahasia (flag) yang diduga merupakan milik sebuah organisasi bawah tanah yang selama ini tidak sejalan dengan pemerintahan Planet Viltrumite. Tunggu apa lagi, segera kerjakan tugas magang tersebut agar kalian bisa mendapatkan pujian serta kenaikan jabatan di kementerian tersebut!

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.

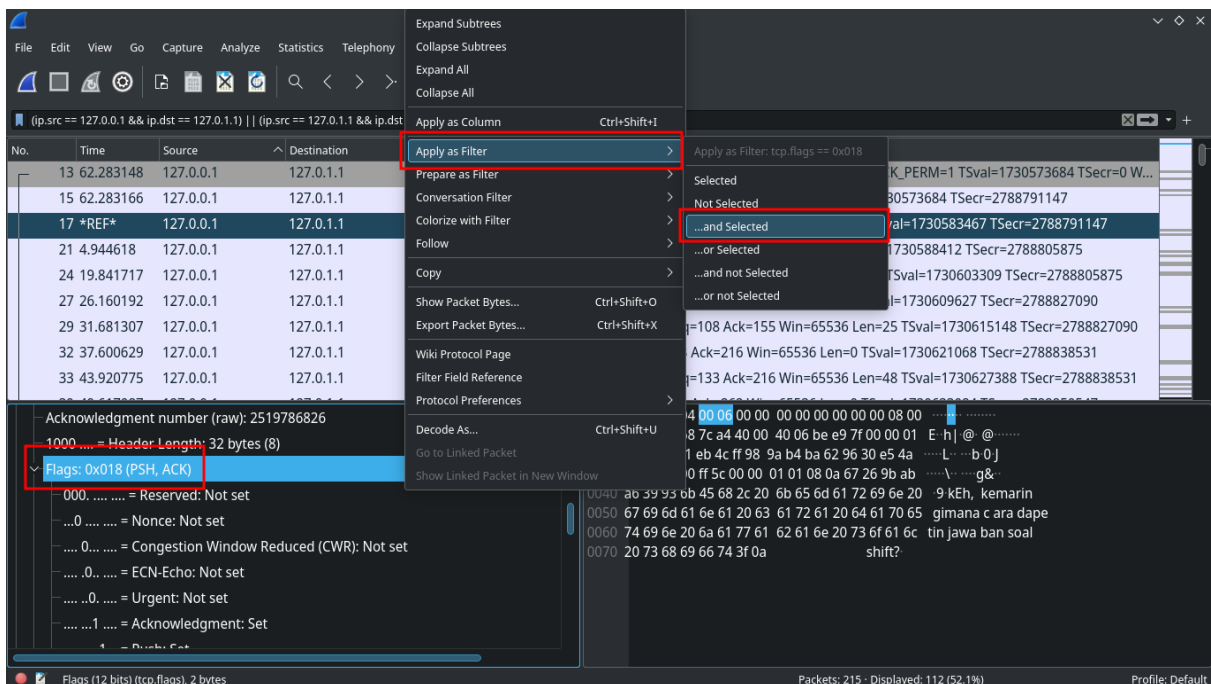
Pertama, cari percakapan di dalam localhost (dari 127.0.0.1 ke 127.0.1.1 dan sebaliknya), dengan display filter:

(ip.src == 127.0.0.1 && ip.dst == 127.0.1.1) || (ip.src == 127.0.1.1 && ip.dst == 127.0.0.1)

dari situ, dapat ditemukan bahwa paket TCP yang mengandung flag PSH berisi pesan komunikasi antara dua mahasiswa tersebut.

