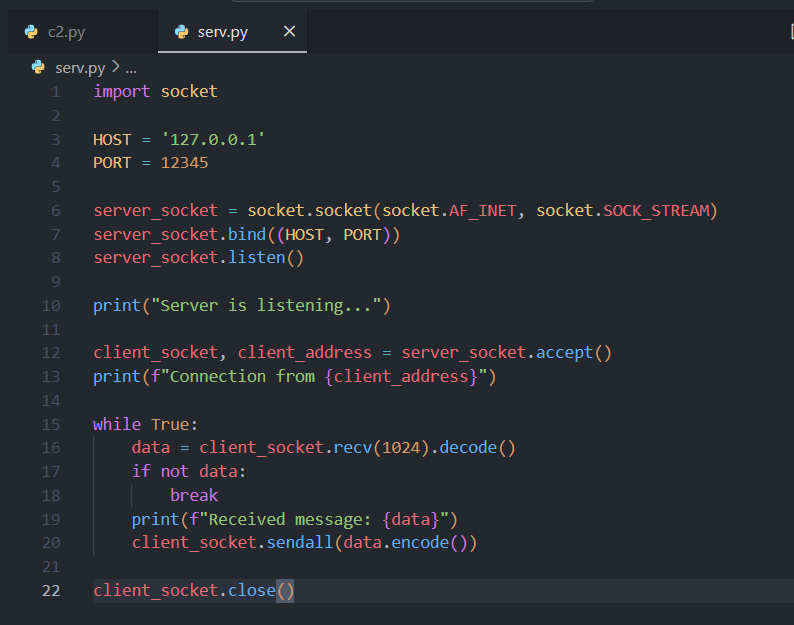
**تکلیف : داکیومنت آزمایش 2**

**نام و نام خانوادگی:فاطمه یوسفی**

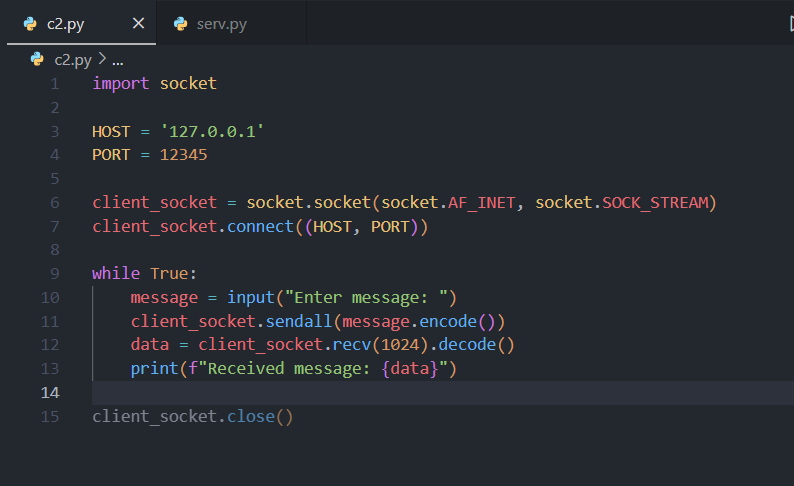
**شماره دانشجویی:9912762212**

1. تعریف سناریو:

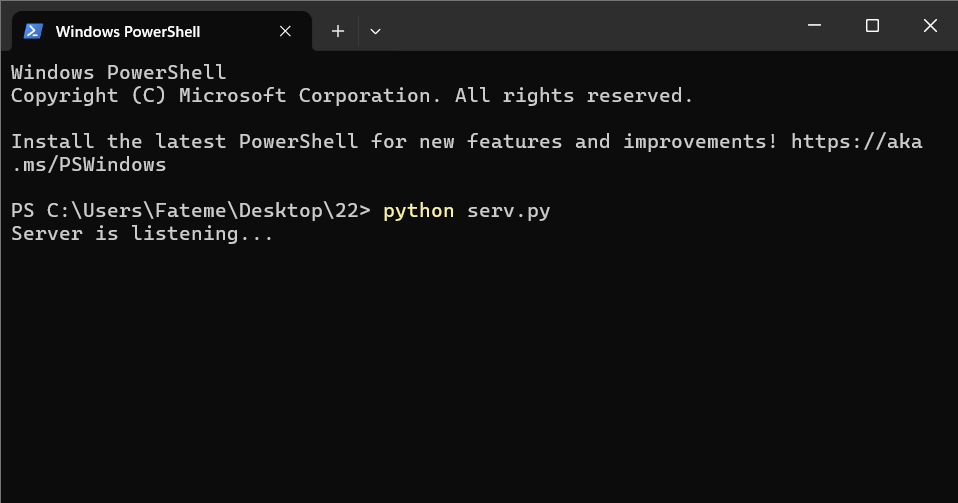
در ابتدا دو سوکت ایجاد میکنیم و بعد پیام ارسال میکنیم در وایرشاک بخش دیتا میتوان دید که پیام بدون رمز هست و این اشکال امنیتی cryptography failureهست بنابراین باید پیام را رمز کنیم.

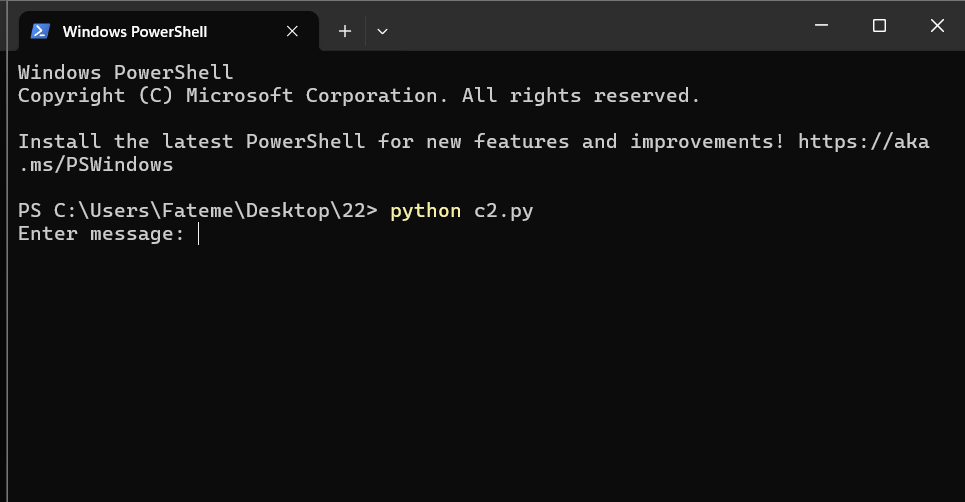


کد بالا، کد سرور من هست.

