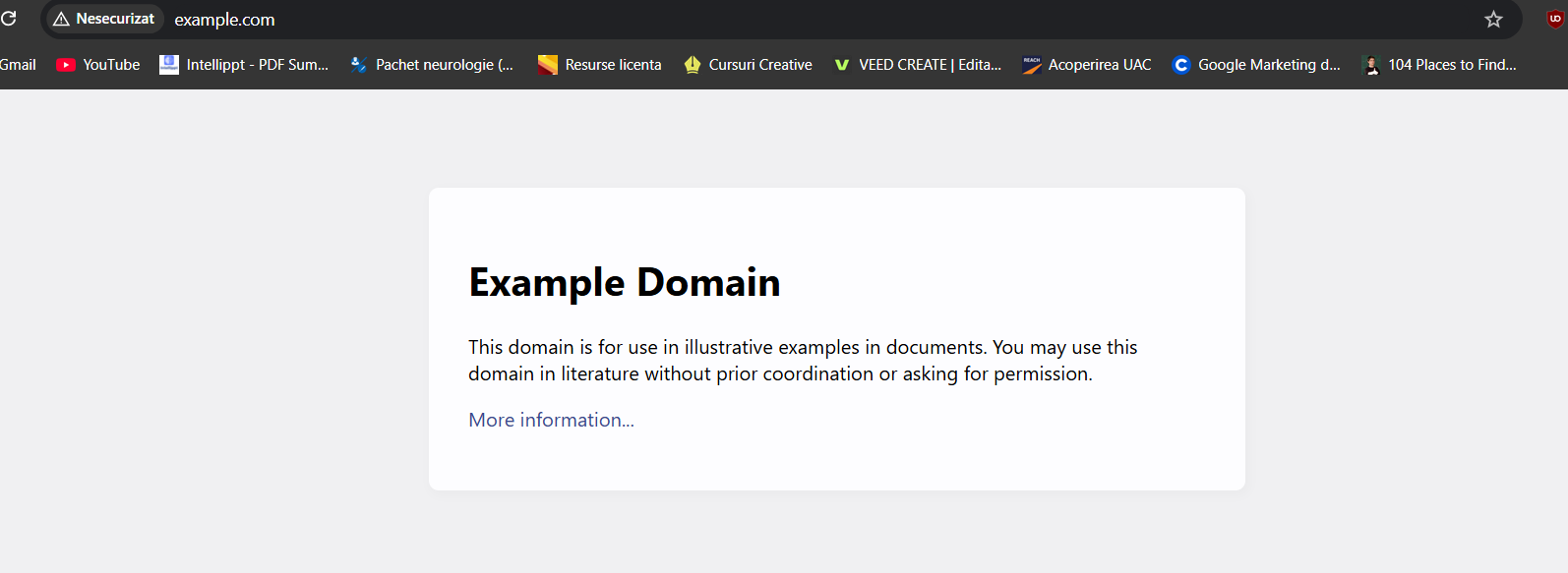
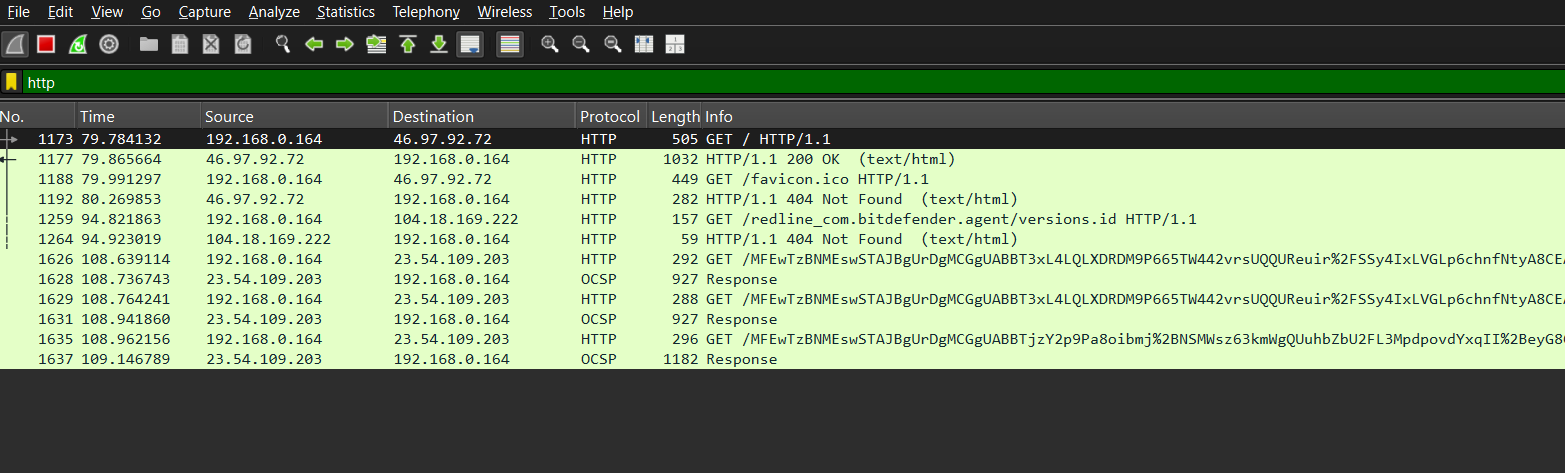
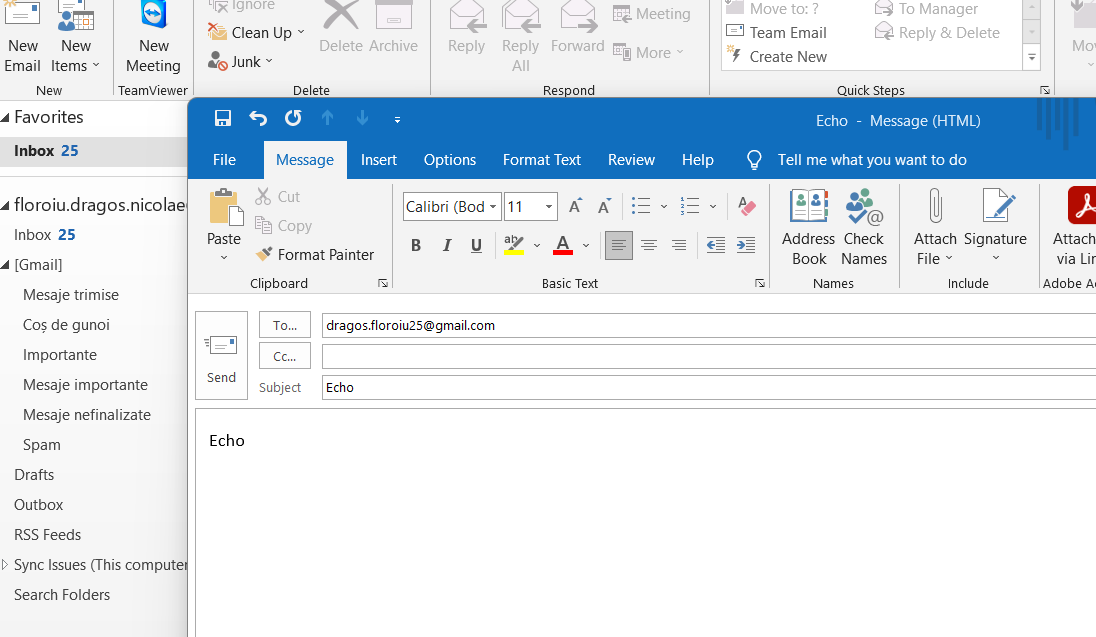
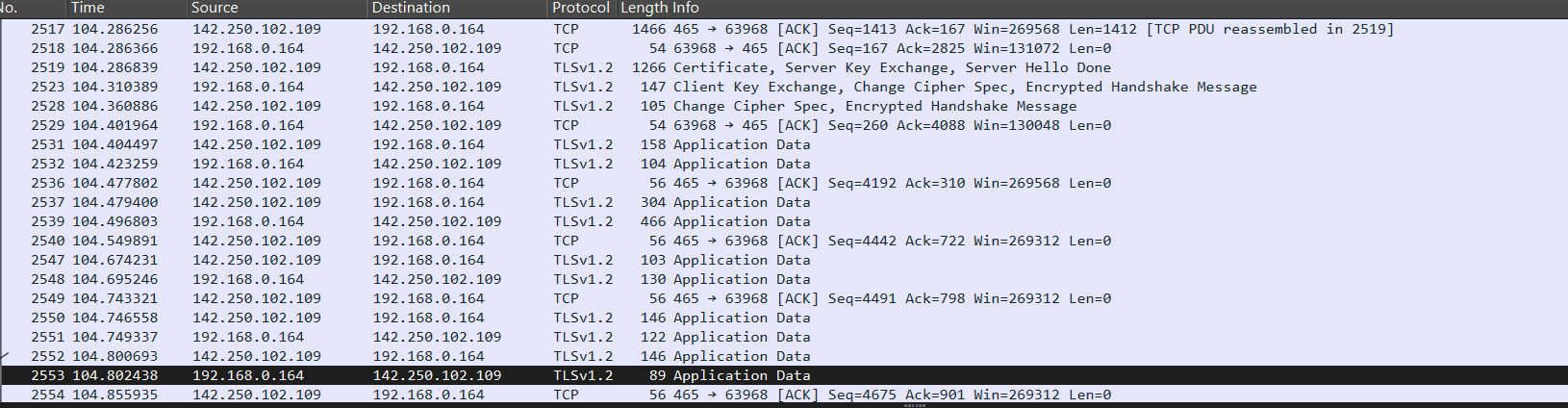
