# به نام خدا

پروژه اول شبکه‌های کامپیوتری(پروتکل FTP)

محمد یاسین کرباسیان ft علیرضا میرحسینی

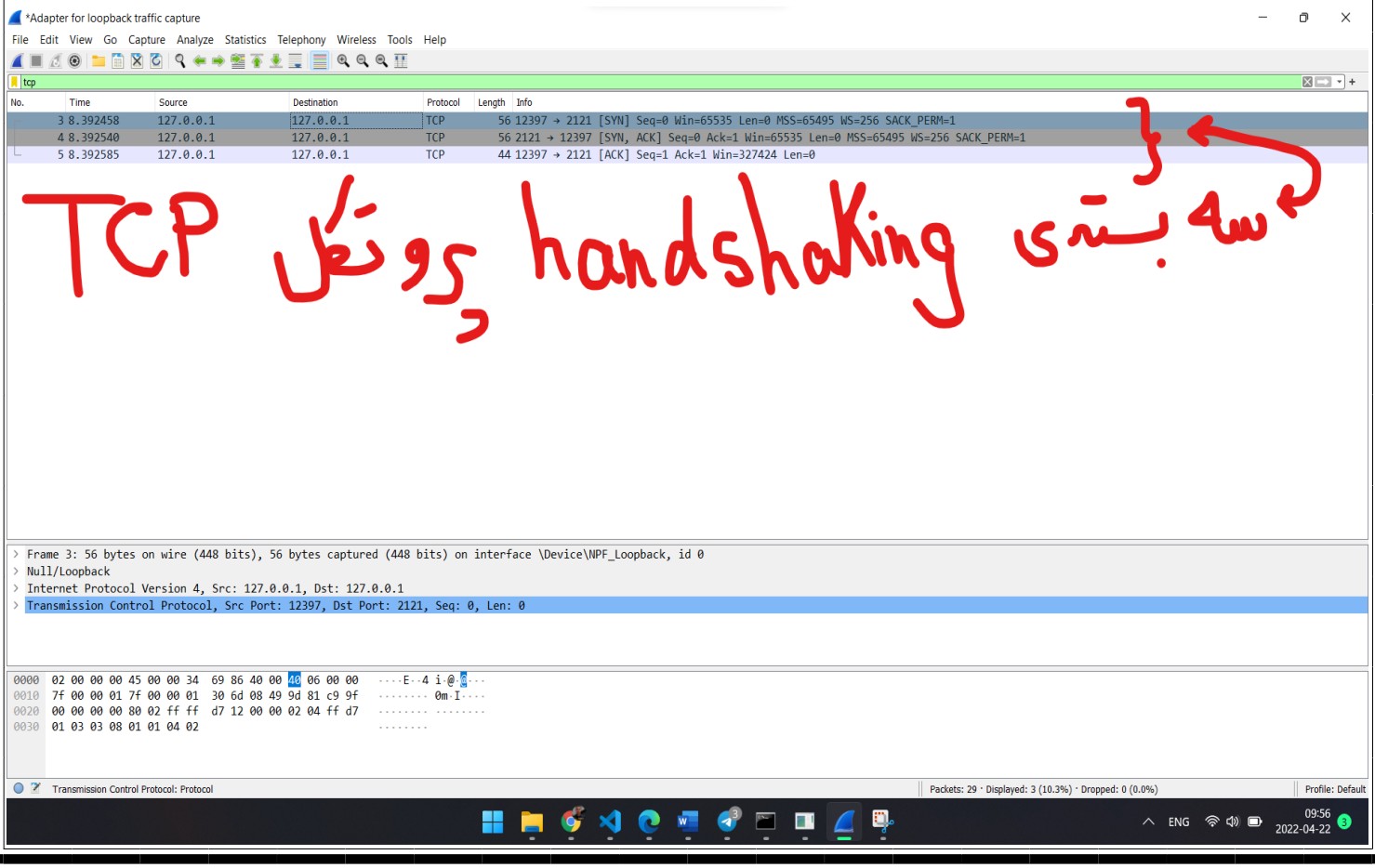
۱) سوال بالا صفحه ۳ : چرا روند دانلود برعکس نیست که کلاینت یک پورت باز کند و آنرا به سرور اطلاع دهد و سرور فایل را از روی آن پورت برای کلاینت بفرستد؟

ـ چون کلاینت فایروال دارد که مانع این کار میشود ولی سرور فایروال ندارد.

