

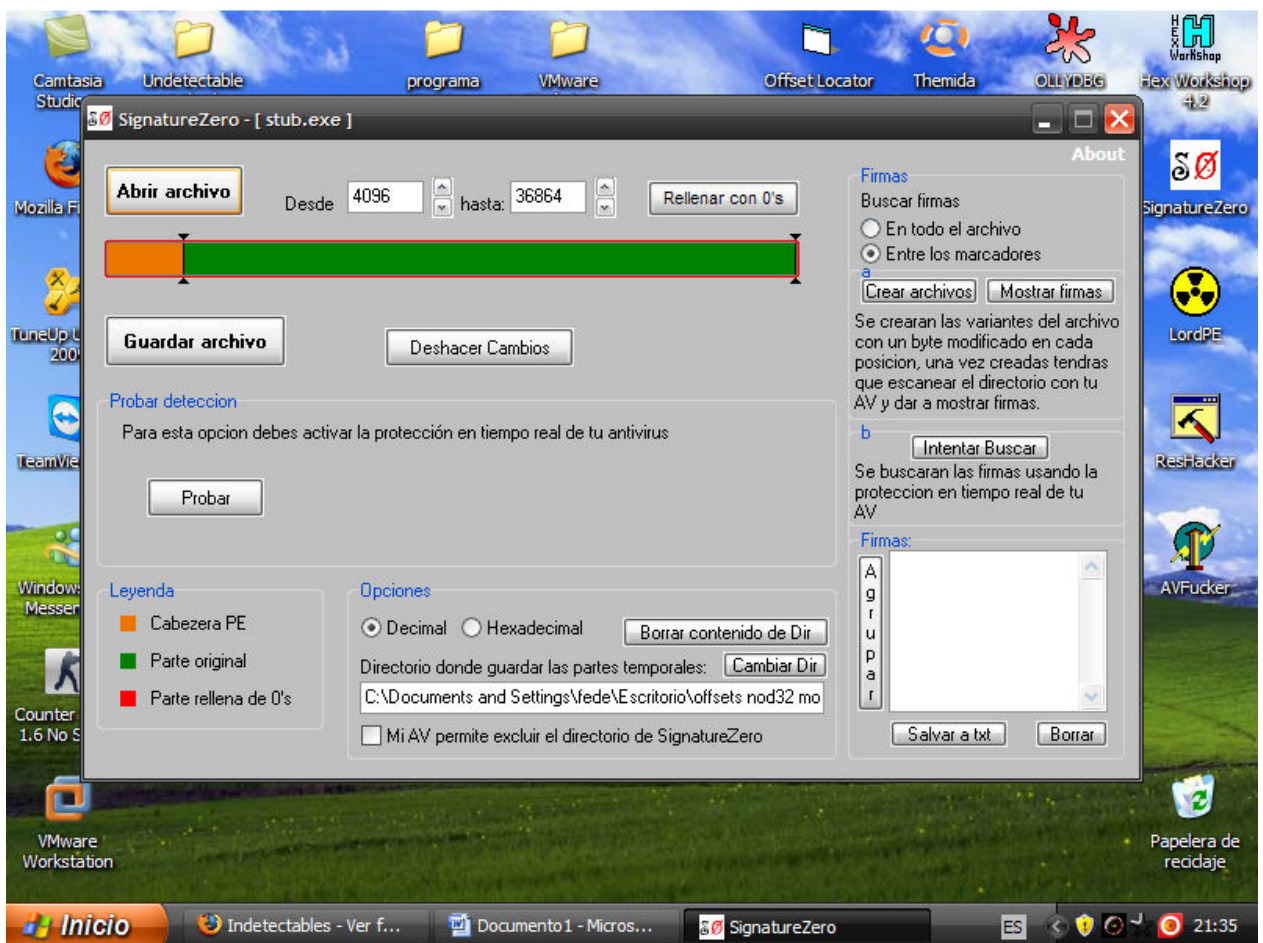
Hola hoy veremos cómo sacarle la firma a un stub o server muchos más rápido

Lo que haremos será cercar lo más posible la firma con el singatuzero , luego pondremos los marcaadores desde el inicio de la firma hasta el final y usaremos la opción parecida al avfucker que tiene el singatuzero para crear los offsets y proceder a analizar la carpeta en donde se crearon los offsets para terminar por completo de sacar la firma con esto nos ahorramos que si lo hacemos con el singatuzero la parte del hex que es la más molesta para mí y la parte del avfucker que es comerse el análisis de todos los offsets que creamos y esperar como 1 hora,

