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

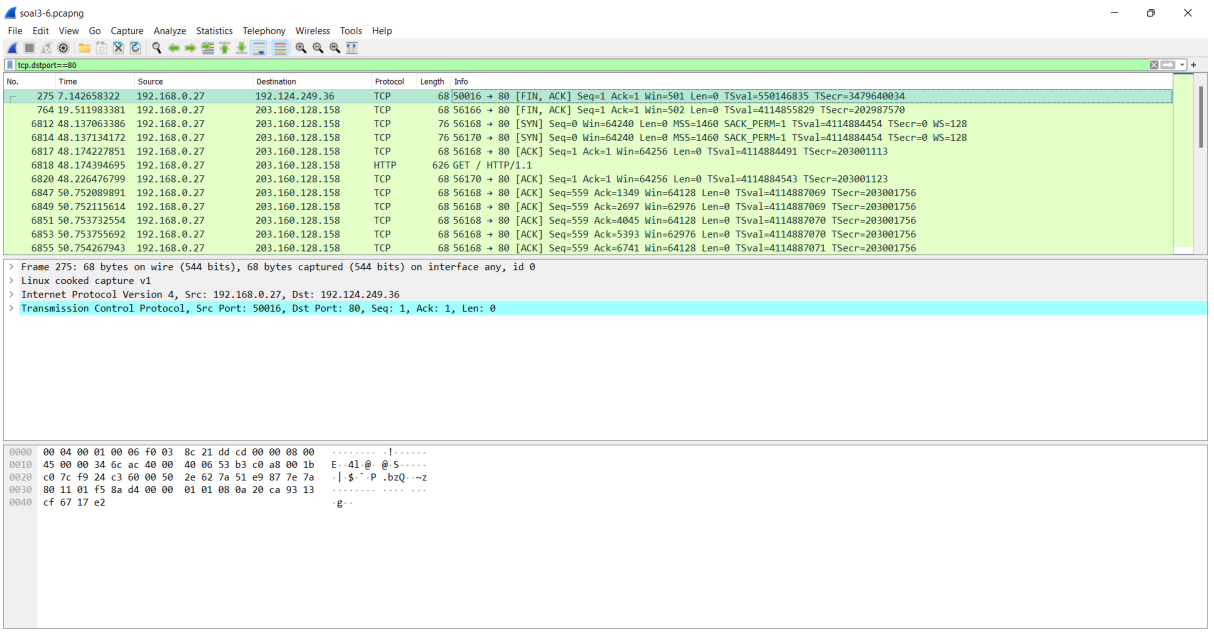
2022/2023

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

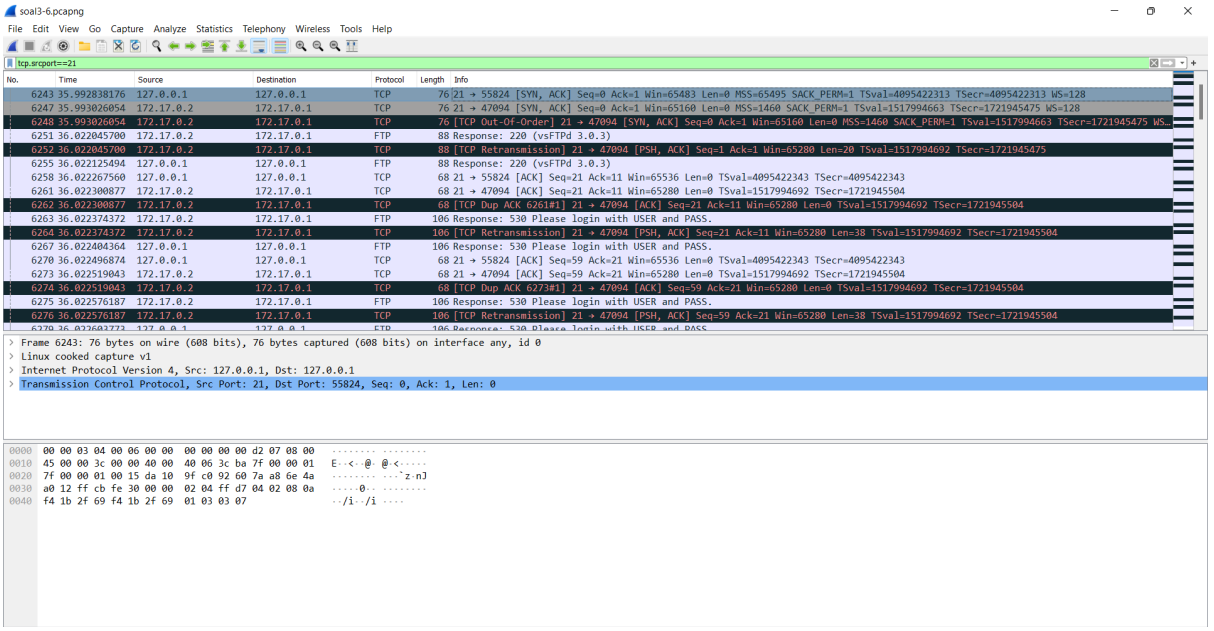


4. Filter sehingga wireshark hanya mengambil paket yang berasal dari port 21!