۲) سوال وسط صفحه ۳ : حمله‌ای که کلاینت با دادن ورودی که باعث شود فایلی دانلود شود یا فولدری باز شود که در زیر شاخه‌های فولدر اصلی سرور قرار ندارند چه نام دارد ؟

ـ Path Traversal Attack

۳) دیدن سه بسته برای handshaking پروتکل TCP :



۴) سوال ۴/۲ : آیا TCPمحدودیتی برای اندازه پکت ها دارد؟ ـ بله 64kb است.

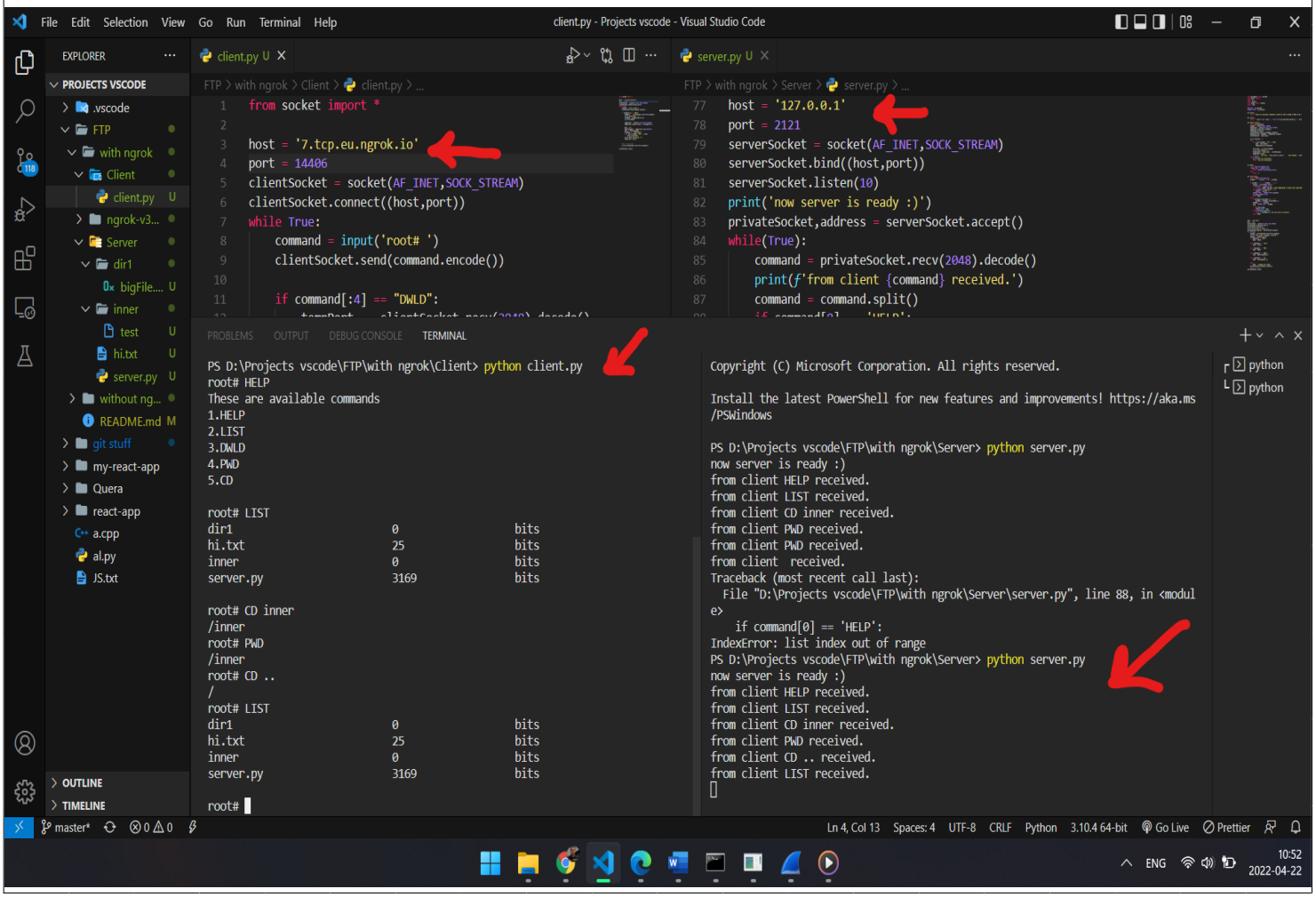
۵) فایل های بزرگ چگونه توسط سوکت TCP ارسال میشوند؟ ـ با شکستن به چندین پکت با حداکثر سایز 64k این کار انجام میشود.

