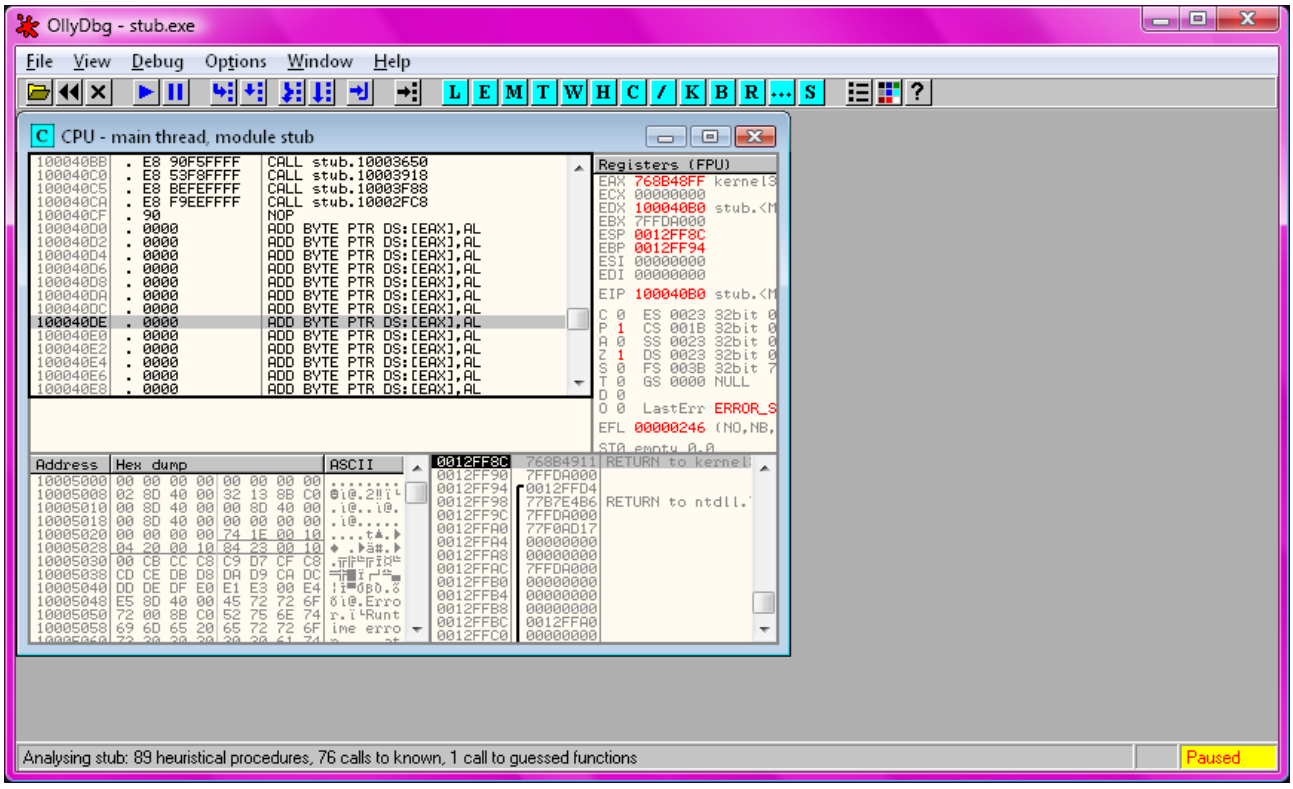
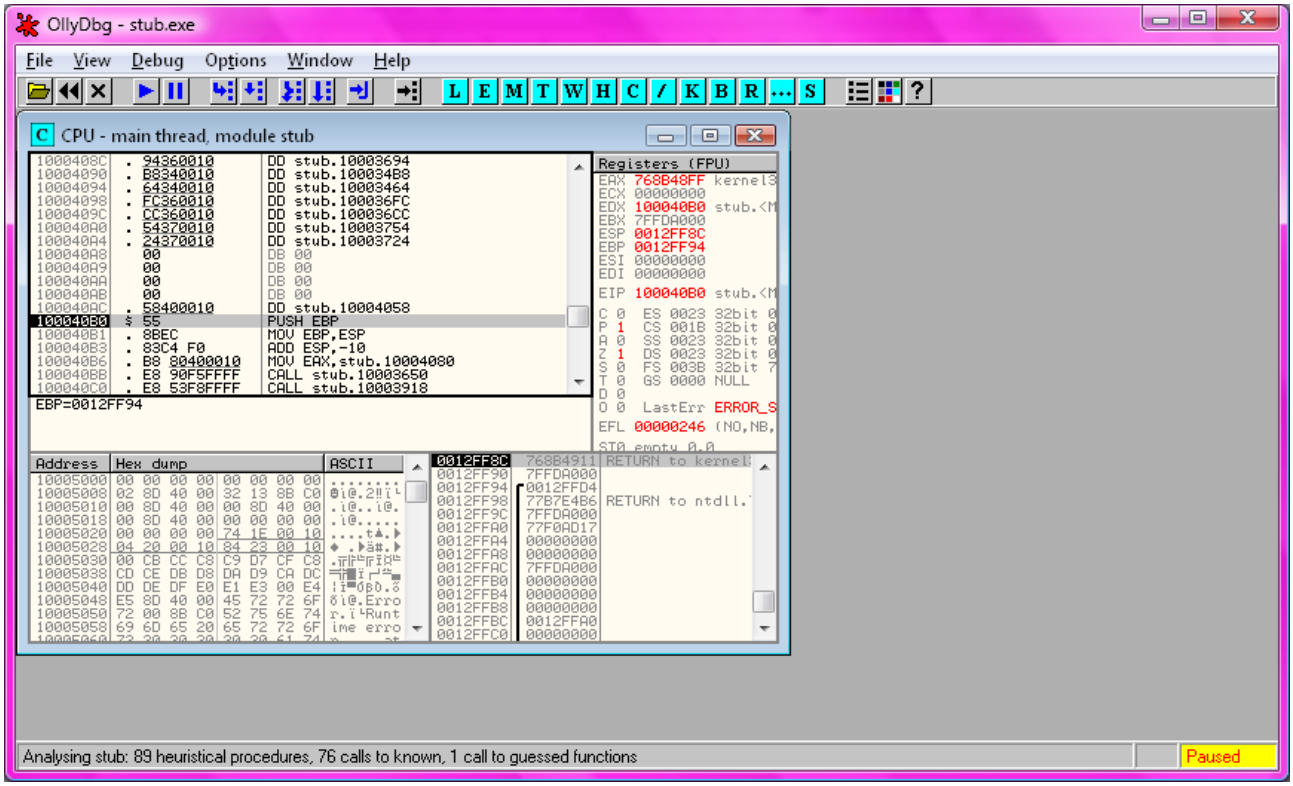
# Modificación de firmas por el método WYR
# [Muy efectivo y súper sencillo]