Jawab:

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

tcp.srcport==21

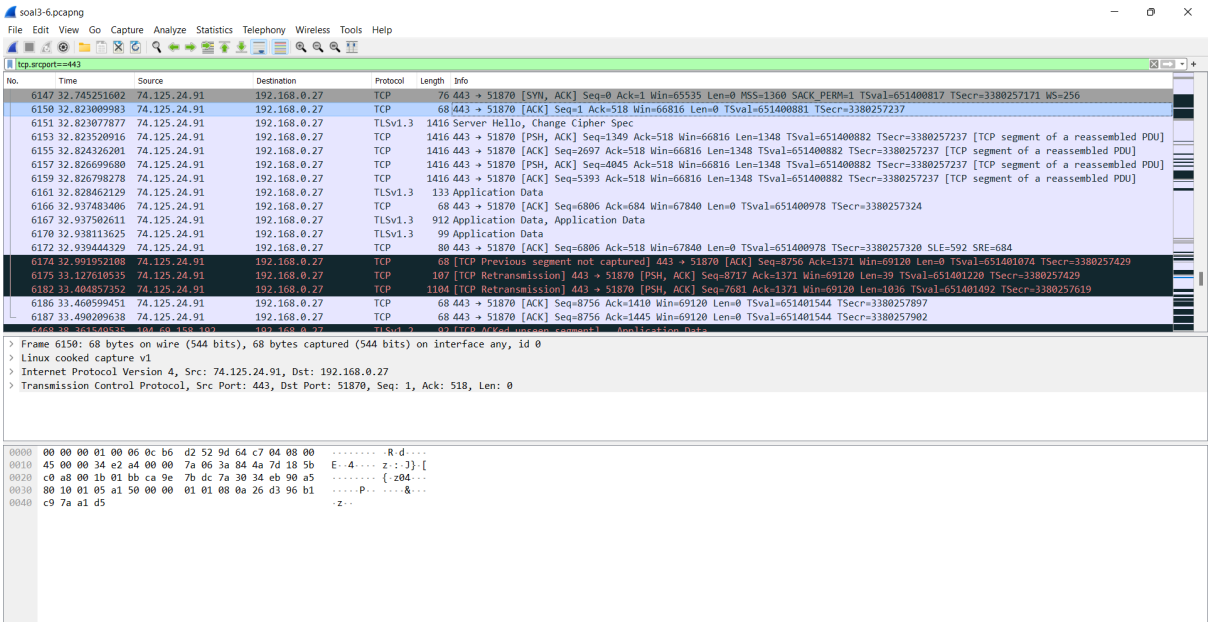


5. Filter sehingga wireshark hanya mengambil paket yang berasal dari port 443!

Jawab:

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

tcp.srcport==443



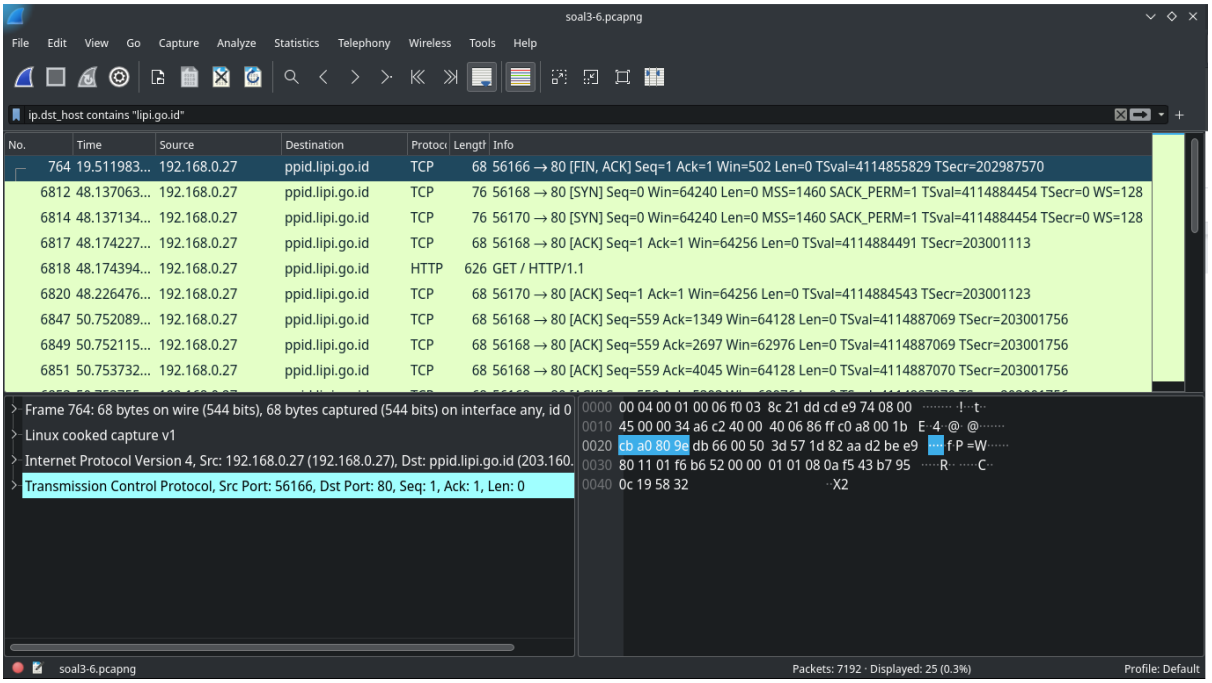
6 .Filter sehingga wireshark hanya menampilkan paket yang menuju ke lipi.go.id !

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"



