

[Tutorial] Conhecendo o OllyDBG

Alterar um GS ou main usando um Editor de Hex é relativamente fácil (desde que saibamos quais os hex a serem modificados). No entanto, fazemos as alterações sem entendê-las ou entender seu significado.

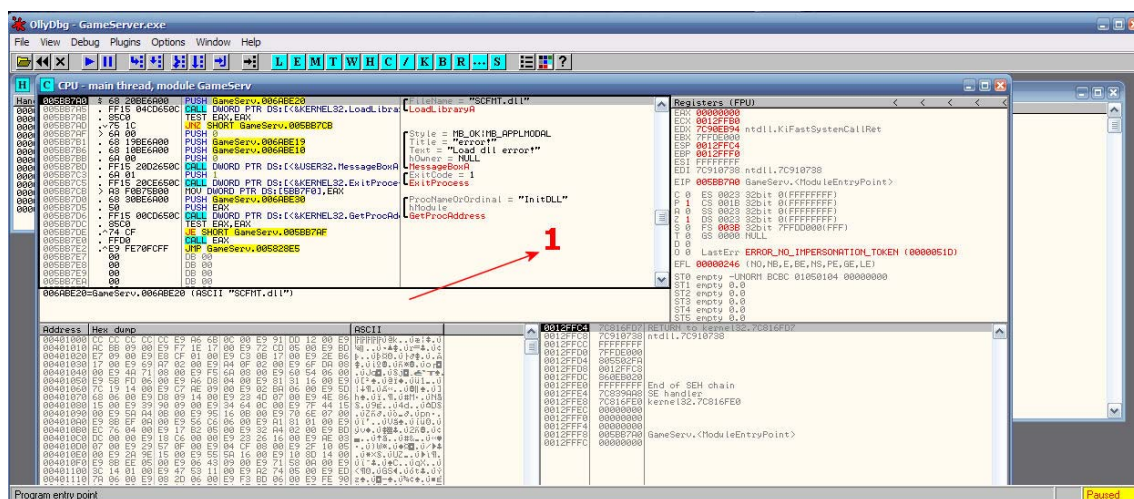
Já alterar o GS ou main usando o OllyDBG, embora mais complicado e difícil, torna o processo mais compreensível e, assim, sabendo onde estão os comandos, fica fácil localizá-los em qualquer versão do GS ou do main...

Assim, vamos conhecer um pouco do OllyDBG e, assim, podermos localizar os comandos, lembrando que é preciso no entanto saber quais os comandos e como eles funcionam...

Para visualizar melhor as imagens, selecione a opção ZOOM no Adobe Acrobat.

Procurar um comando/função

1 - Abra um GS ou main pelo OllyDBG... Nesse momento, não importa a versão a ser usada, pois vamos apenas conhecer algumas funções básicas desse programa... Ao abri-lo, você terá a seguinte imagem:



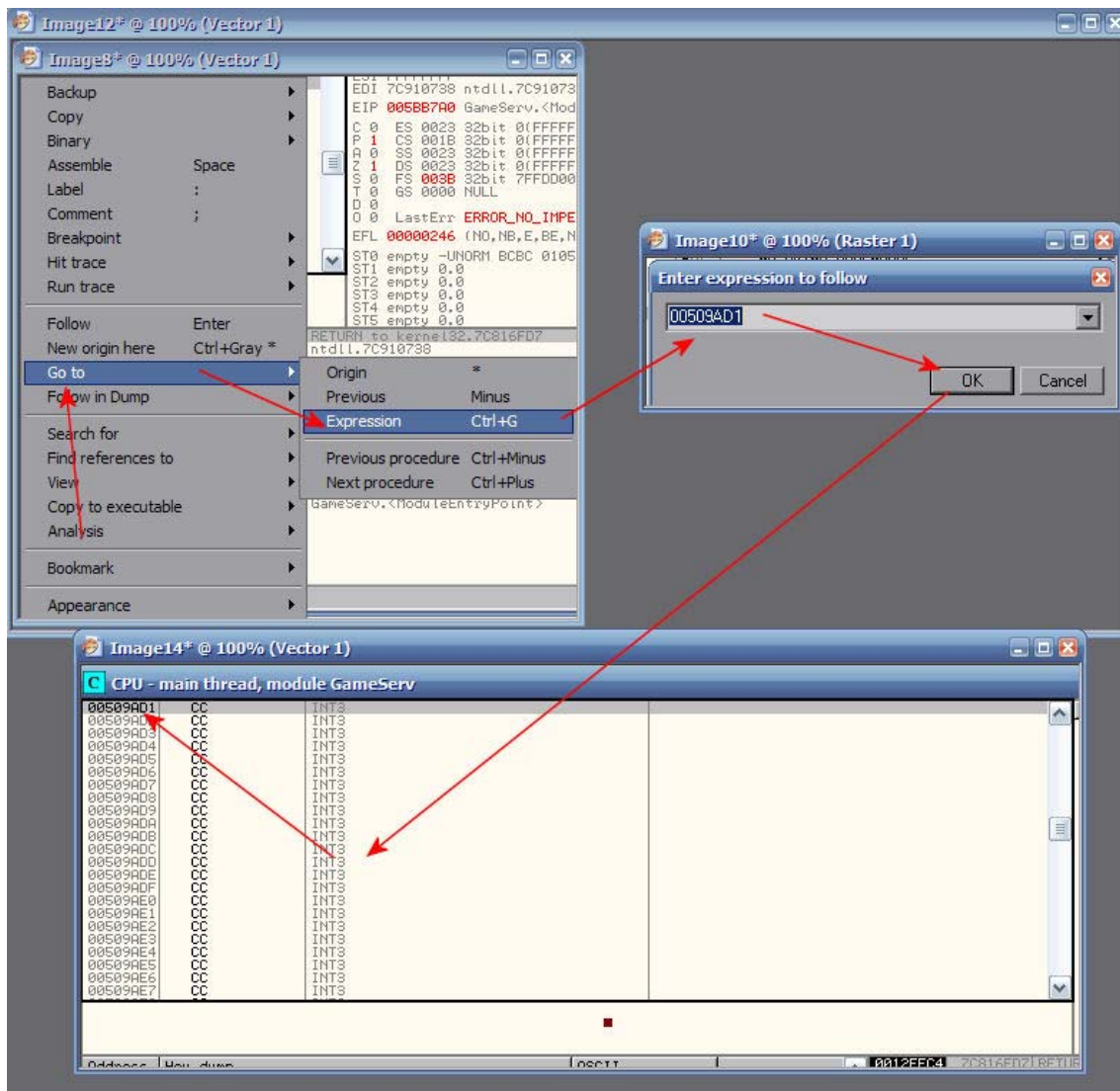
2 - Ao clicar com o botão direito na parte superior do programa (indicada pelo número 1), será aberta uma janela com várias opções:



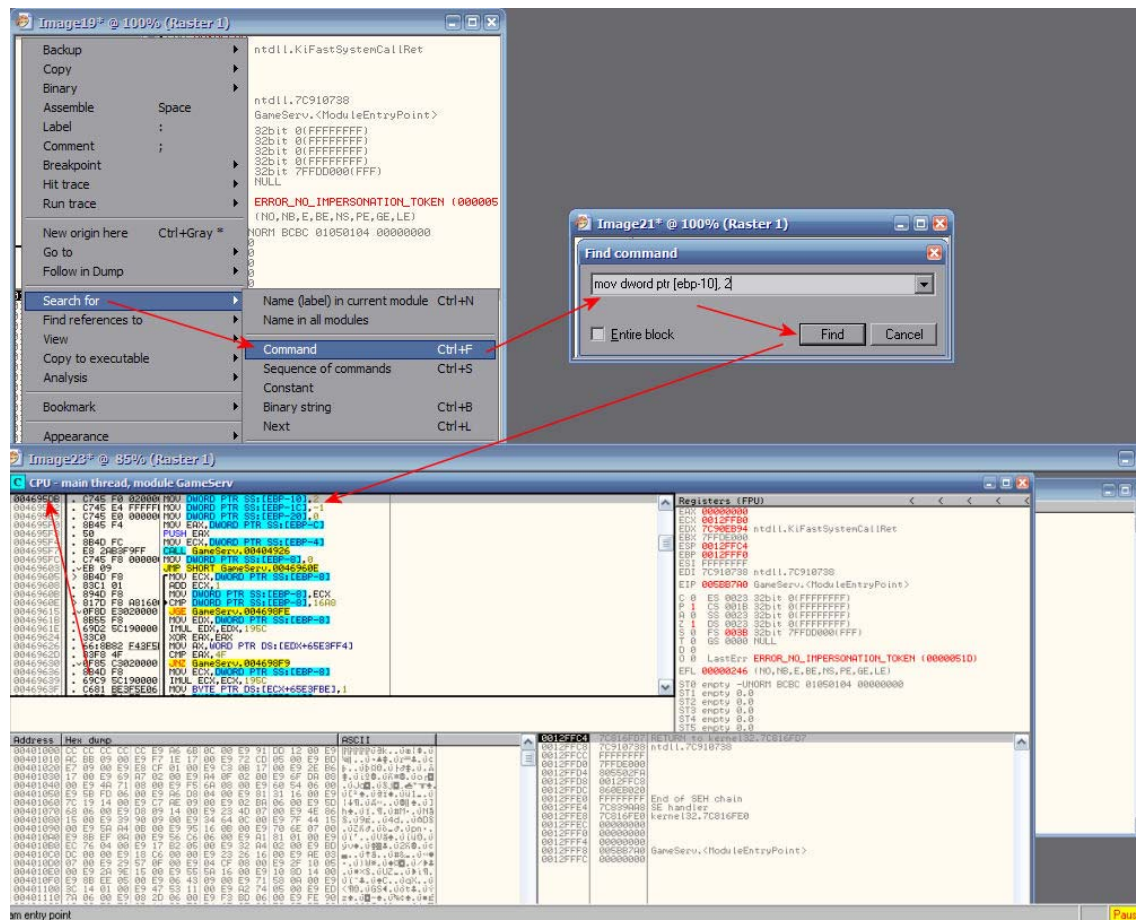
Como não conheço ainda todas as funções, vou explicar somente as básicas e que são as necessárias para fazermos algumas alterações nos arquivos...

3 – Quando queremos procurar um offset (isso quando sabemos qual o offset que queremos), selecionamos a opção Go to -> Expression, ou simplesmente pressionamos as teclas CTRL G. Será então aberta uma janela, onde colocamos o offset e pressionamos OK. Isso nos levará ao offset desejado:

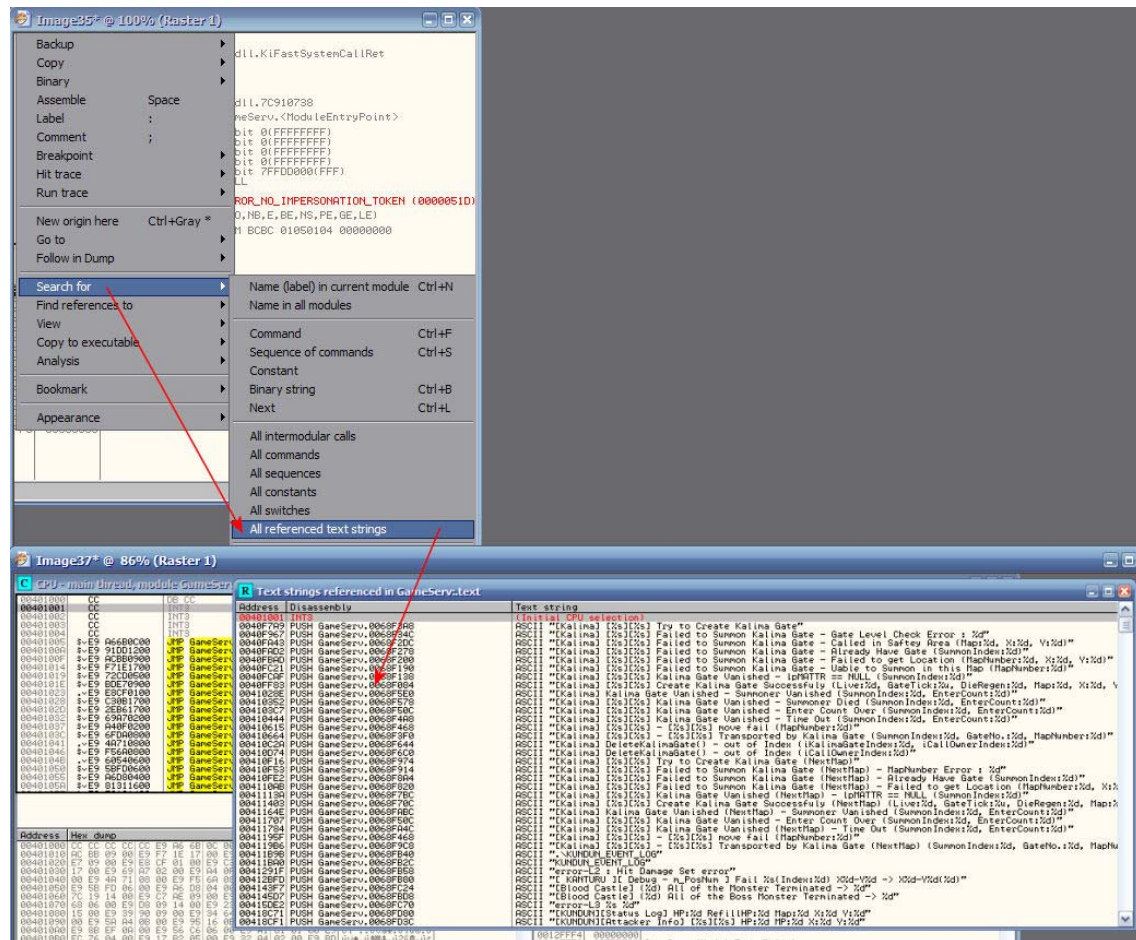
IMPORTANTE: Sempre que for procurar uma função, coloque o Scroll no início do arquivo.



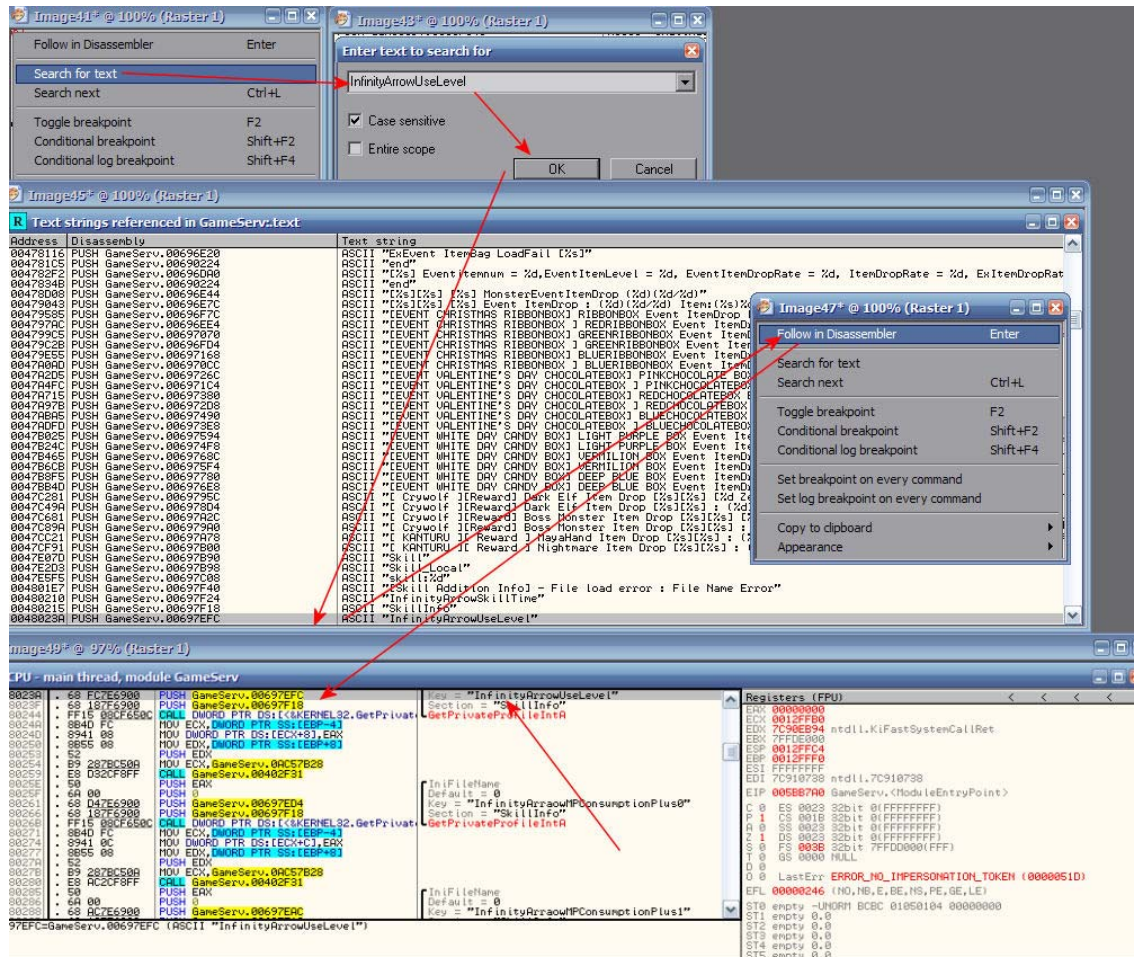
4 – Se não temos o offset e queremos localizar o comando/função, a busca deverá ser feita então pela opção Search for -> Command (ou simplesmente CTRL F). Será aberta então uma janela, onde deveremos colocar o comando que queremos localizar.



6 – Por último, há ainda outra maneira de localizar uma informação: através do ASCII. Para isso, selecionamos a opção Search for -> All referenced text strings, sendo aberta então uma janela com todos os ASCII.



7 – Clique então com o botão direito nessa janela que se abriu e selecione a opção Search for text e na janela que abrir digite o ASCII que pretende localizar. Ao clicar em OK, será mostrada a linha onde se encontra o ASCII. Clique então com o botão direito e selecione a opção Follow in Disassembler (ou simplesmente pressione a tecla ENTER ou ainda clique duas vezes na linha do ASCII).



Fazendo alteração e salvando

Para as explicações, vamos alterar então os monstros dos anéis de transformação. Vamos usar então um GS 1.00.16 (lembrando que isso poderá ser feito em QUALQUER versão de GS). É importante ressaltar que muitos coders colocam a opção de alterar esses monstros em um arquivo *.ini. Mas, como o objetivo desse tutorial é explicar como fazer uma alteração no GS e salvá-la, não vamos nos preocupar com isso...