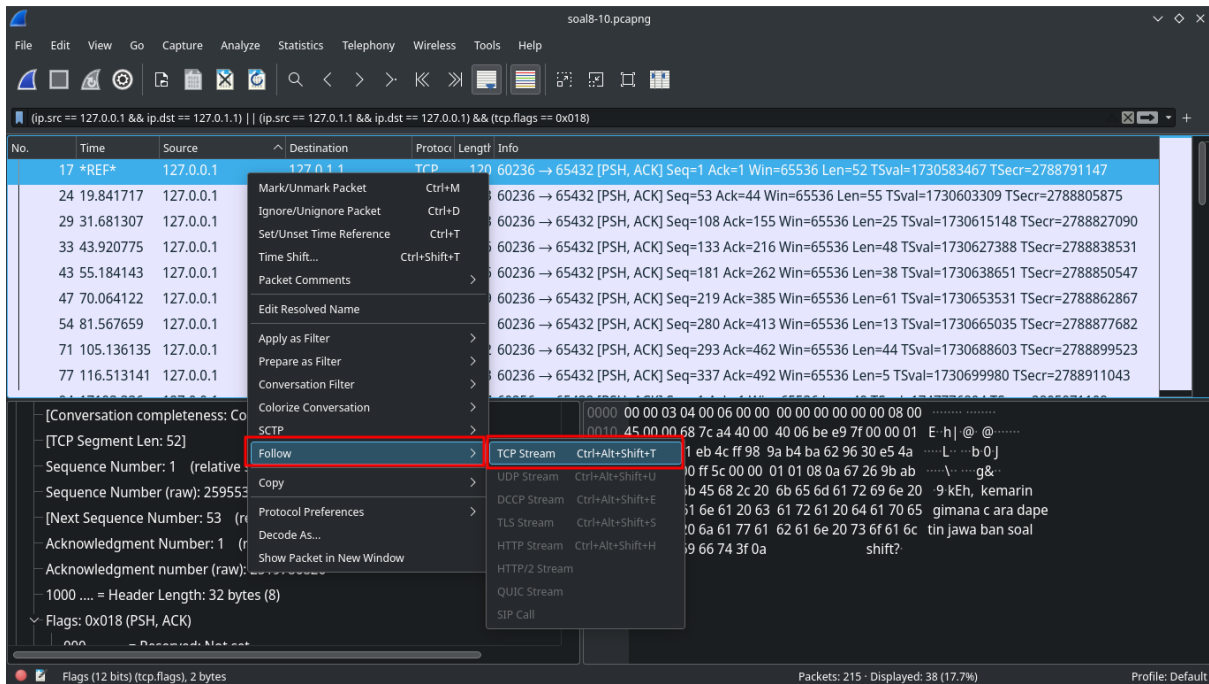


Untuk memfilter agar hanya paket TCP yang terdapat flag PSH-nya saja, kita dapat menuju ke bagian Packet Details -> TCP -> Flags, lalu klik kanan Flags, **Apply as Filter -> ...and Selected**