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

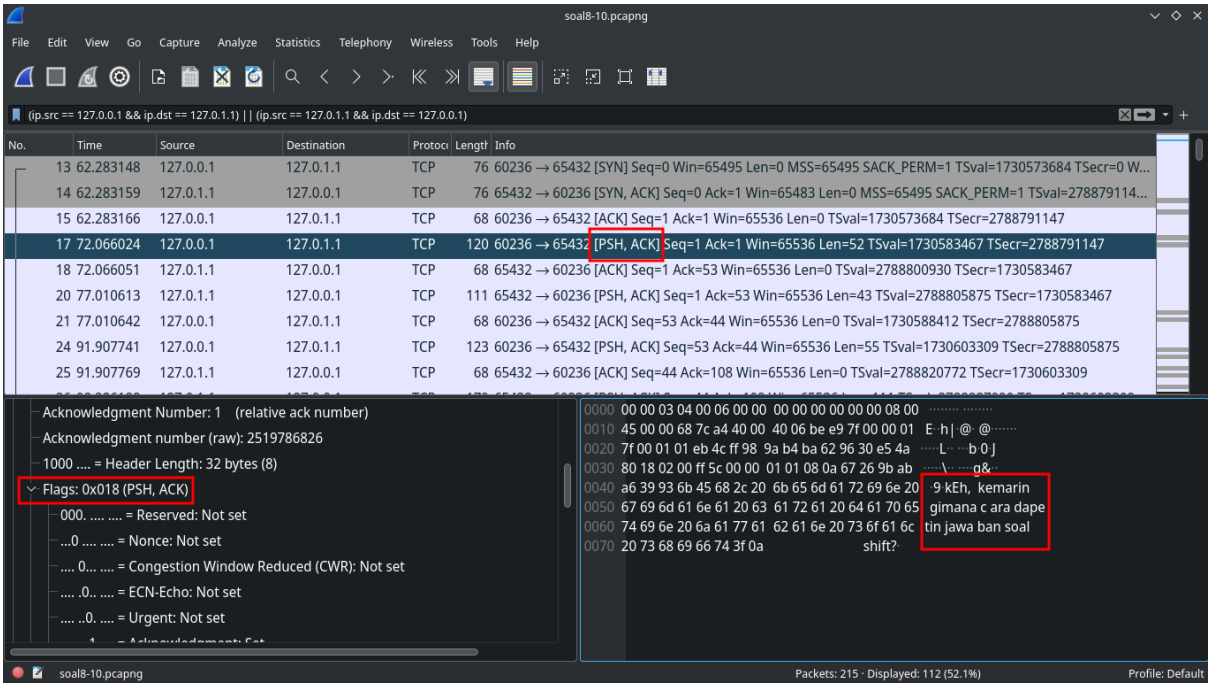
Di sebuah planet bernama Viltrumite, terdapat Kementerian Komunikasi dan Informatika yang baru saja menetapkan kebijakan baru. Dalam kebijakan baru tersebut, pemerintah dapat mengakses data pribadi masyarakat secara bebas jika memang dibutuhkan, baik dengan maupun tanpa persetujuan pihak yang bersangkutan. 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.

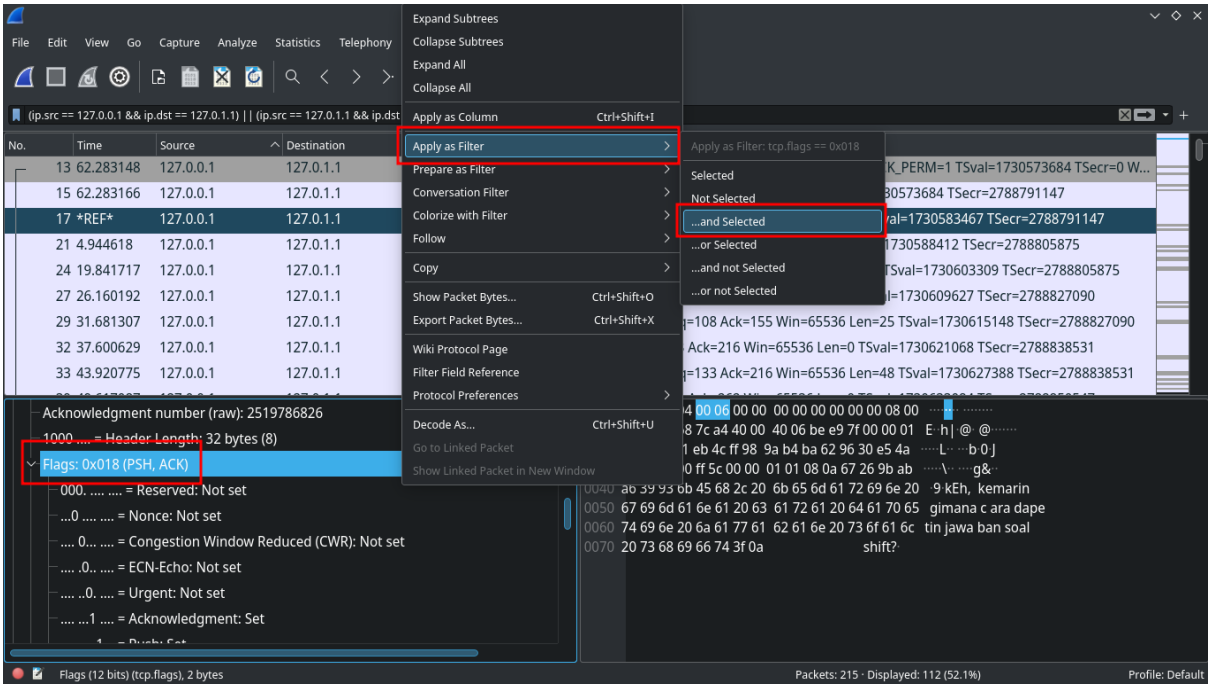
Pertama, cari percakapan di dalam localhost (dari 127.0.0.1 ke 127.0.1.1 dan sebaliknya), dengan display filter:

(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.

