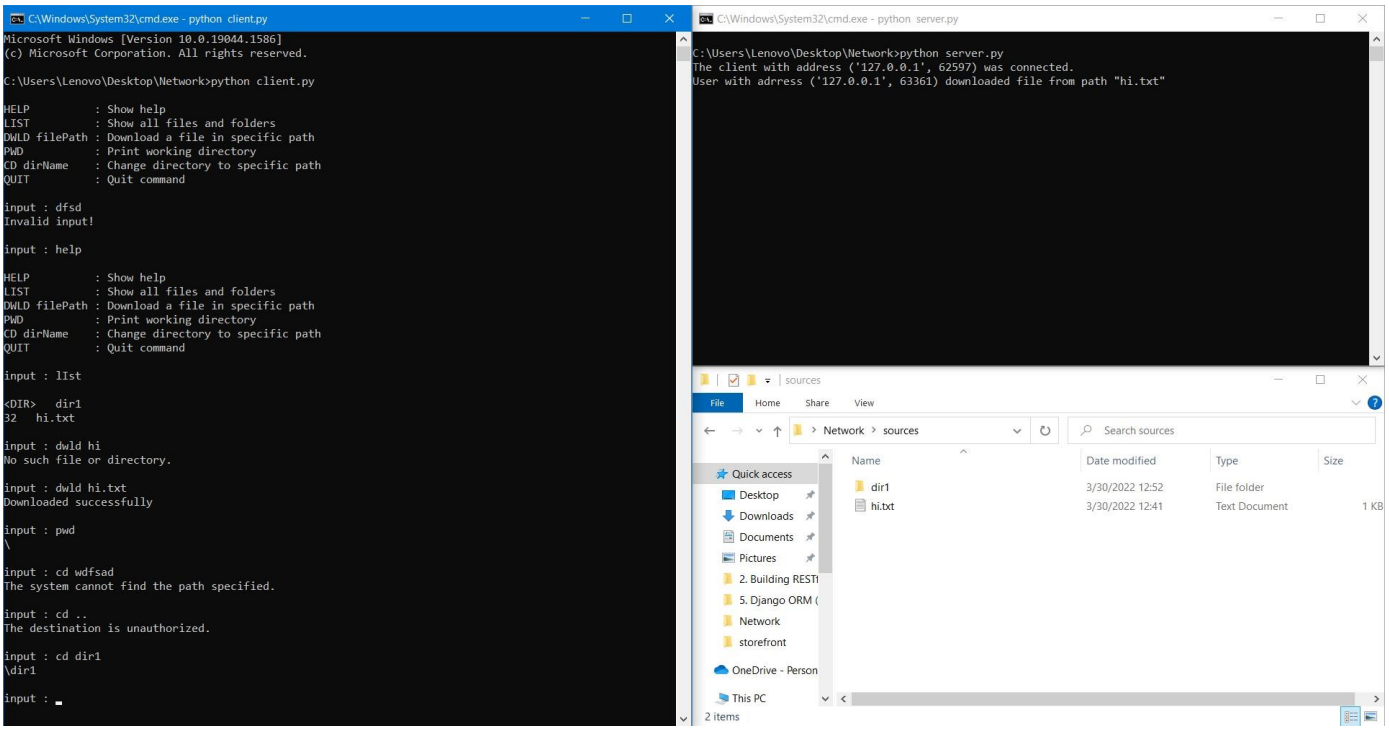
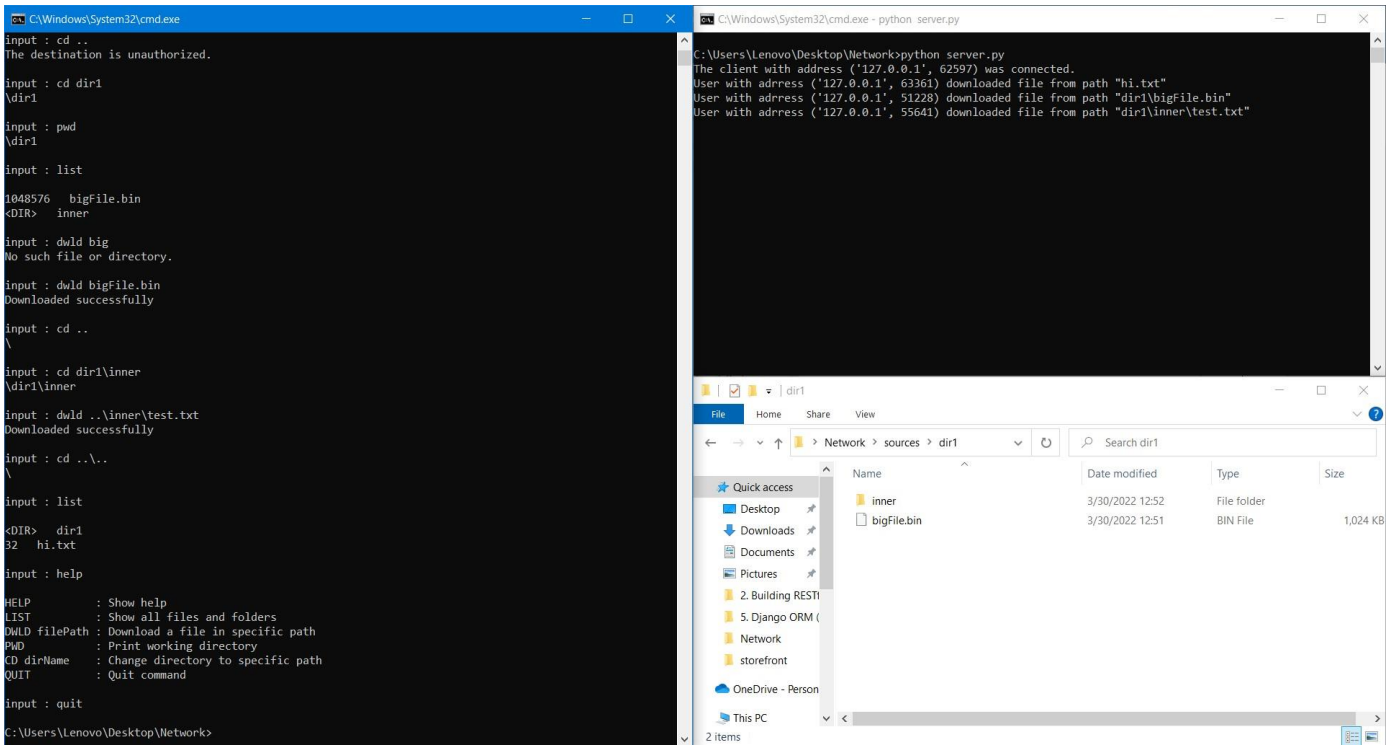
۱) چون معمولا Client در پشت Firewall یا Nat است پس نمیتواند برای خودش پورت جدیدی باز کند، اما میتواند با دستگاه دیگری ارتباط برقرار کند. بدین سبب Server یک پورت رندوم باز کرده و در Control channel آن پورت را به Client گزارش میدهد و از این طریق Client به پورت گزارش شده ی سرور، متصل میشود.

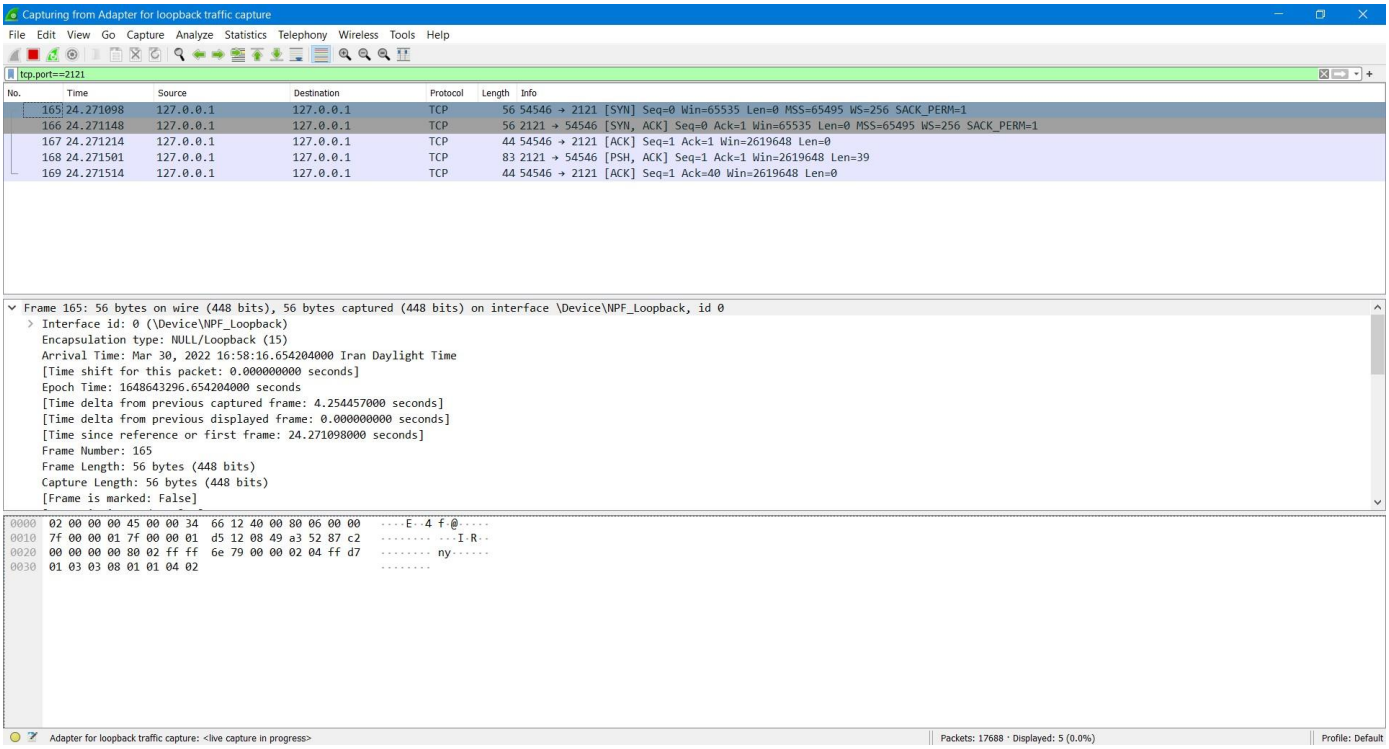
۲) تصاویر مربوط به ران کردن کلاینت و سرور

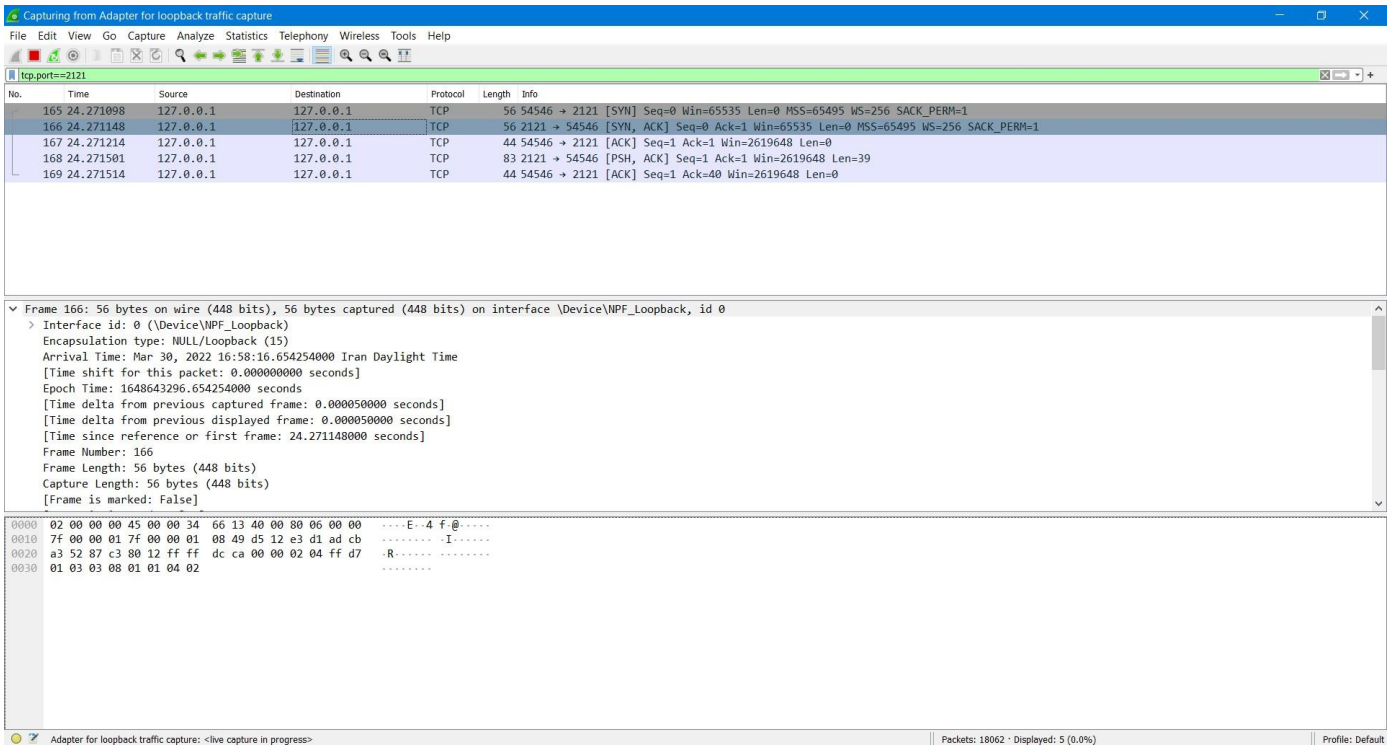


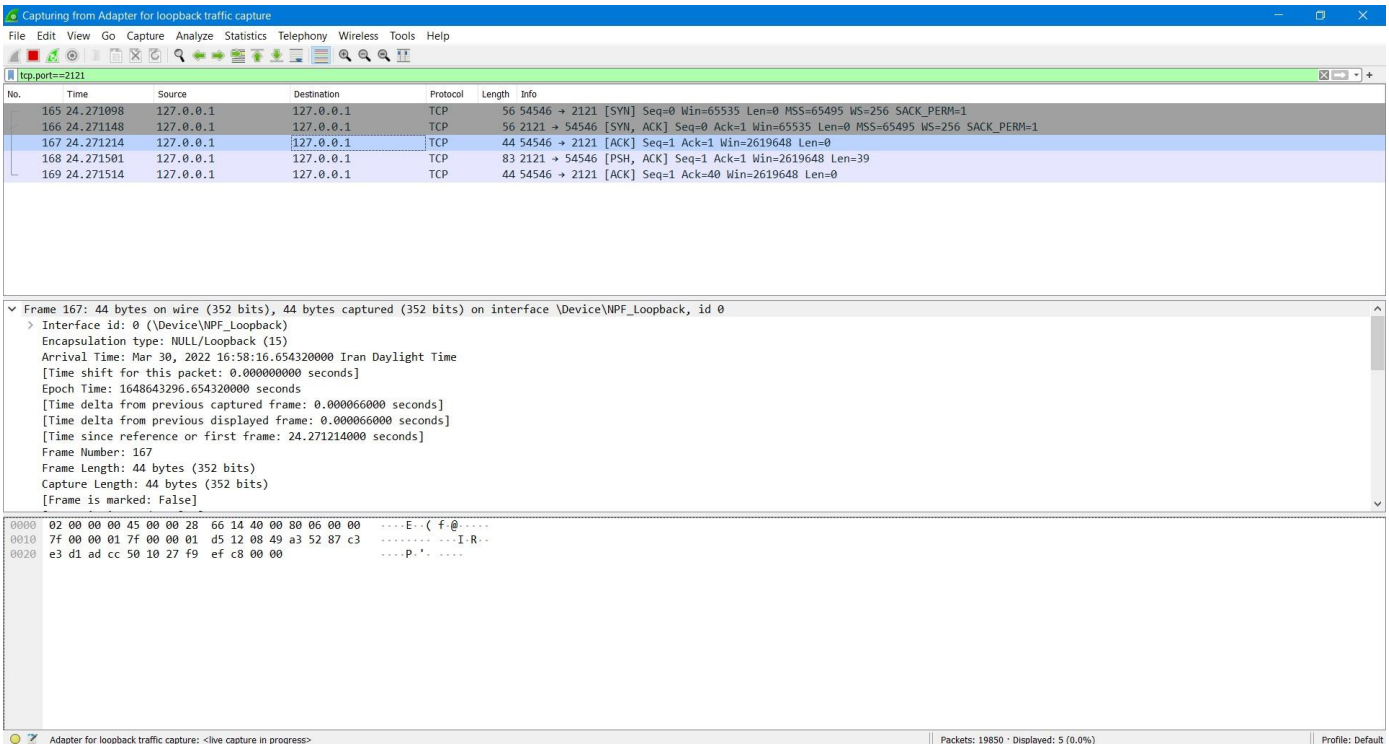


نام حمله ای که مهاجم به فایل‌های سیستم دسترسی پیدا میکند، به Dot Dot Slash یا Directory Traversal و یا Directory Climbing مشهور است و طی این حمله، مهاجم میتواند به اطلاعات کامپیوتر قربانی دست پیدا کند.

۴) سه عکس مربوط به handshaking

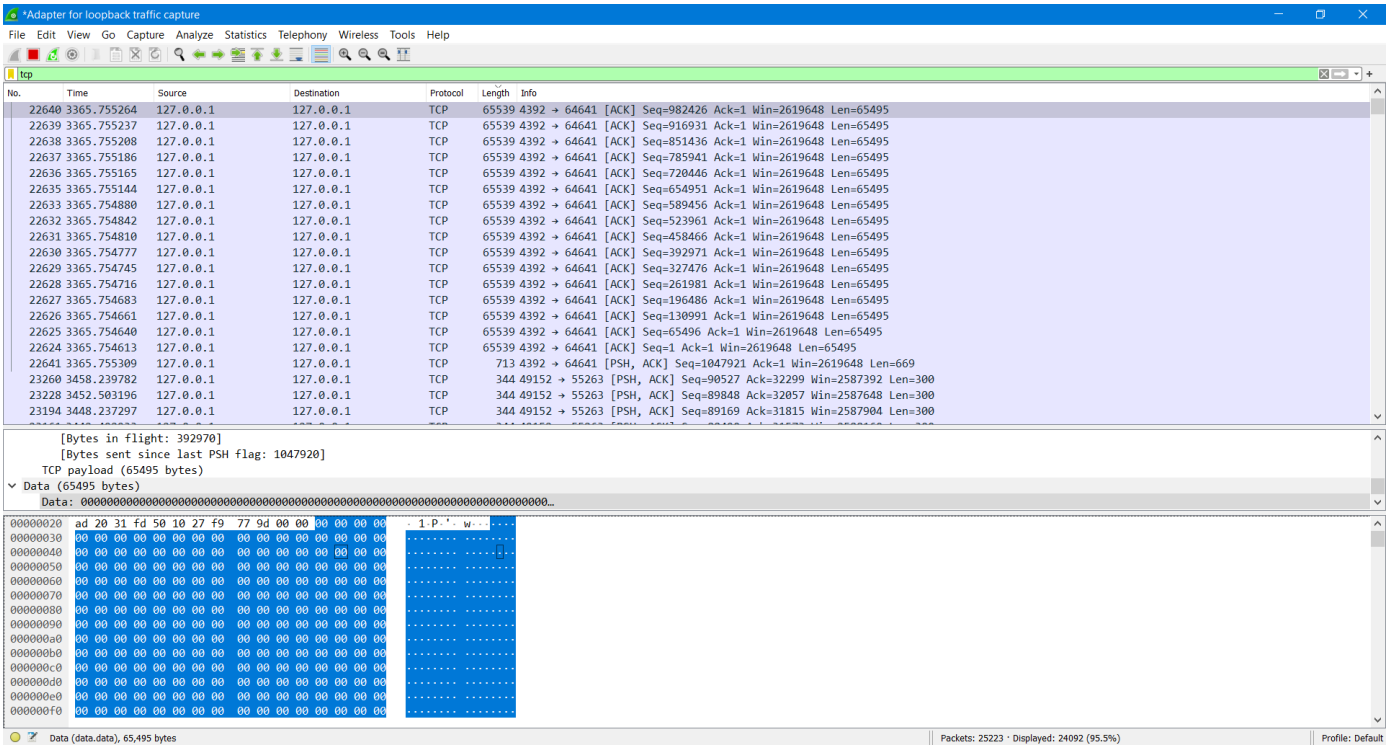




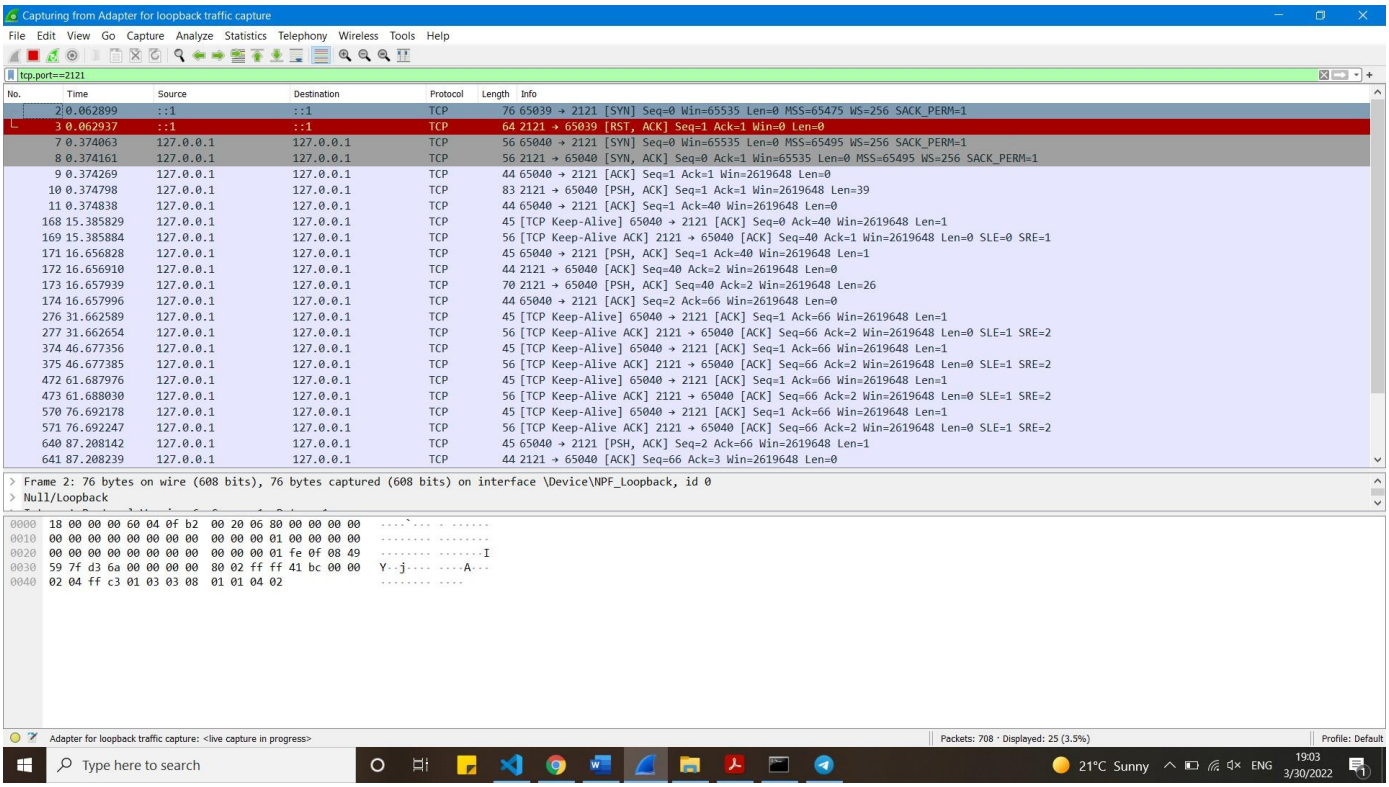


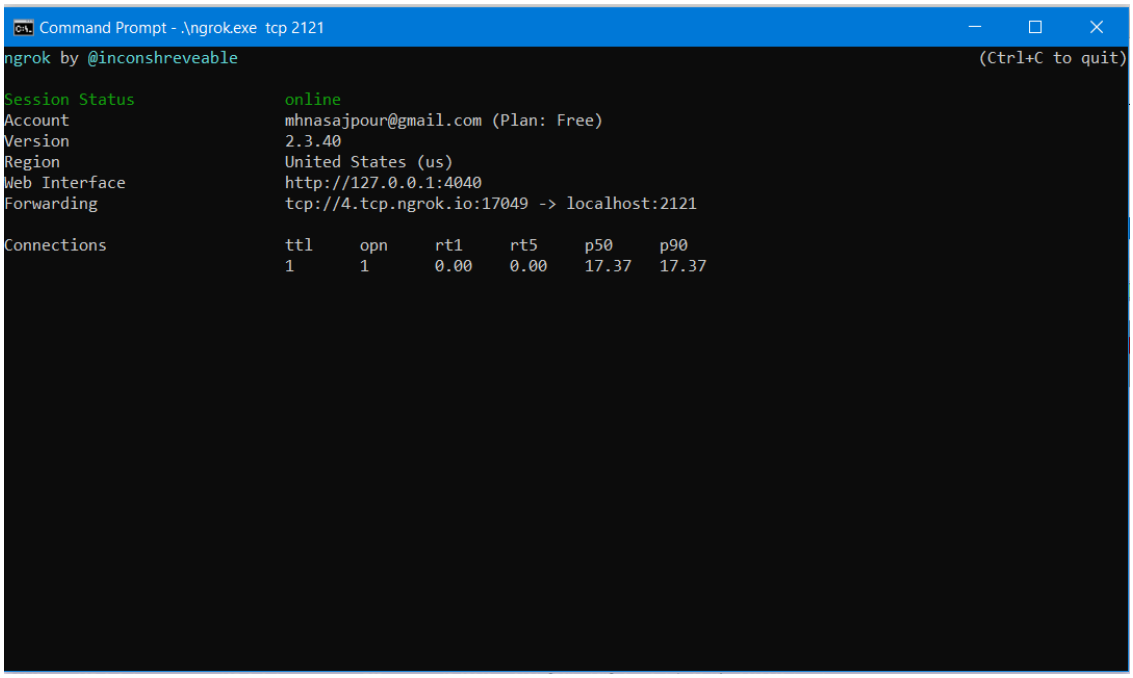
۵-الف) بله. بیشینه سایزی که TCP در بسته ها میتواند انتقال دهد برابر ۶۵۵۳۹ بایت یعنی ۶۴ کیلوبایت است.

۵-ب) طبق عکس، TCP برای این عمل ۱۶ بسته به حجم ۶۵۵۳۹ بایت فرستاده است .



۶) کار با ngrok





۷) زمانی که از ngrok استفاده میکنیم دستورات ابتدا از بستر اینترنت به سرورهای آن رفته و سپس به کامپیوتر می‌آید. اما اگر از ngrok استفاده نکنیم، دستورات در همین کامپیوتر فرستاده میشوند و به سرورها فرستاده نمیشوند.

با این مکانیزم و با ngrok نمیتوانم فایلی ارسال کنیم. در مکانیزم انتقال فایل ابتدا سرور پورت جدیدی باز میکند و آنرا به کلاینت اطلاع میدهد. اما در این بین ngrok پورت خود را تعویض نمیکند و کانال داده و کانال کنترل دچار کانفیلیکت میشوند.

برای حل این مشکل میتوان از یک پورت کانستنت به جای رندوم اسفاده کرد که این راه نیز مشکلاتی از جمله پاسخ دهی به کلاینت ها را در بر دارد.