۶) سوال ۴/۲.ب : ۱۶ بسته فرستاده است

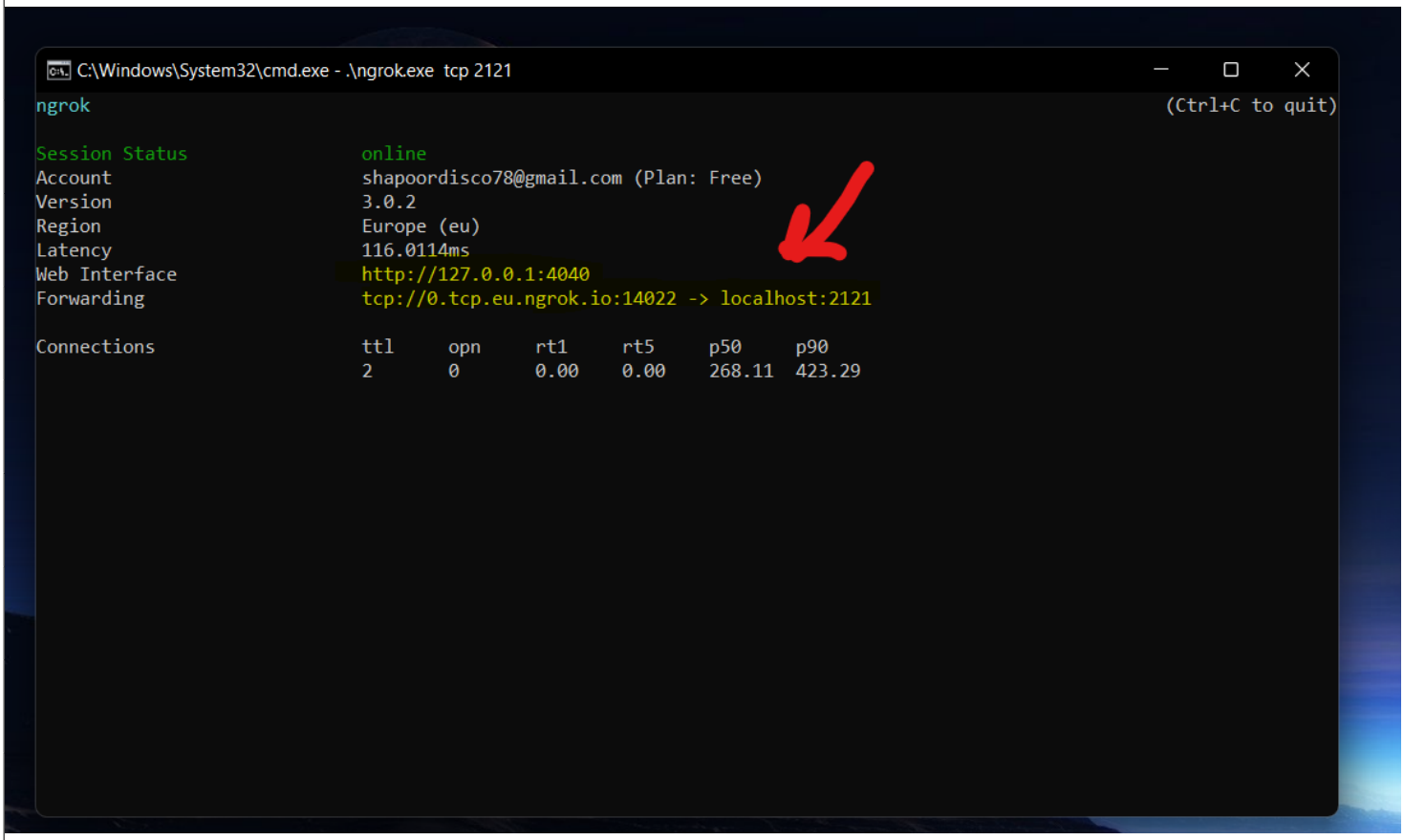
| | | | | | |
|---|---|---|---|---|---|
| 25 | 41.684984 | 127.0.0.1 | 127.0.0.1 | TCP | 56 45160 → 12487 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1 |
| 26 | 41.685037 | 127.0.0.1 | 127.0.0.1 | TCP | 44 12487 → 45160 [ACK] Seq=1 Ack=1 Win=327424 Len=0 |
| 27 | 42.039740 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=1 Ack=1 Win=2161152 Len=65495 |
| 28 | 42.039870 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=65496 Ack=1 Win=2161152 Len=65495 |
| 29 | 42.039998 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=130991 Ack=1 Win=2161152 Len=65495 |
| 30 | 42.040170 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=196486 Ack=1 Win=2161152 Len=65495 |
| 31 | 42.040717 | 127.0.0.1 | 127.0.0.1 | TCP | 44 12487 → 45160 [ACK] Seq=1 Ack=261981 Win=327424 Len=0 |
| 32 | 42.040855 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=261981 Ack=1 Win=2161152 Len=65495 |
| 33 | 42.040979 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=327476 Ack=1 Win=2161152 Len=65495 |
| 34 | 42.041147 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=392971 Ack=1 Win=2161152 Len=65495 |
| 35 | 42.041359 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=458466 Ack=1 Win=2161152 Len=65495 |
| 36 | 42.041850 | 127.0.0.1 | 127.0.0.1 | TCP | 44 12487 → 45160 [ACK] Seq=1 Ack=523961 Win=327424 Len=0 |
| 37 | 42.041974 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=523961 Ack=1 Win=2161152 Len=65495 |