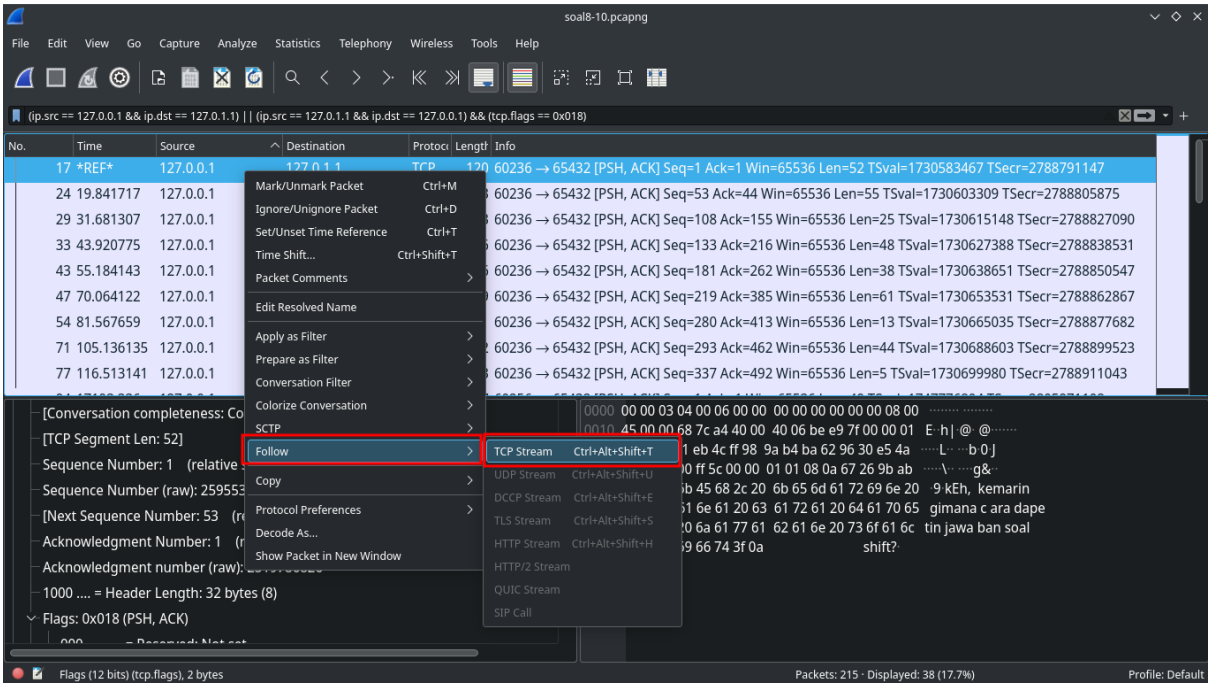


Untuk memfilter agar hanya paket TCP yang terdapat flag PSH-nya saja, kita dapat menuju ke bagian Packet Details -> TCP -> Flags, lalu klik kanan Flags, **Apply as Filter -> …and Selected**

