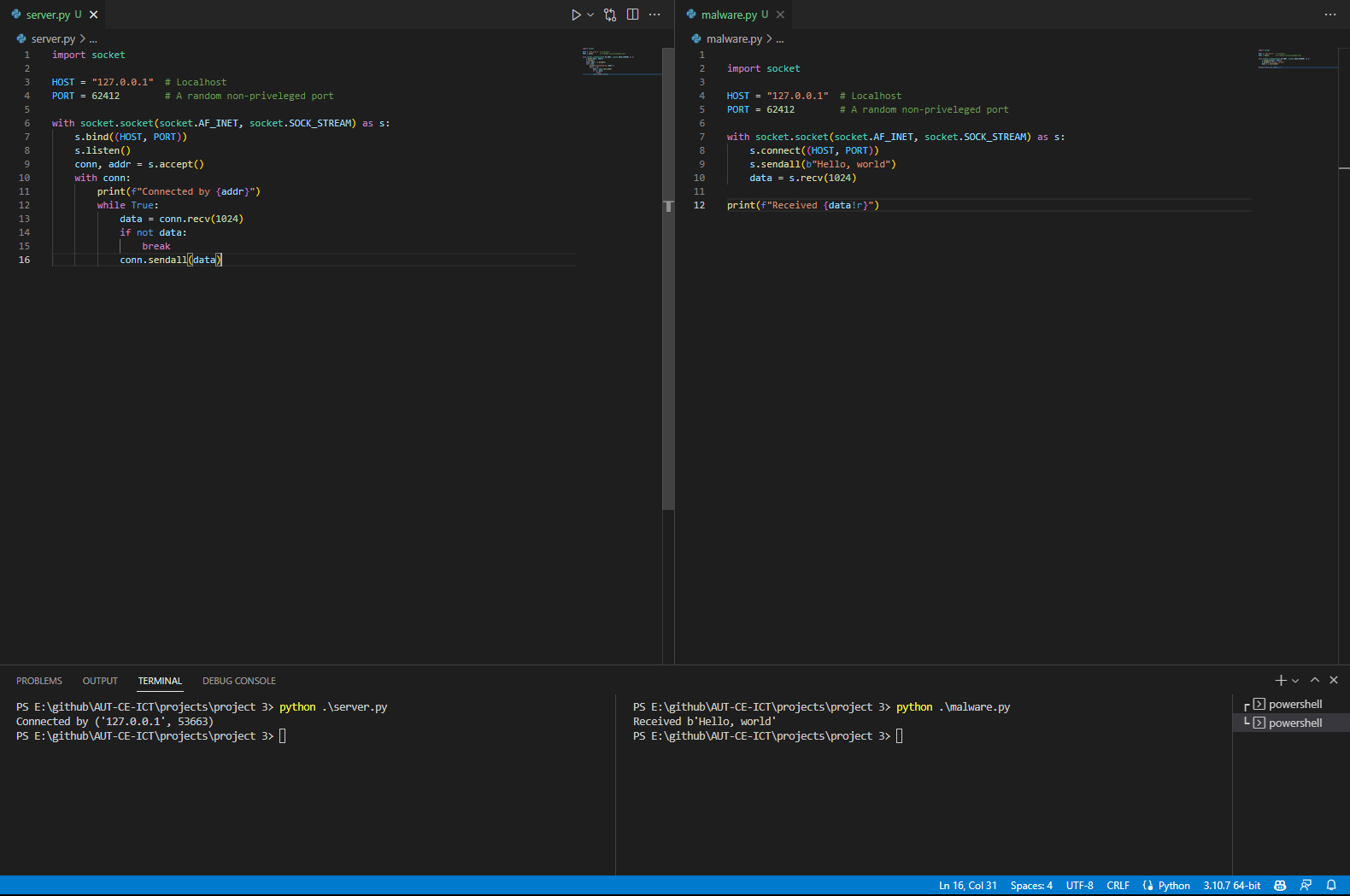
بخش اول

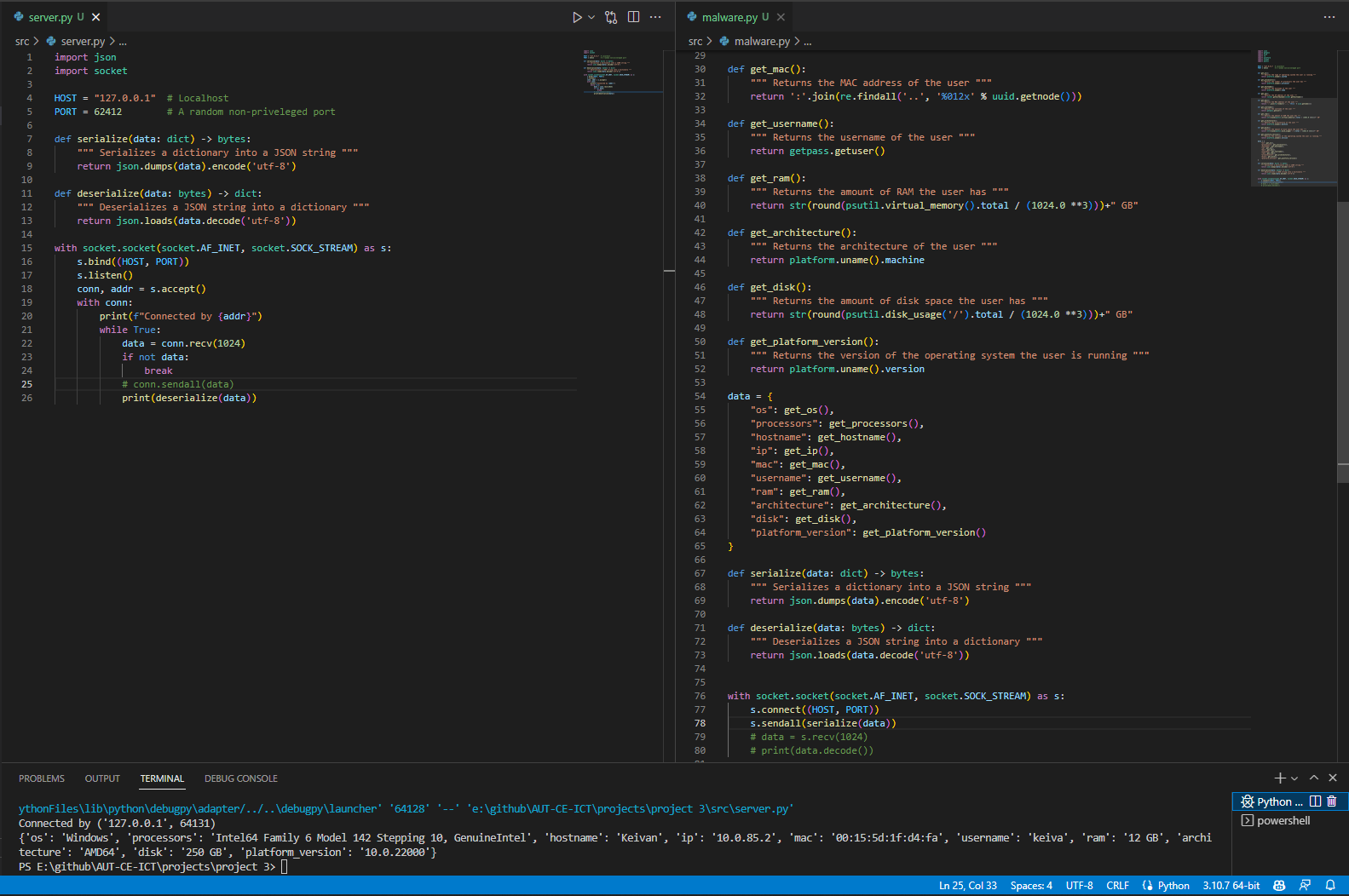


در این بخش دو برنامه server.py و malware.py داریم که در محیط داخلی یا localhost و پورت 62412 که یک پورت استفاده عموم است متصل میشوند. مطابق تصویر بالا هر دو برنامه اجرا شده، رشته از malware.py به سرور ارسال شده و server.py آن را برگردانده است که نشانه یک اتصال موفقیت آمیز است.

بخش دوم

در این بخش، با استفاده از کتابخانه های متنوع توابع زیادی نوشتیم که اطلاعاتی در خصوص سیستمی که فایل malware.py رو آن اجرا میشود ارسال میکند. سپس برای ارسال این اطلاعات آنها را به شکل dictionary در آورده و با استفاده از کتابخانه JSON آنها را serialize و سپس به bytes تبدیل کرده و ارسال میکنیم به سمت serer.py.

سپس فایل server.py این اطلاعات را خوانده و decode و deserialize کرده (به ترتیب) و نمایش میدهد. تصویر پایین نشان دهنده اقدامات انجام شده است.



بخش سوم

در بخش سوم، این server.py است که با malware.py درخواست دریافت اطلاعات قربانی را میدهد و malware.py آن را به سرور ارسال میکند. در اینجا server.py دو دستور sysinfo برای دریافت نتایج و دستور exit برای اتمام ارتباط بین دو فایل وجود دارد. در ابتدا سرور دستور sysinfo را در قالب رشته به malware.py ارسال کرده و سپس malware.py فایل serialize شده خروجی را به server.py میفرستد.

سپس در طراحی یک دستور exit گذاشته تا بتوانیم ارتباط را به پایان برسانیم که به طور خودکار بعد از دستور sysinfo اجرا میشود. در صورت نگذاشتن دستور exit، ارتباط برای همیشه براقرار خواهد ماند!