| 38 | 42.042115 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=589456 Ack=1 Win=2161152 Len=65495 |
| 39 | 42.042326 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=654951 Ack=1 Win=2161152 Len=65495 |
| 40 | 42.042529 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=720446 Ack=1 Win=2161152 Len=65495 |
| 41 | 42.043375 | 127.0.0.1 | 127.0.0.1 | TCP | 44 12487 → 45160 [ACK] Seq=1 Ack=785941 Win=65280 Len=0 |
| 42 | 42.045519 | 127.0.0.1 | 127.0.0.1 | TCP | 197 2121 → 12485 [PSH, ACK] Seq=347 Ack=36 Win=2161152 Len=153 |
| 43 | 42.045599 | 127.0.0.1 | 127.0.0.1 | TCP | 44 12485 → 2121 [ACK] Seq=36 Ack=500 Win=2160640 Len=0 |
| 44 | 42.061773 | 127.0.0.1 | 127.0.0.1 | TCP | 44 [TCP Window Update] 12487 → 45160 [ACK] Seq=1 Ack=785941 Win=327424 Len=0 |
| 45 | 42.061874 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=785941 Ack=1 Win=2161152 Len=65495 |
| 46 | 42.061902 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=851436 Ack=1 Win=2161152 Len=65495 |
| 47 | 42.061952 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=916931 Ack=1 Win=2161152 Len=65495 |
| 48 | 42.062002 | 127.0.0.1 | 127.0.0.1 | TCP | 65539 45160 → 12487 [ACK] Seq=982426 Ack=1 Win=2161152 Len=65495 |
| 49 | 42.062051 | 127.0.0.1 | 127.0.0.1 | TCP | 700 45160 → 12487 [FIN, PSH, ACK] Seq=1047921 Ack=1 Win=2161152 Len=656 |
| 50 | 42.062177 | 127.0.0.1 | 127.0.0.1 | TCP | 44 12487 → 45160 [ACK] Seq=1 Ack=1048578 Win=64768 Len=0 |

از شروع تا پایان دانلود

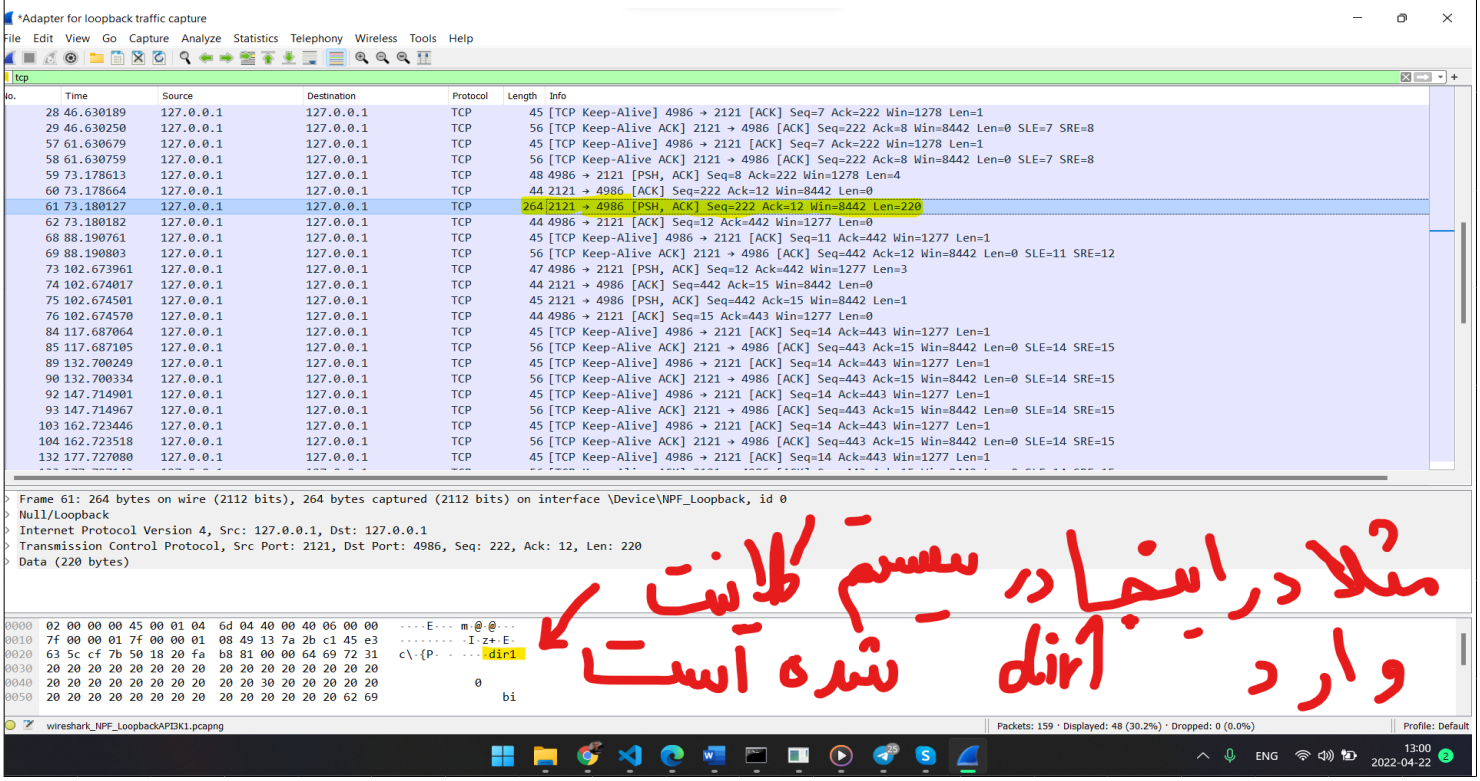
۷) سوال ۵/۱ : اجرای دستورات به جز DWLD با استفاده از ngrok :



۸) سوال ۵/۲ : ابتدا ngrok را اجرا کردیم ...