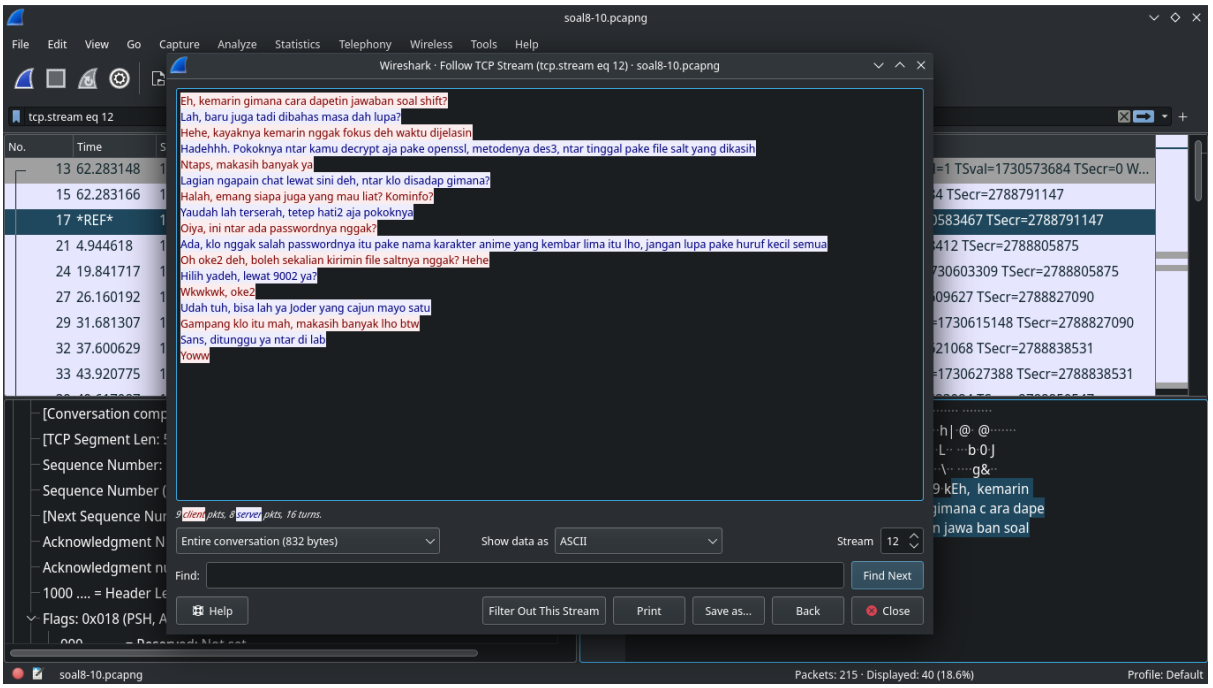


Ini akan menambahkan filter **tcp.flags == 0x018** pada display filter, yang hanya memfilter paket TCP dengan flags [PSH, ACK] saja.

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:

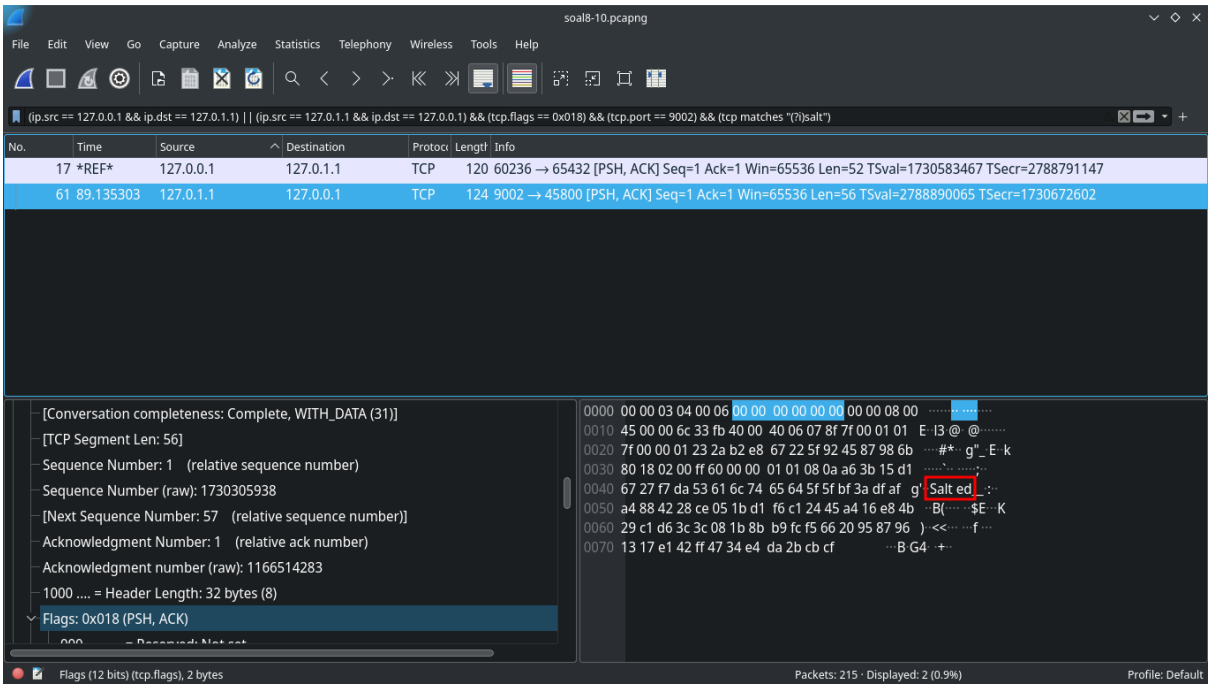
Berdasarkan percakapan kedua orang diatas, dapat diketahui bahwa file salt dikirim menggunakan `port 9002`. Oleh karena itu, tampilkan file salt yang dikirim