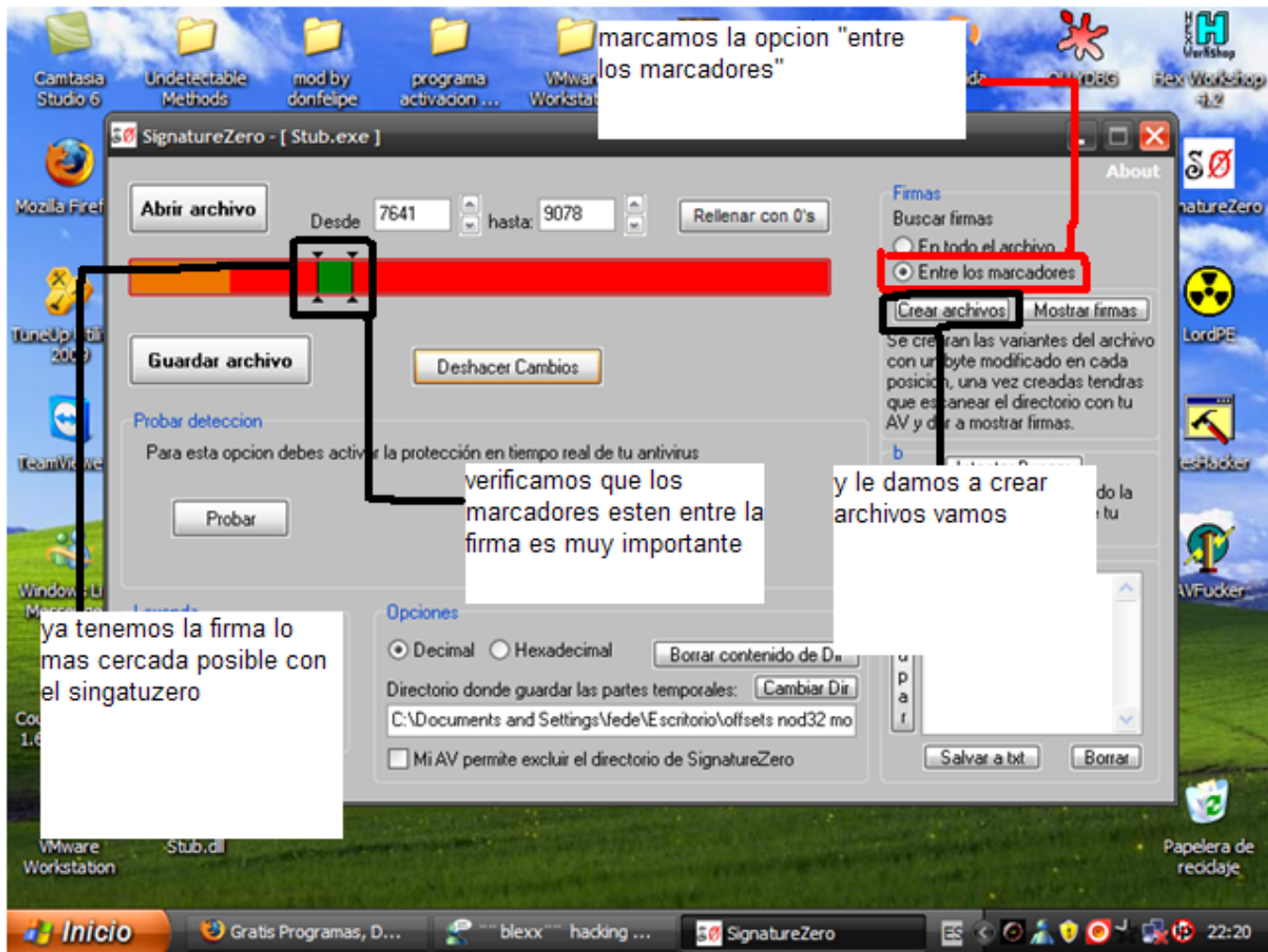
Básicamente en pocas palabras cercaremos la firma lo mas que podamos con el singatuzero y usaremos como el avfucker pero que lo tiene incorporado el singatuzero entre la firma cercada para crear menos offsets y que el antivirus lo escanee más rápido

Si no entendieron tranquilos que ahora pongo como hacerlo en imágenes y eso xdx dx:

Abrimos el stub que querramos con el singatuzero y veremos algo como esto:



Ahora buscamos la firma lo más posible masomenos asi solo que ustedes utilizaran otro stub y la firma la tendrán en otro lado dx dx dx:



Listo!!! lo único que falta es analizar la carpeta con los archivos crados por el singatuzero entre los marcadores porque ya hemos acorralado la firma lo más posible y lo que queda es la firma

Saludos y hasta la próxima

By fexx