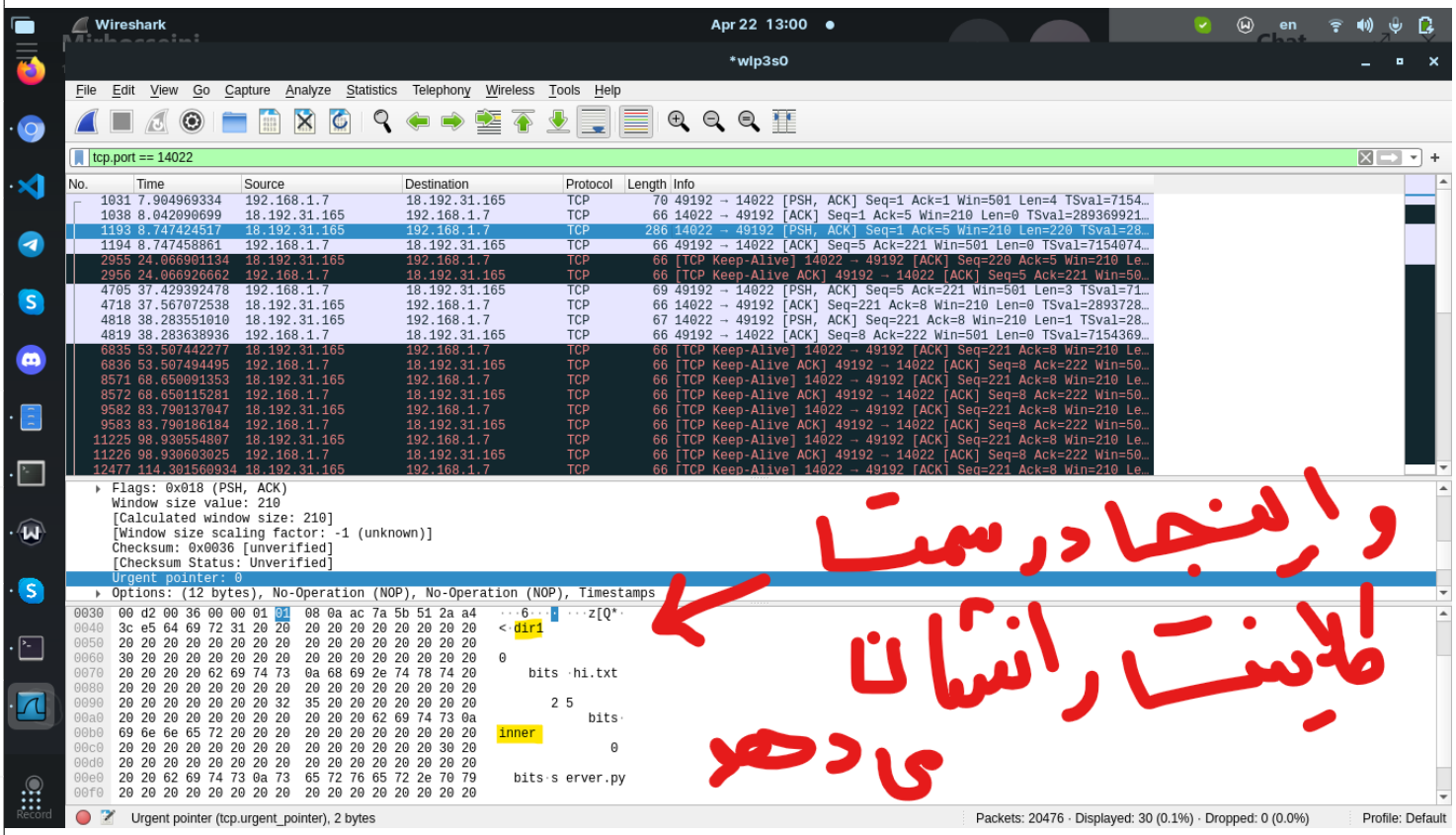



سپس در سیستم من سرور را ران کردیم و در حالت loopback به نتایج زیر رسیدیم :




مثلا در اینجا در سیستم کلاینت وارد dir شده است

و در سیستم آقای کرباسیان در وایرشارک در حالت Wi-Fi به نتایج زیر رسیدیم :




۹) سوال ۵/۳ : خیر نمیتوان دانلود کرد چون اولا اکانت Permium در خوده ngrok نداریم فقط یکی توکن به ما میدهد و نمیتوانیم دوتا توکن داشته باشیم تا یکی برای Data Channel و یکی برای Control Channel تخصیص بدهیم و تقریبا باید این دو چنل را ادغام کنیم و از یکی برای هردو استفاده کنیم .

با این حال با وارد کردن کامند DWLD برنامه کرش میکند. مشکلش این است که چون در تابع DWLD ما داریم یک پورت جدید میسازیم و باید به نحوی این را به ngrok هم بفهمانیم که پورت جدید ( همان پورت رندوم بین ۳۰۰۰ تا ۵۰۰۰۰ ) را برای کلاینت بفرستد. راهکاری که برای حل این مشکل پیدا نمودیم این است که در تابع DWLD به نحوی ngrok را اجرا کنیم و از بخش forwarding آن ، آرگومان‌های host و port را برای کلاینت بفرستیم تا کلاینت بتواند هاست و پورت خودش را آپدیت کند و بتواند عملیات دانلود را انجام دهد.