Computer Networks Project 2

## Shirin Behnaminia 9919863

## Narges Montazeri 9931053

# Part 1:

## 1-1:

زمانی که ما سوکتمون رو ساختیم از دستور زیر استفاده کردیم:

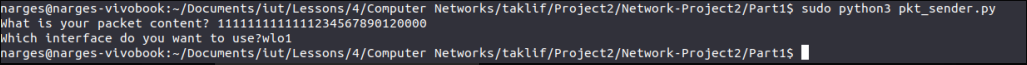
s = socket(AF\_PACKET, SOCK\_RAW)

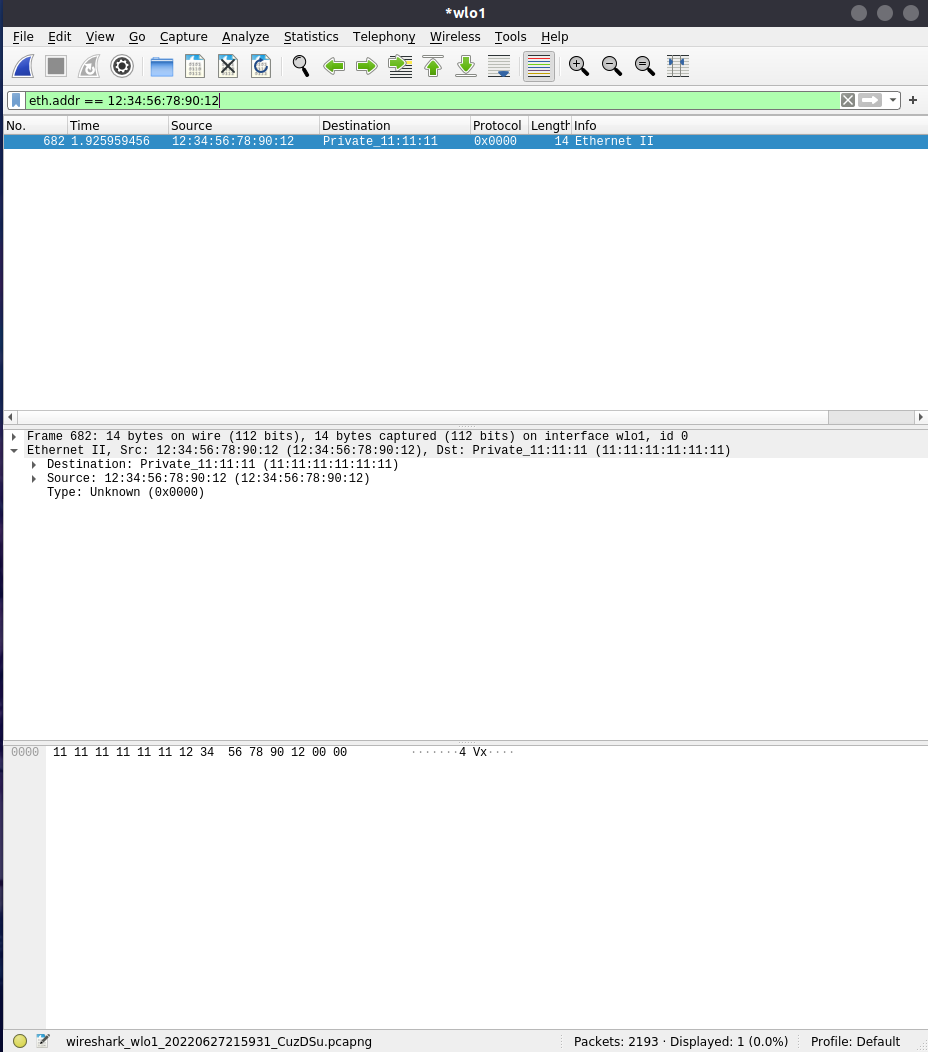
این تایپ از سوکت SOCK\_RAW به ما اجازه میدهد که مستقیما در لایه ی ip یا ethernet قرار بگیریم و بسته ها را ارسال کنیم. در نتیجه حداقل طولی که لازمه یه بسته داشته باشه 14 بایته و کمتر از اون رو ارور میده. چون اگر یه مسیج رندوم به این سوکت بدیم تا منتقل کنه خودش میاد 14 بایت اول رو به عنوان ethernet header در نظر میگیره.(طول هدر اترنت 14 بایته)

## 1-2:

بسته مون باید هدر اترنتش هدر ولیدی باشه. در نتیجه با توجه به نحوه ورودی گرفتن ما که یک رشته هگزادسیمال ورودی میگیره باید به تعداد زوج تا کاراکتر و حداقل 28 تا کاراکتر وارد کنیم که هر کاراکتر عددی بین 0 تا 9 یا حرفی بین a تا f است. اینکه قسمت type عدد ولیدی درنیاد مهم نیس چون وایرشارک میشناسه پکتو فقط type اش unknown در نظر گرفته میشه.

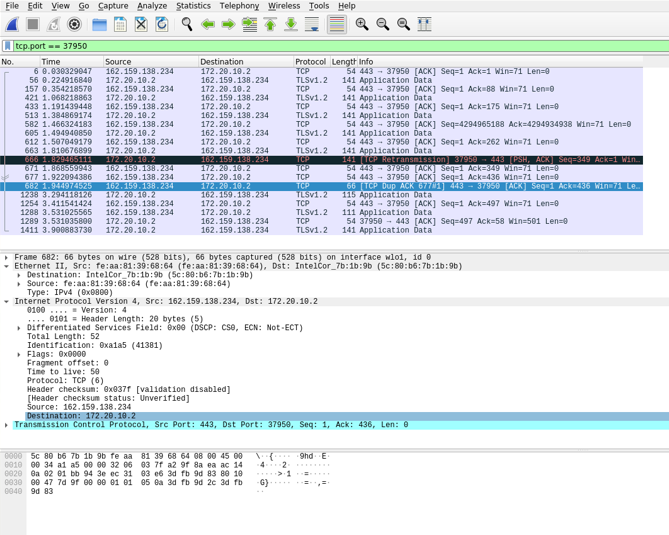
## 1-3:





## 1-4:





پکتی که به عنوان duplicated ack شناخته شده پکتیه که ما مجددا با همون seq num و ack num فرستادیم به همین دلیل dup ack در نظر گرفته شده.

## 1-5:

در این حمله، فرد هکر با شیوه های مختلف ip spoofing و sniff کردن پکت ها به محتوای ریکوستی که فرضا A برای web server میفرستد دست پیدا میکند و بدون اینکه نیاز باشد محتوای ان را بخواند یا رمزگشایی کند ان را برای سرور retransmit(replay) میکند. این موضوع باعث میشور سرور به اشتباه بیفتد و تصور کند پیام از سمت شخص A است که مثلا قصد داره دوباره لاگین کند. در نتیجه دیتا را برای فرد هکر میفرستد.

کاری که ما در سوال قبل انجام دادیم به نوعی یجور replay attack بود.

# Part 2:

## 2-1:

# Part 3:

## 3-1:

14 Bytes

## 3-2:

14 Bytes 😐

## 3-3:

با چک کردن فلک های SYN , ACK در هدر tcp بسته ی موردنظر

## 3-4:

# Part 4: