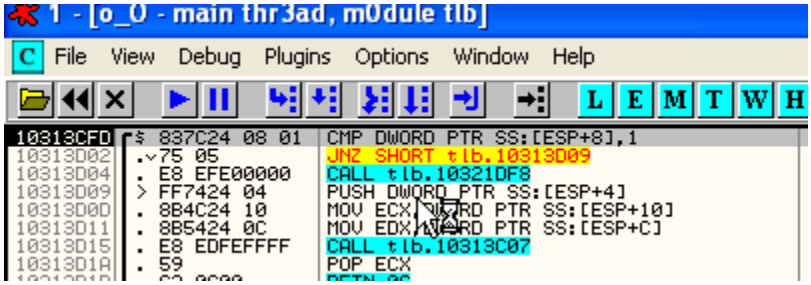
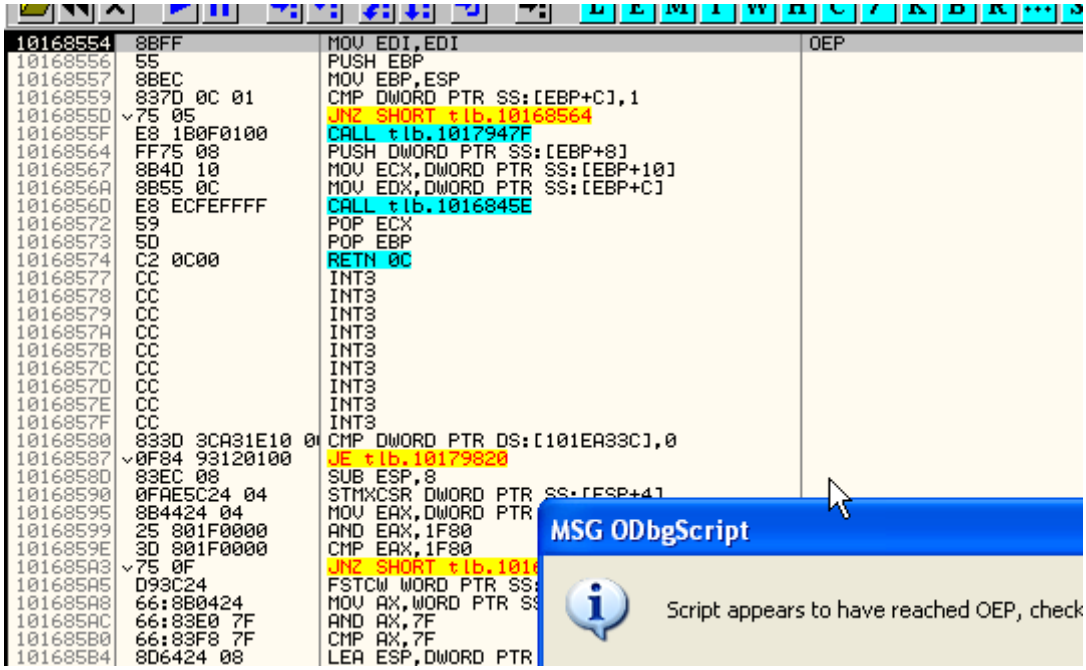
True Launch Bar

Comienzo investigando la dll esta empacada con armadillo 7.4:

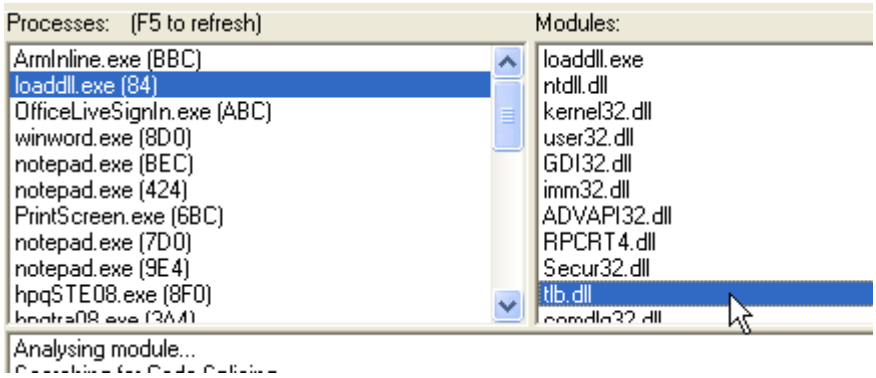
```
<- 28-10-2010 13:31:51 - [2.0] ->
C:\archivos de programa\TrueLaunchBar\t
Protected Armadillo
<-Find Protect
Protection system (Professional)
<Protection Options>
System File
Import Table Elimination
Strategic Code Splicing
<Backup Key Options>
Main Key Only, No Backup Keys
<Compression Options>
Minimal/Fastest Compression
<Other Options>
Disable Monitoring Thread
<-Find Version
Version 7.40 27-07-2010
<- Elapsed Time 00h 00m 03s 312ms ->
```