Sarcina 1: Interceptarea traficului HTTP necriptat





Sarcina 2: Analizarea traficului SMTP pentru a identifica vulnerabilitățile de e-mail

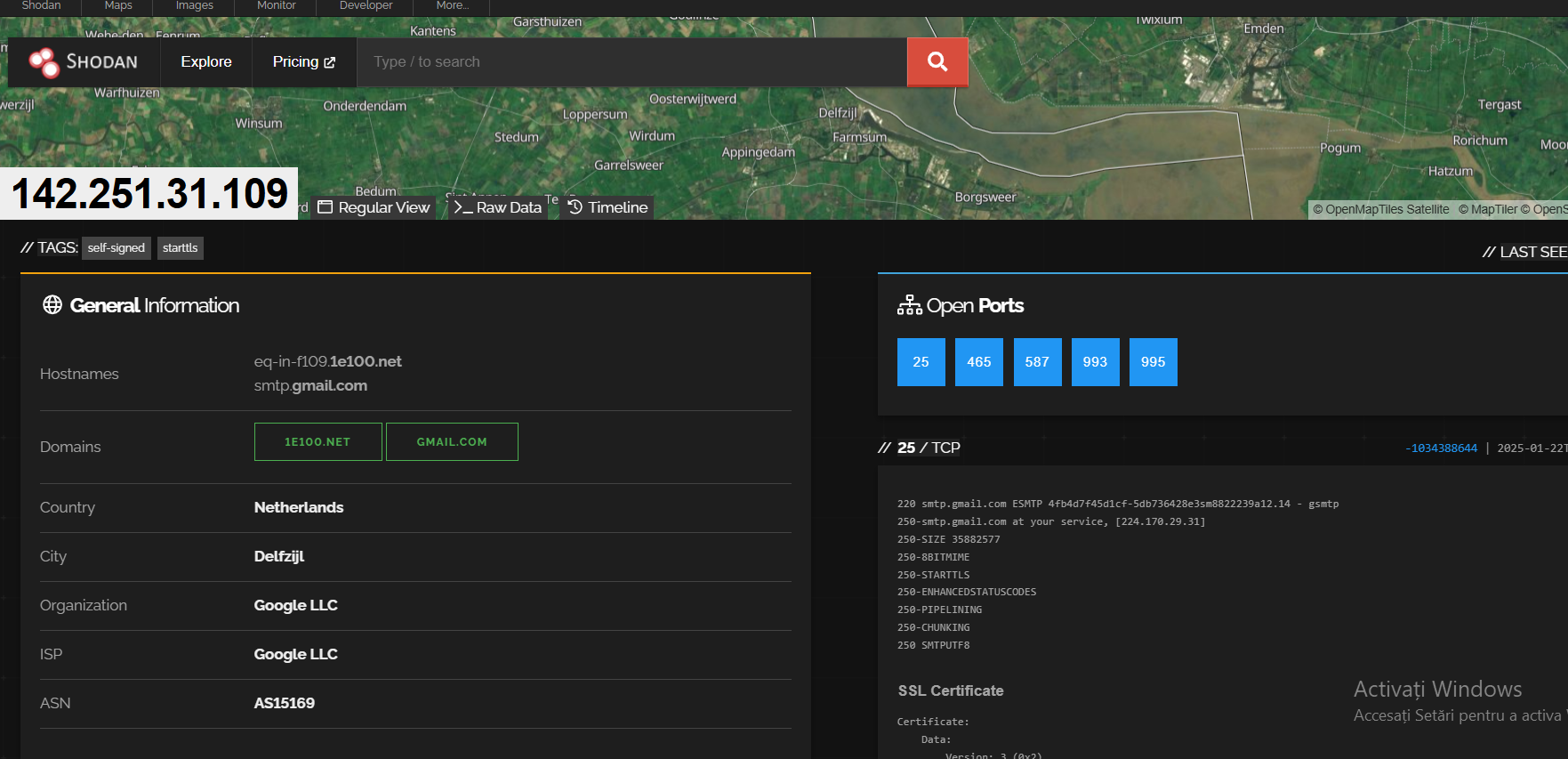
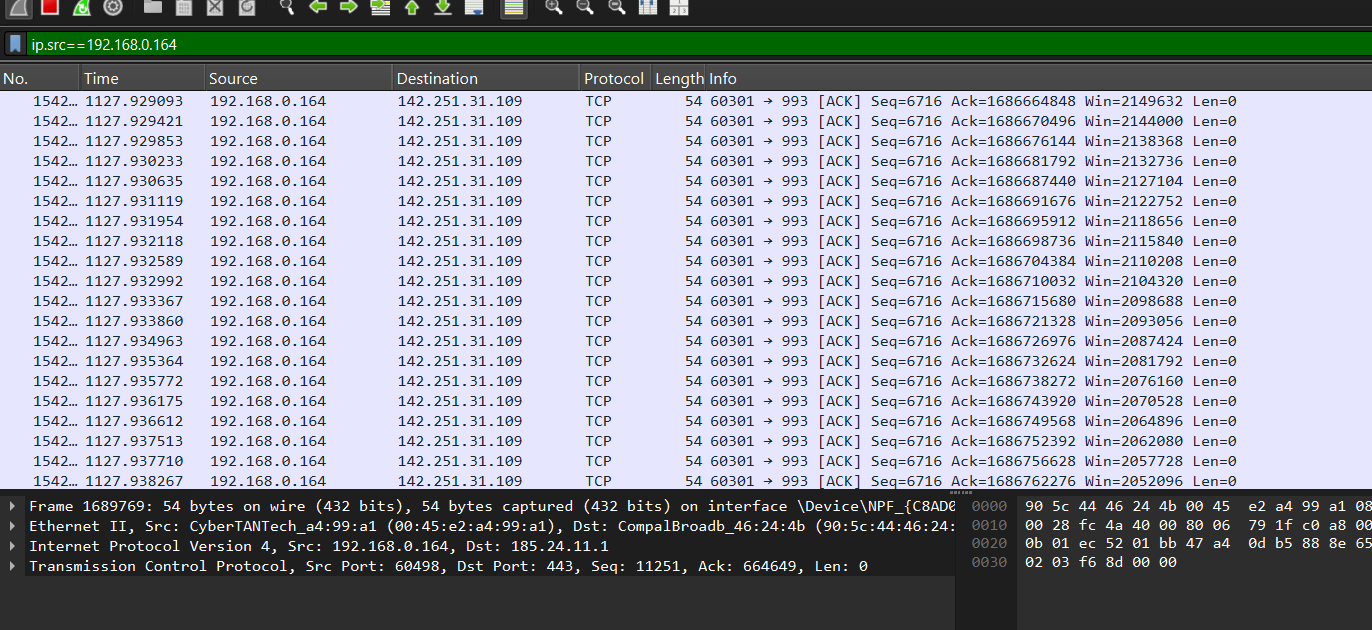