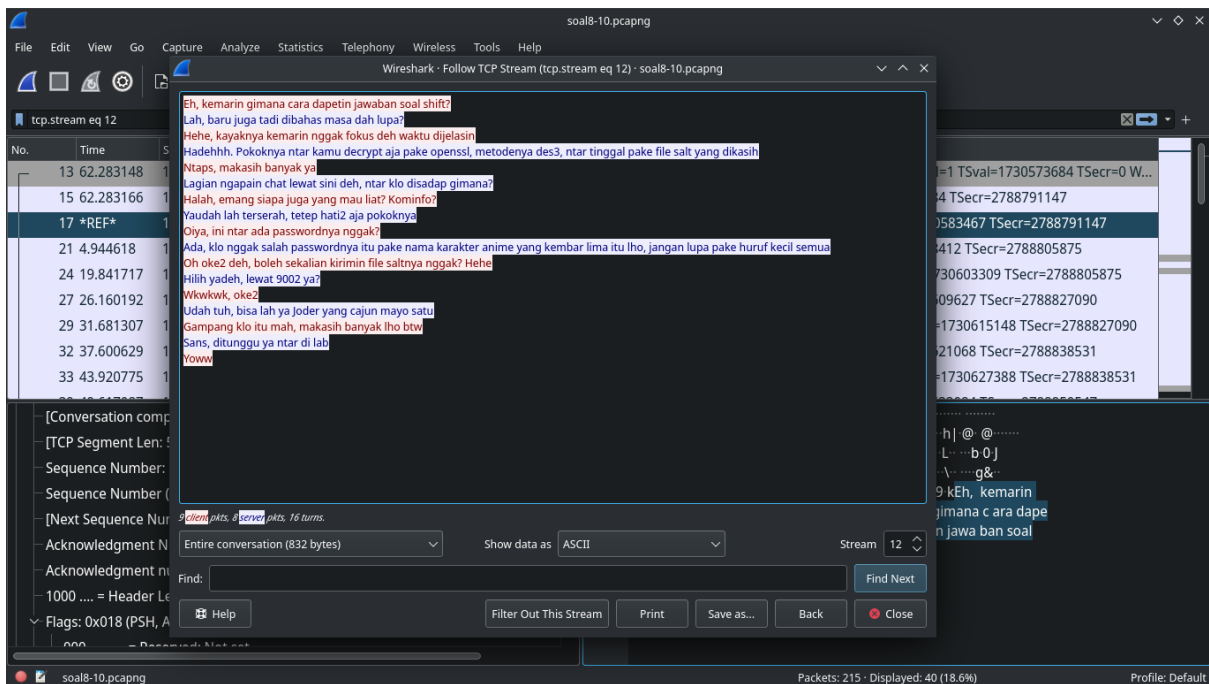


Ini akan menambahkan filter **tcp.flags == 0x018** pada display filter, yang hanya memfilter paket TCP dengan flags [PSH, ACK] saja.

Untuk melihat seluruh percakapannya, kita bisa melihat paket satu per satu lalu lihat pada bagian Packet Bytes, atau klik kanan pada salah satu paket, lalu klik **Follow -> TCP Stream**



yang akan menampilkan dialog sebagai berikut



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.

Jawab:

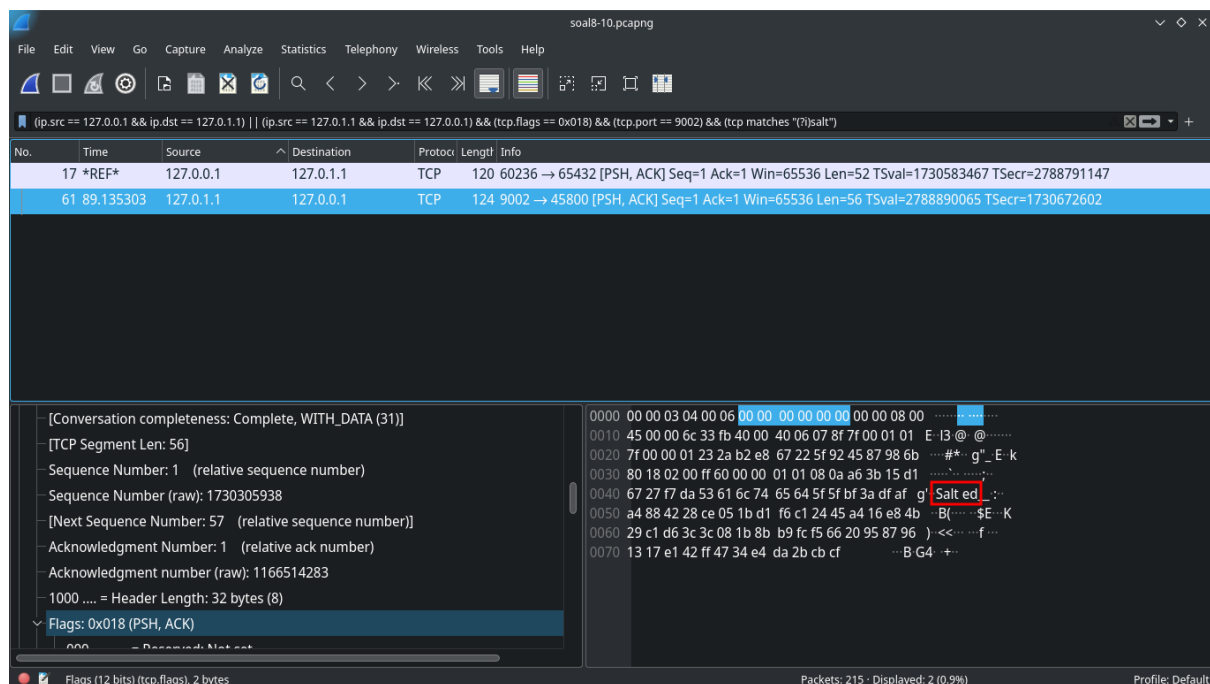
Berdasarkan percakapan kedua orang diatas, dapat diketahui bahwa file salt dikirim menggunakan port 9002. Oleh karena itu, tampilkan file salt yang dikirim

menggunakan port 9002 dengan menambahkan display filter dari nomor 8 dengan **tcp.port == 9002** sehingga seluruh display filternya menjadi:

(ip.src == 127.0.0.1 && ip.dst == 127.0.1.1) || (ip.src == 127.0.1.1 && ip.dst == 127.0.0.1) && (tcp.flags == 0x018) && (tcp.port == 9002)

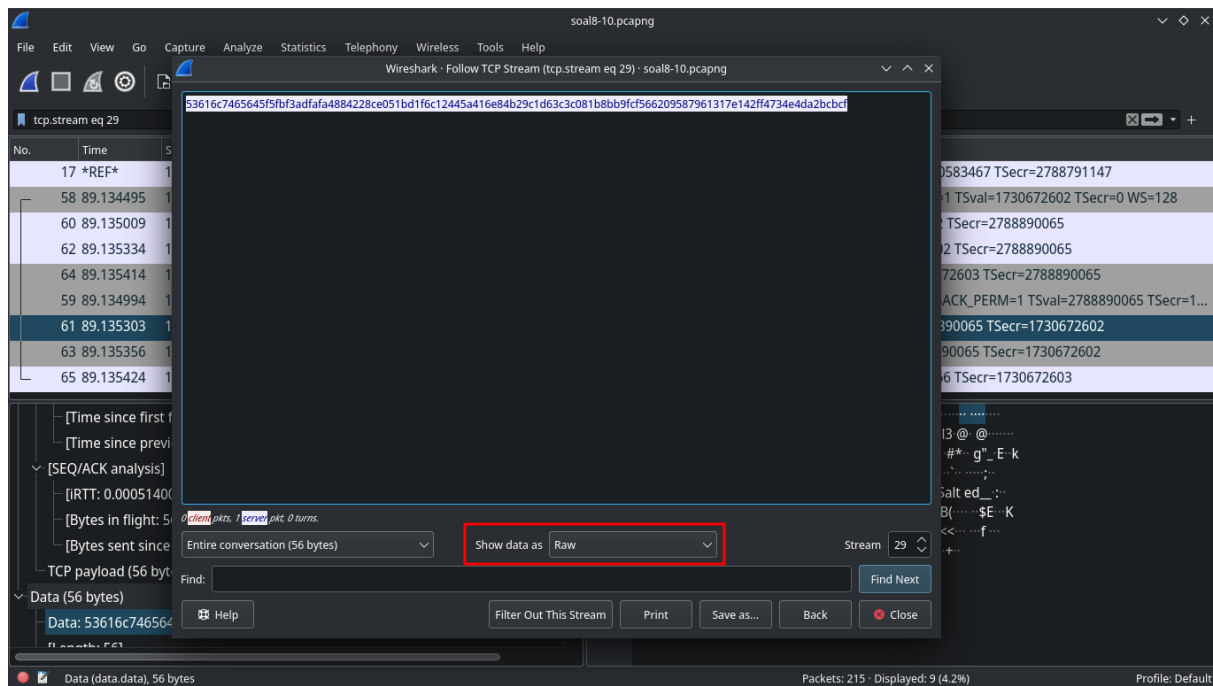
Dari situ, akan ada 4 paket, kita bisa mencari file salt-nya dengan menelusuri satu per satu paket tersebut lalu mencari paket yang berhubungan dengan “salt”, atau kita bisa memfilter paket agar menunjukkan paket yang mengandung “salt” saja yang tampil, dengan cara menambahkan **tcp matches “(?)salt”** pada display filter, syntax **(?)** di sini digunakan agar hasil pencariannya case-insensitive. Seluruh filternya menjadi:

(ip.src == 127.0.0.1 && ip.dst == 127.0.1.1) || (ip.src == 127.0.1.1 && ip.dst == 127.0.0.1) && (tcp.flags == 0x018) && (tcp.port == 9002) && (tcp matches “(?)salt”)



Dari situ, hanya akan ada 1 paket dengan port 9002, dan pada info Packet Bytes-nya terdapat kata “**Salted**”

Untuk mendapatkan file salt-nya, follow TCP Stream paket tersebut, pilih “**Show data as: Raw**”, lalu simpan dengan nama file sesuai soal, yaitu **D06.des3**



Untuk mendekripsi file des3-nya, ikuti arahan dari percakapan tersebut, menggunakan openssl dengan metode des3
openssl des3 -d -in D06.des3 -out flag.txt

Password untuk dekripsinya terdapat pada *clue* di percakapan, yaitu “**nakano**”