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

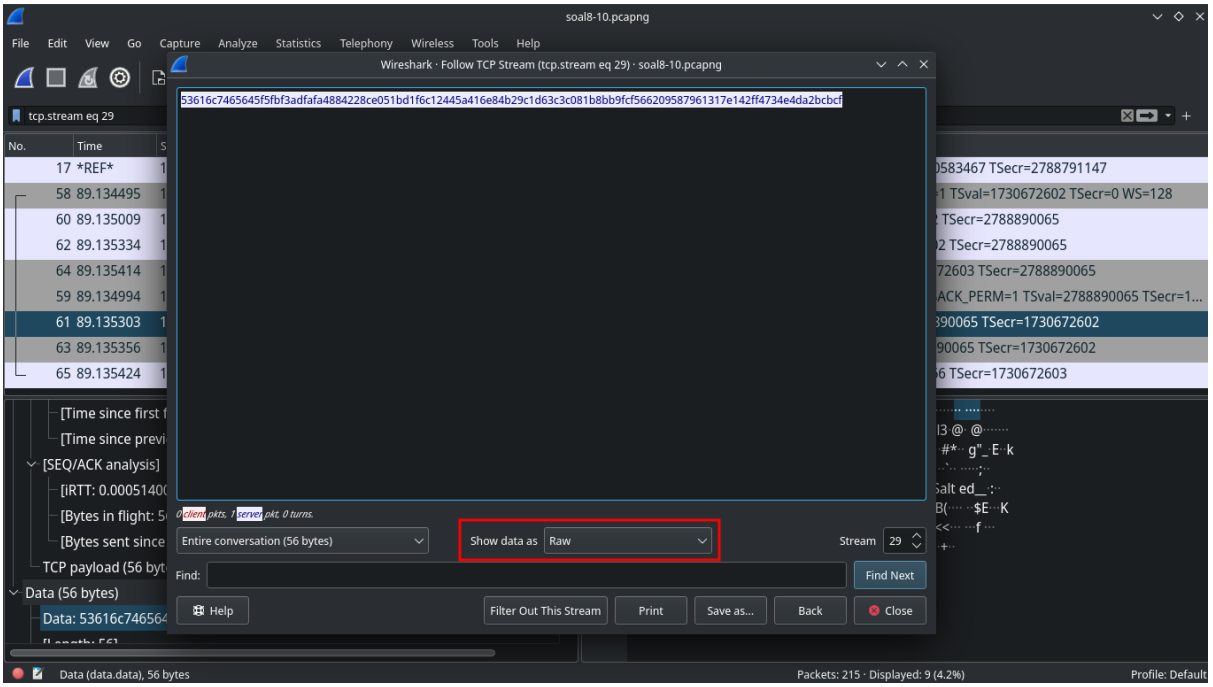
(ip.src == 127.0.0.1 && ip.dst == 127.0.1.1) || (ip.src == 127.0.1.1 && ip.dst == 127.0.0.1) && (tcp.flags == 0x018) && (tcp.port == 9002)

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 “(?i)salt**” pada display filter, syntax **(?i)** 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 "(?i)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”**