En este videotutorial veremos como modificar la firma de un stub/server utilizando el método WYR. Es un método muy sencillo que se hace en cuestión de segundos y además es muy útil. Con este método quitarás aproximádamente unos 3-7 anti-virus de un stub/server en tan solo unos segundos, como ya dije.

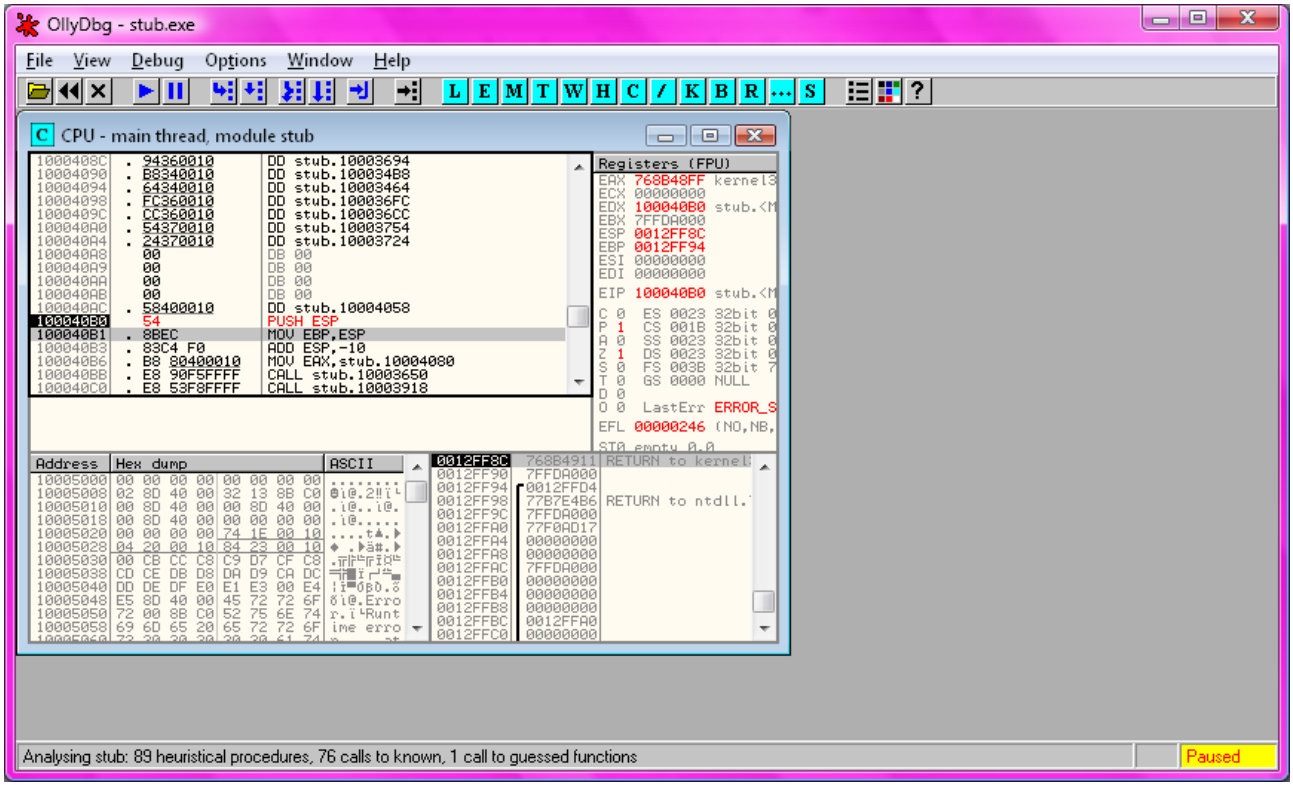
Lo primero que haremos será ejecutar el OllyDBG y luego le damos a “File”>”Open” y luego escogemos el stub/server que queremos modificar. Nos aparecerá una pantalla como esta:



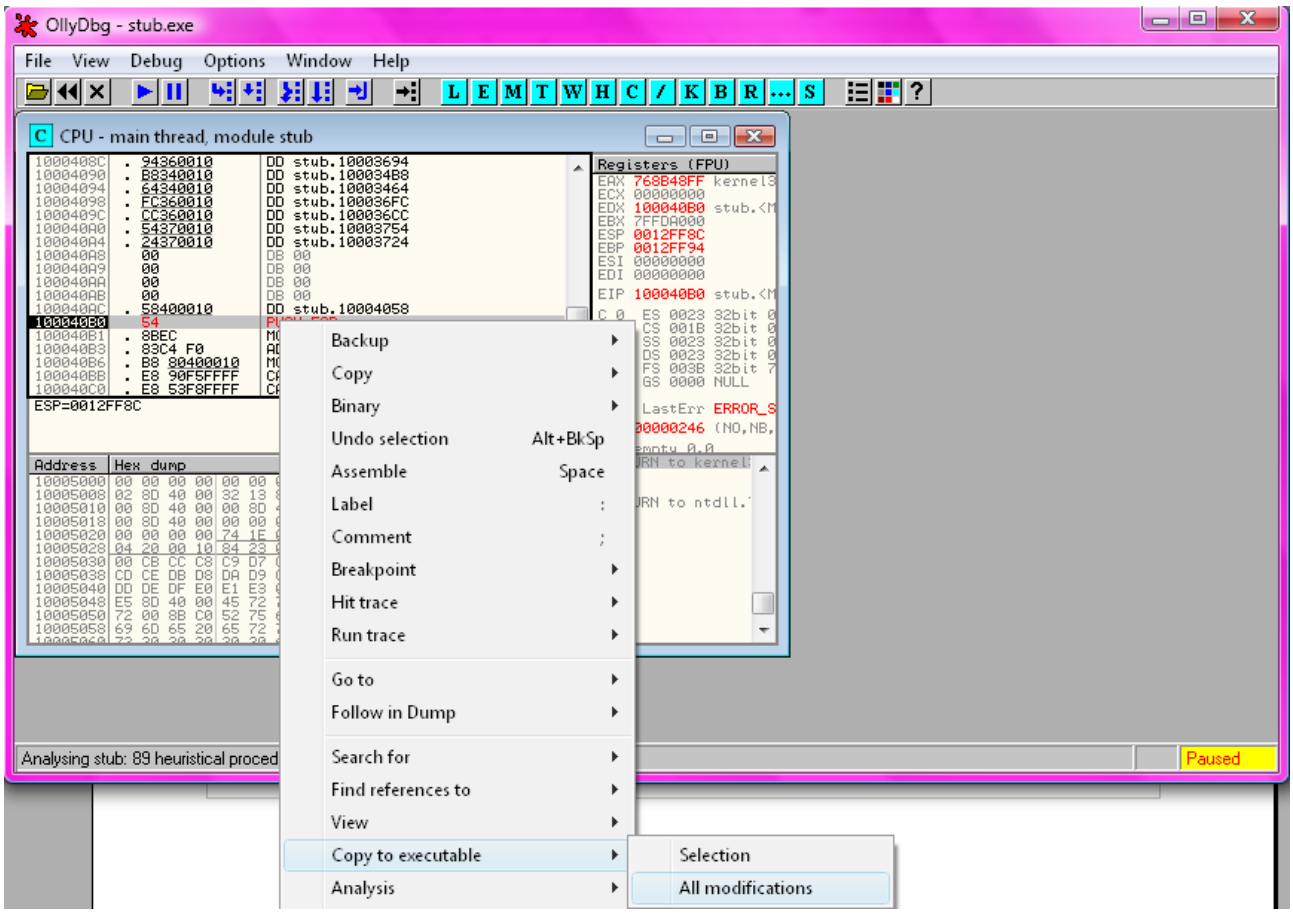

Vemos que hay una linea (la marcada)en la que aparece “POR AX,4”. En esa misma columna debemos encontrar “PUSH EBP”. En mi caso ya lo encontré. Fijaros:




Le damos doble clic encima de “PUSH EBP” y luego sustituimos “EBP” por “ESP”. A continuación clicamos en “Assemble” y luego en “Cancel”. Quedará así:




Ahora le damos con el botón secundario sobre la linea modificada y clicamos sobre “Copy to executable”>”All modifications”. Algo así...




Se nos abre una pantalla pequeñita, la cual debemos cerrar y nos pregunta si queremos guardar los cambios, le decimos que si y sobreescribimos el archivo y listo, ya lo tenemos indetectable.

**Este tutorial fue hecho por MicroAttackeR (M.A.R.) para:**

**http://CodeKaos.com/foros**