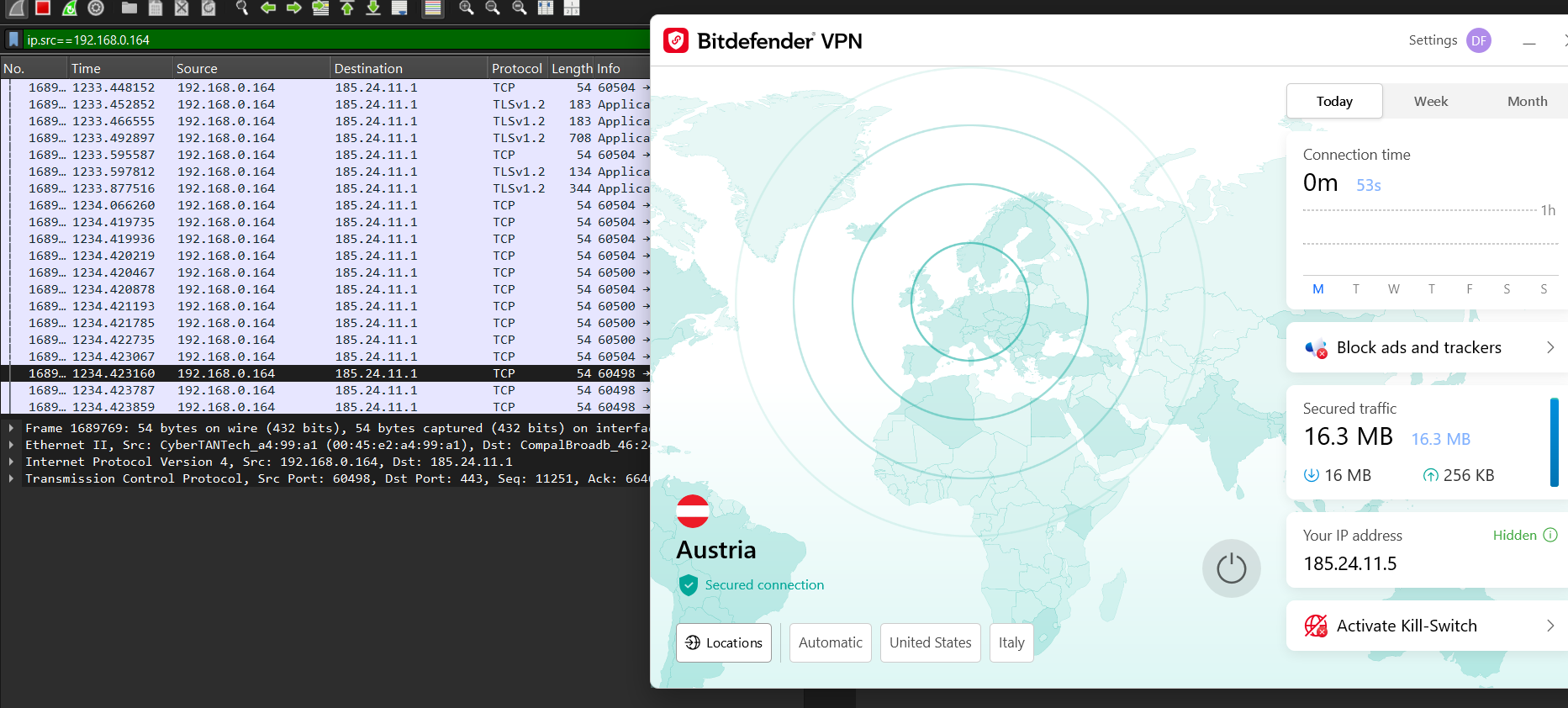


Nu am vazut activitate pe SMTP asa ca am filtrat pe portul 465 care este criptat prin TLS

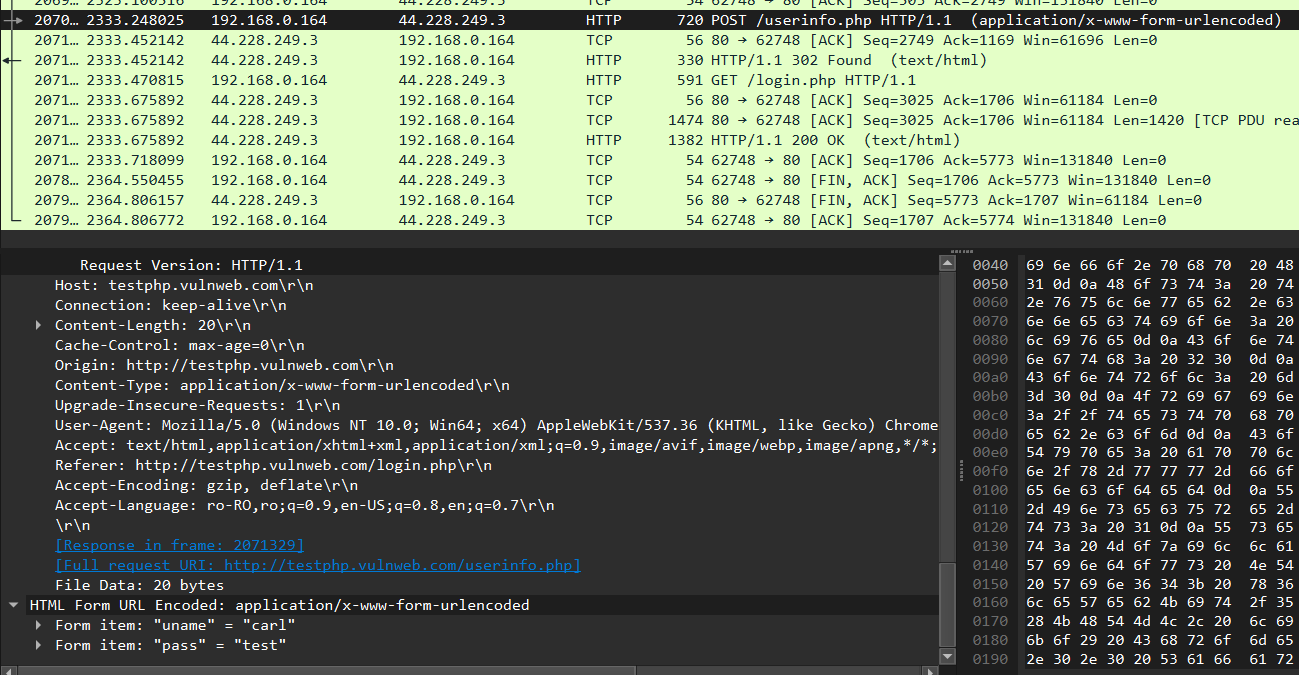
Sarcina 3: Identificarea activității neașteptate în propria rețea

Am luat adresa IP 142.251.31.109 pe care am observat-o si la o cautare in Shodan a fost exact cea utilizata pentru serviciul de mail.



Am testat si o conexiune la VPN si putem observa ca la destination IP este cea din aplicatia VPN.

Sarcina 4: Găsirea în traficul interceptat a unui login și a unei parole



Dupa ce m-am logat pe pagina respectiva am cautat in wireshark si in pachetul post /userinfo.php in html form URL putem observa credentialele folosite username carl si parola test.