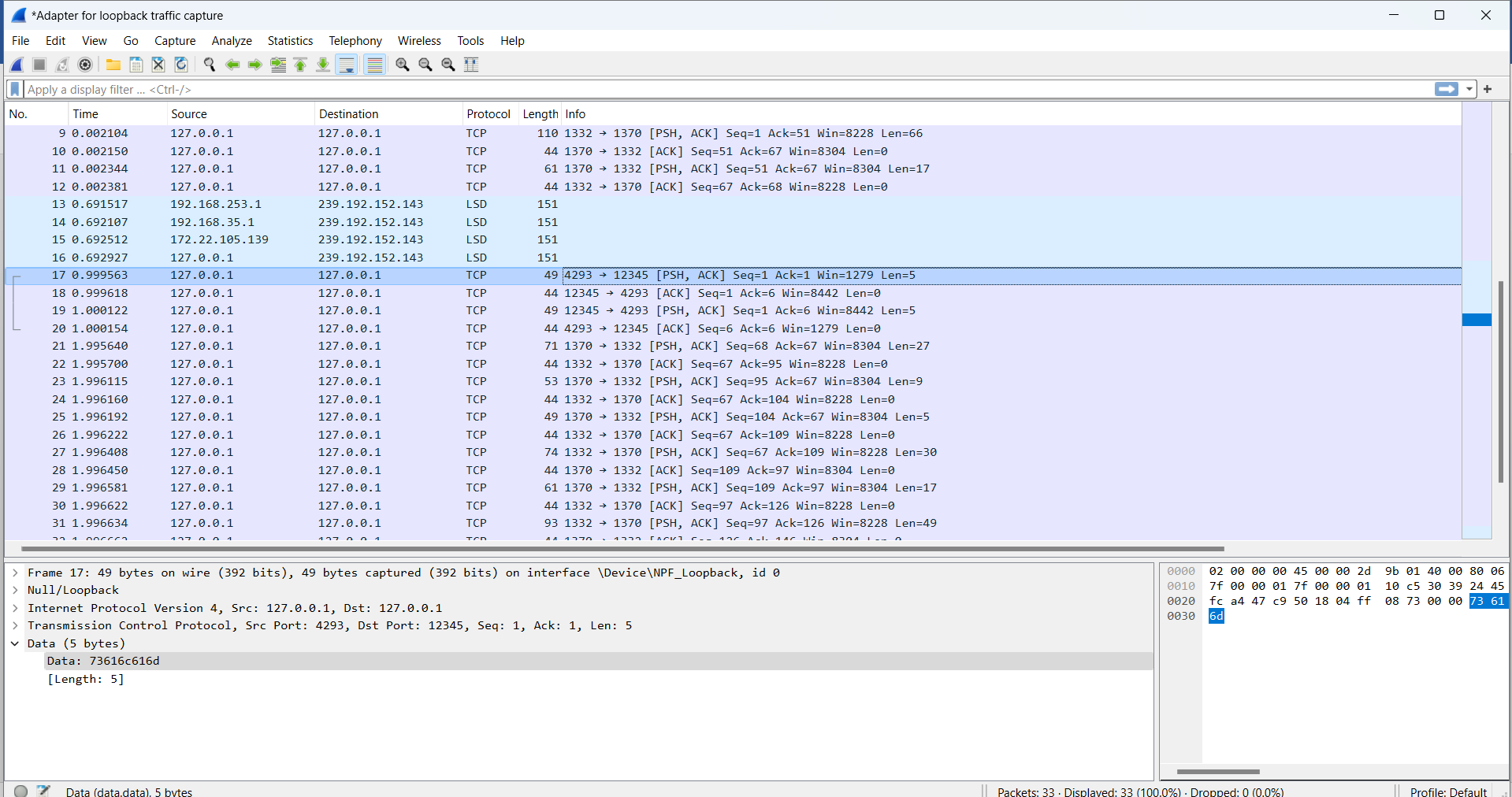


و این نیز کد کلاینت است.

