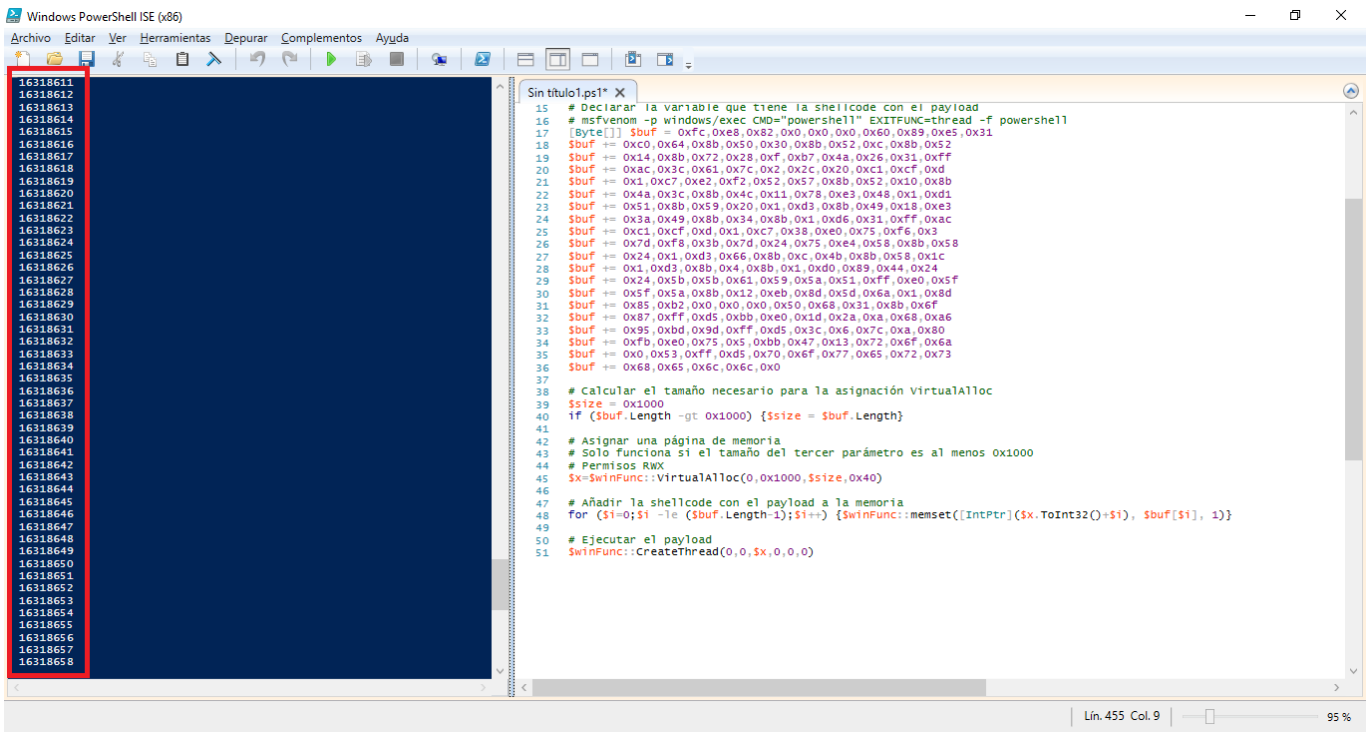
Analizar con Cheat Engine un payload de ejecución de comandos arbitrarios para ejecutar PowerShell

Script para cargar en memoria y ejecutar un payload de ejecución de comandos arbitrarios en PowerShell
[crayon-6a9d60046c7c5633864646/]
Direcciones utilizadas para cargar la shellcode con el payload



Analizar con Cheat Engine el payload de ejecución de comandos arbitrarios cargado en PowerShell

Relación entre la shellcode y la carga en memoria desde Cheat Engine