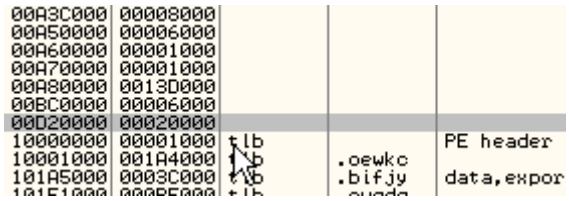


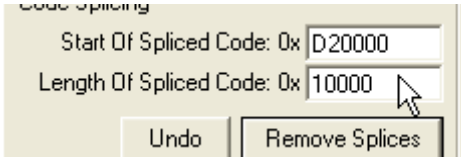
,secured no,

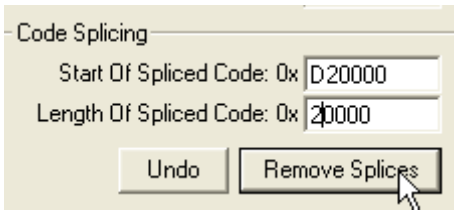


Ahora



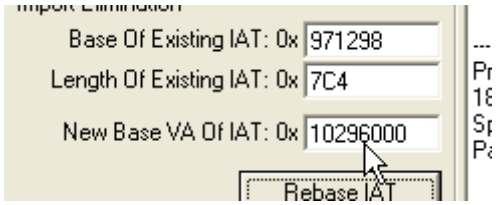


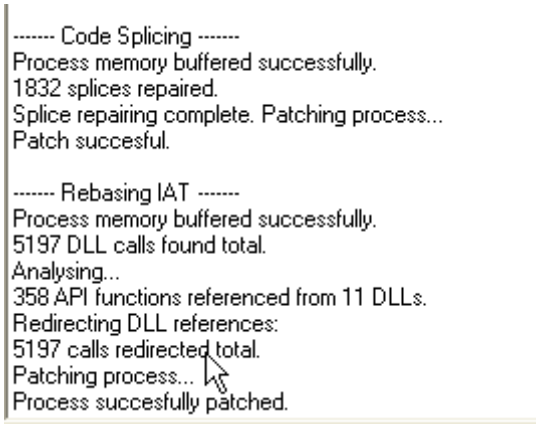




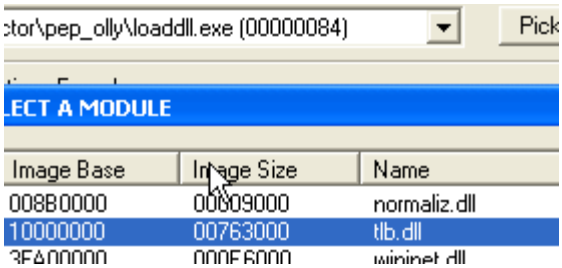
cambio a

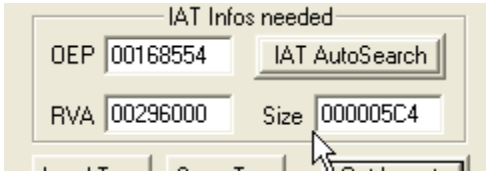
Decia tamaño 5c4, revisando es un poco mayor, coloco 7c4