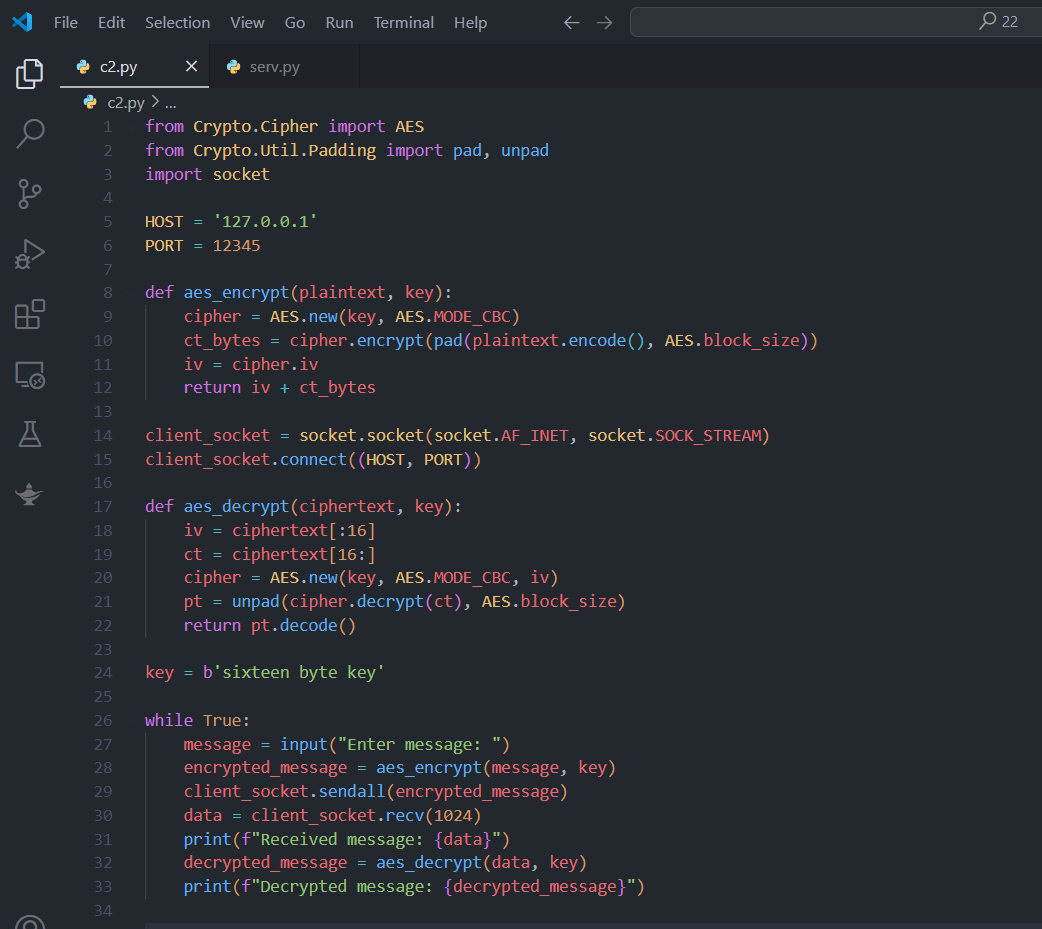


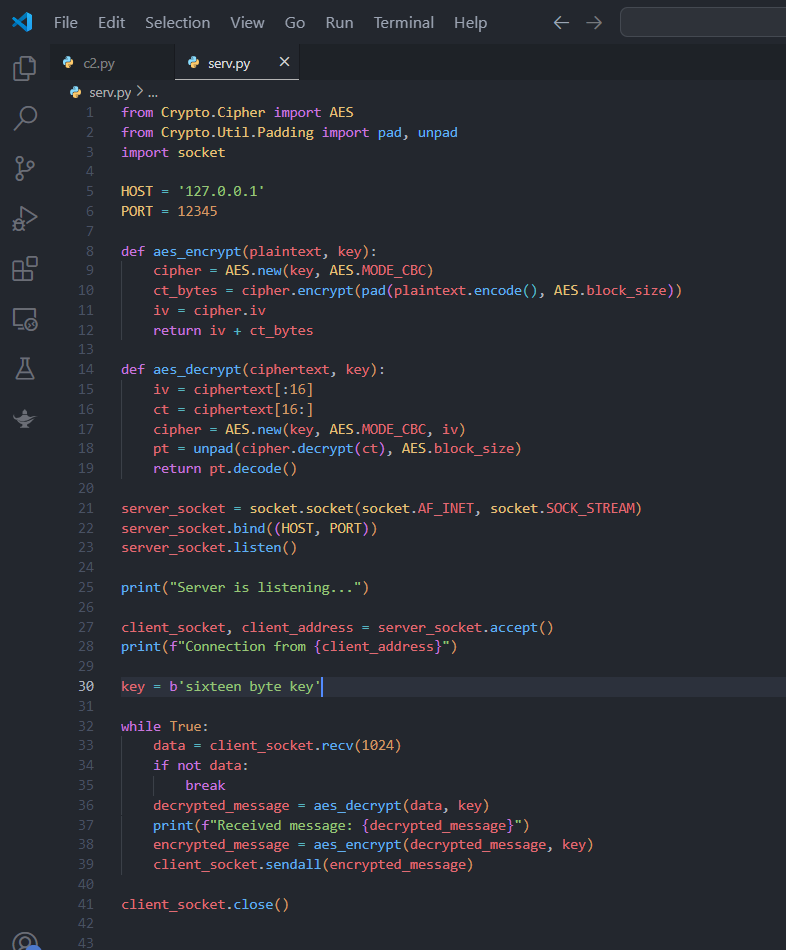


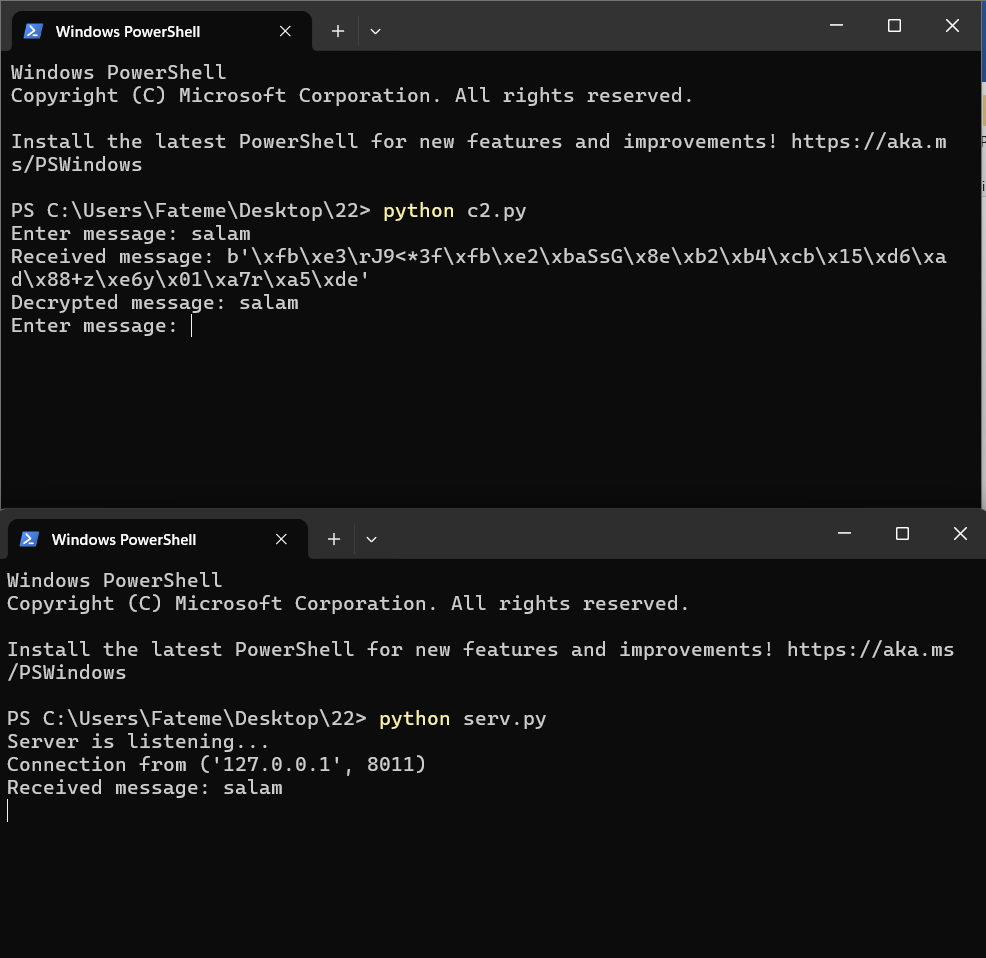


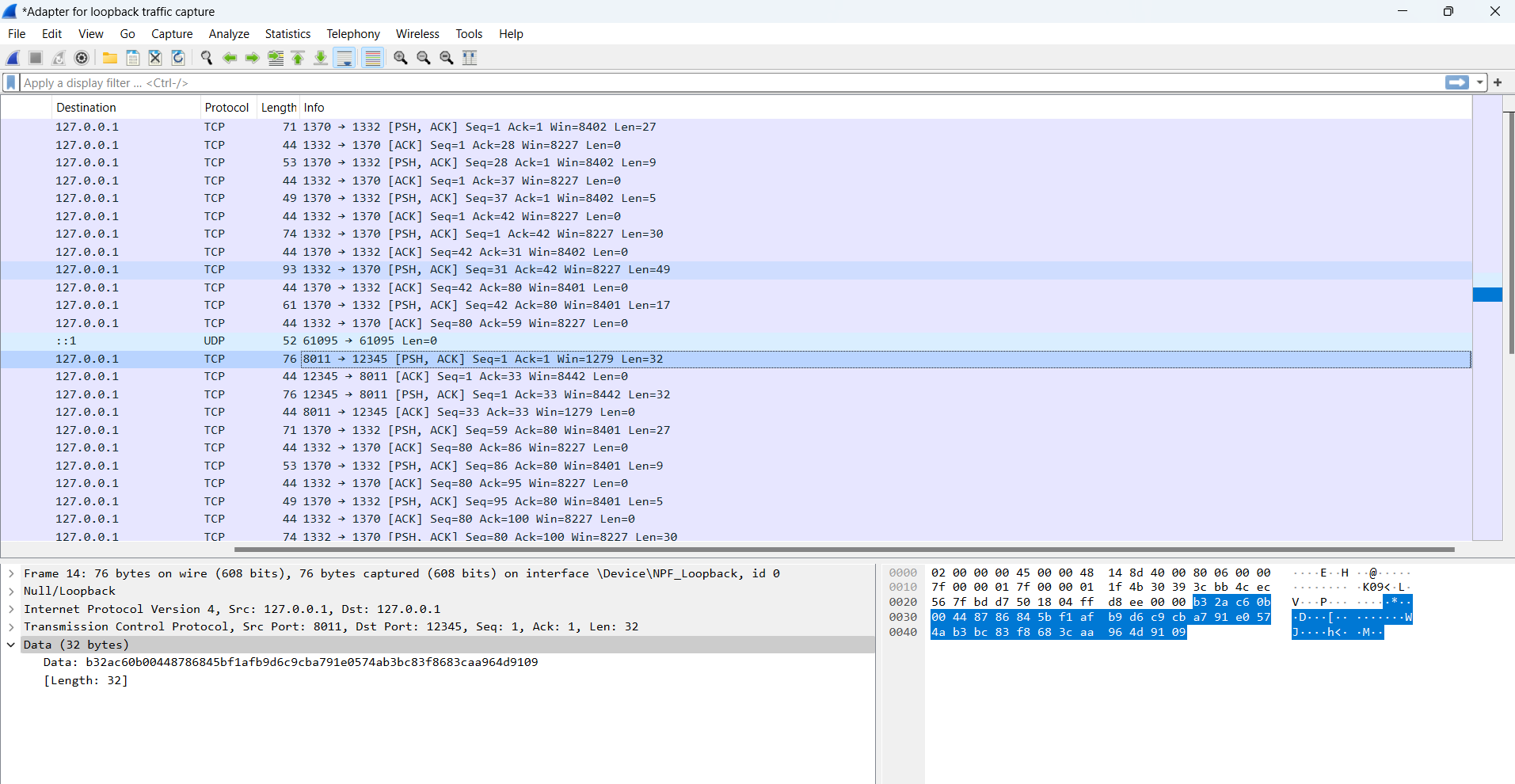


پیام به صورت غیر رمز شده است.









در واقع بستر این سناریو یک سرور سوکت با آدرس آی پی 127.0.0.1 روی پورت 12345 داریم و کلاینت به این سرور وصل میشود و پیام ارسال میکند.

طبق اسکرین شات های بالا یکی از مشکلات رمز نشدن داده هست که باعث میشود نفر سومی بتواند به راحتی مکالمه را ببیند و این باعث ناامنی ارتباط میشود.

راهکار: رمز نگاری داده قبل از ارسال با استفاده از الگوریتم رمزنگاری AES سبب میشود که نفر سوم داده ها را به صورت رمز شده ببیند و بنابراین ارتباط در بستری امن انجام گردد.