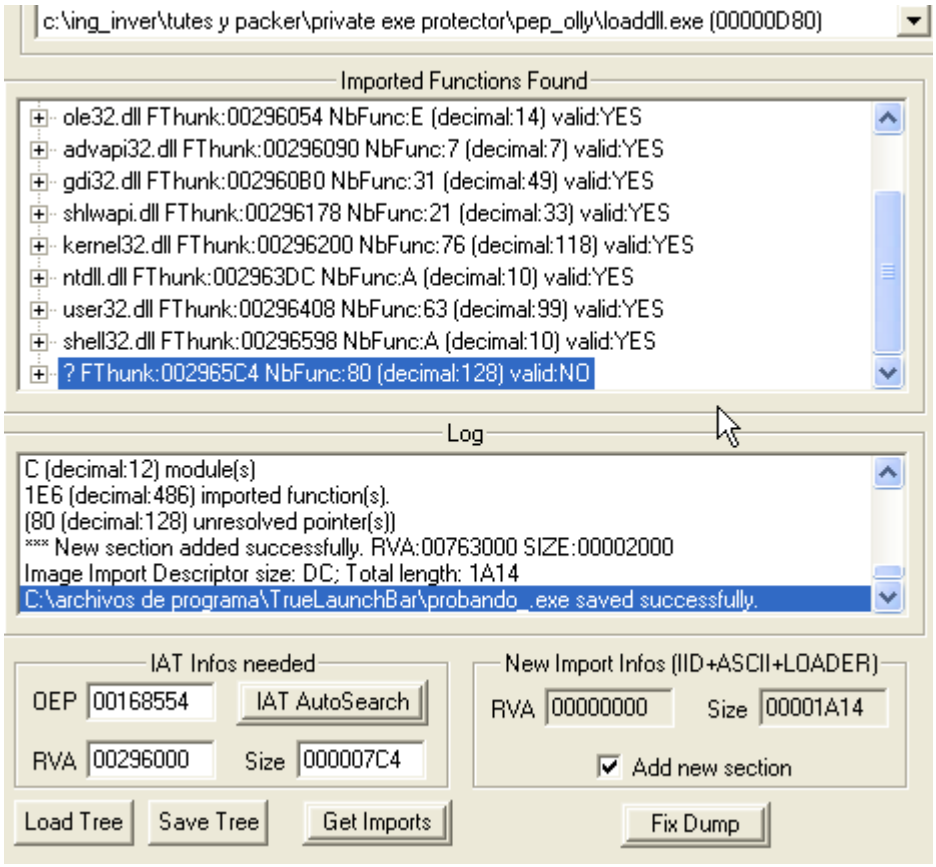


Ahora el import rec





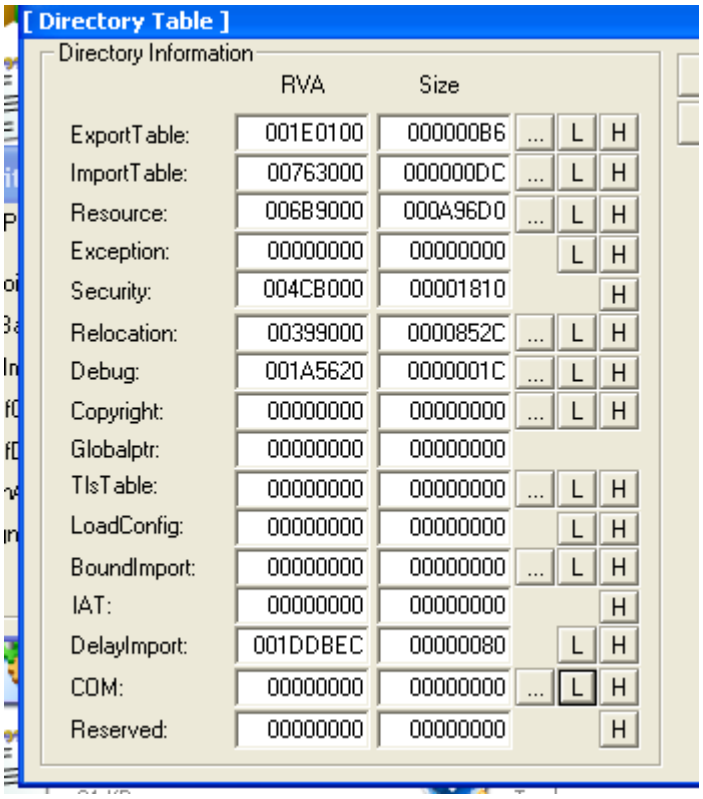
Hago el dump desde import ret y agrego todo incluyendo los invalidos



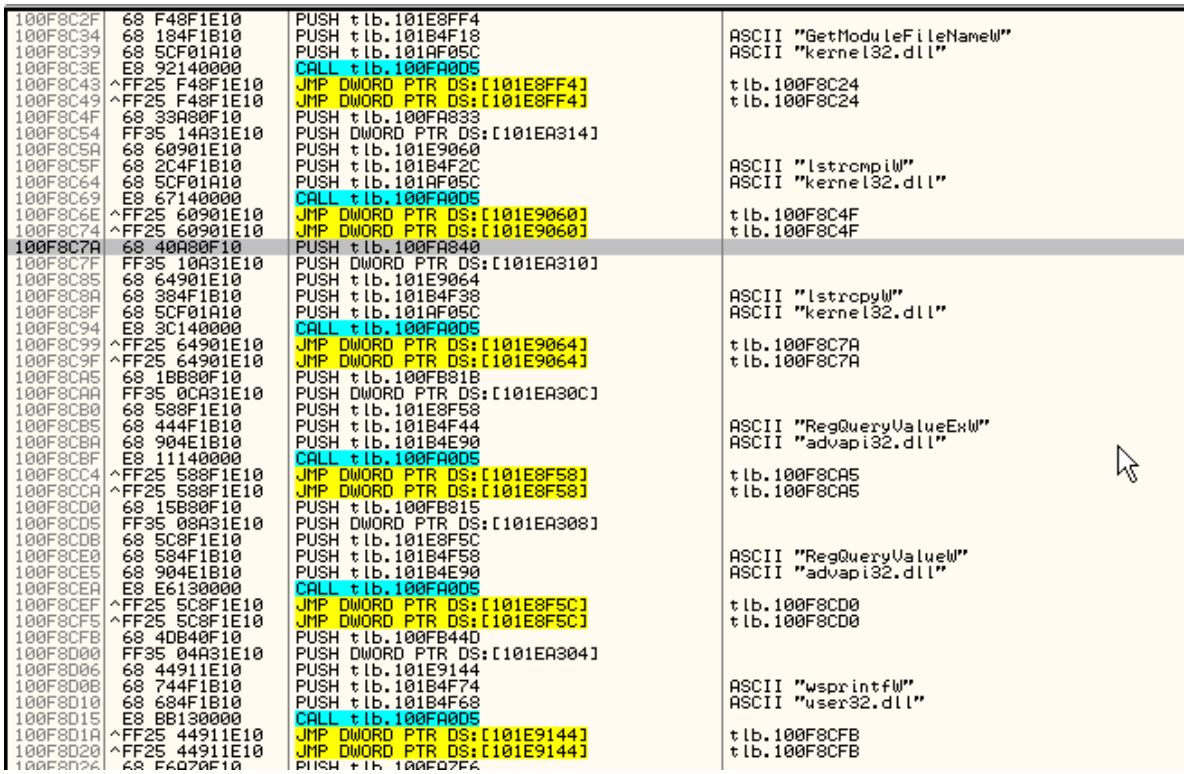
Y renombro el tbl.dll a tbl_original

Y este unpacked como tbl.dll

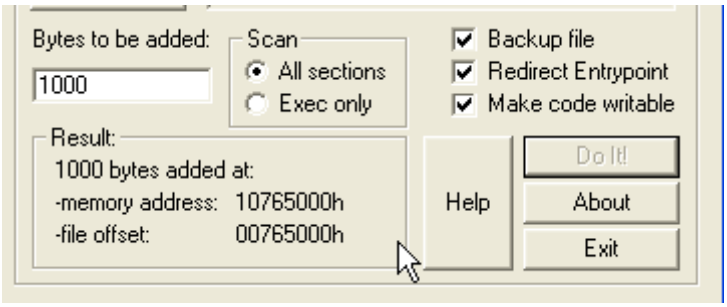
pruebo y ejecuta /unpacked:



Lo especial es que ciertos punteros que parecieran ser malos tienen direcciones apuntadas a

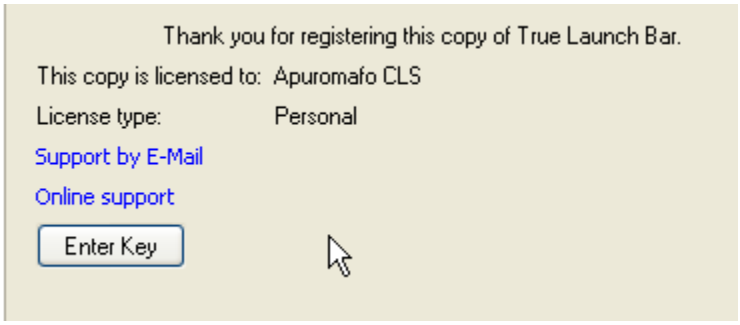


Y como tambien aveces puede resultar pruebo si en la dll es posible Registrarnos con las variables:



Colocando un bp en ejecucion en GetEnvironmentVariableA tendremos las variables necesarias

Con esto se crea por ejemplo un about:



Pd:como el objetivo era descargar un armadillo y aprender de las variables, pues desinstalo la aplicacion y borro las ramas de armadillo con Trial Reset

Saludos Apuromafo