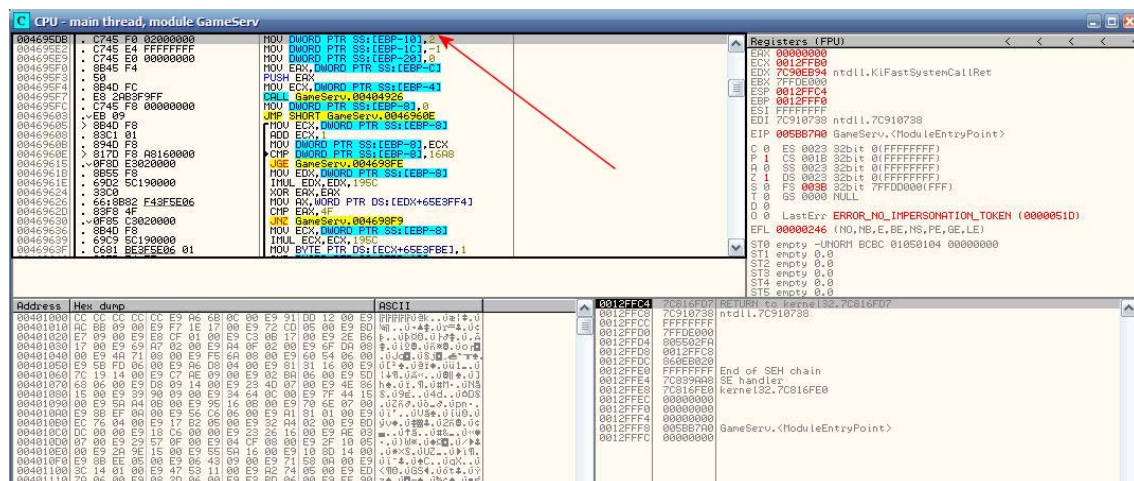
Já sabemos quais são os comandos dos anéis de transformação e seus hex. Mas não sabemos os offsets em que eles se encontram. Assim, vamos fazer uma busca dos comandos usando a opção Search for -> Command (ou simplesmente CTRL F).

Os comandos para os anéis de transformação são:

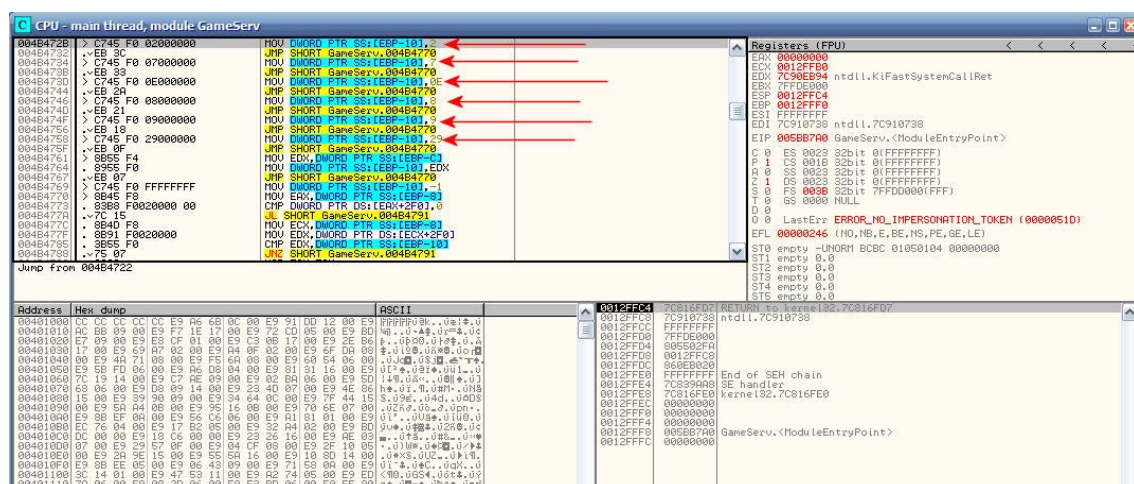
```
mov dword ptr [ebp-10], 2
mov dword ptr [ebp-10], 7
mov dword ptr [ebp-10], 0E
mov dword ptr [ebp-10], 8
mov dword ptr [ebp-10], 9
mov dword ptr [ebp-10], 29
```

O mesmo processo pode ser feito no GS-CS, lembrando que as alterações devem ser idênticas, para que um char, ao mudar de GS, usando anel de transformação, mantenha a mesma aparência.

1 - Abra então o GS no OllyDBG. E selecione então a opção Search for -> Command (ou simplesmente CTRL F). Na janela que vai se abrir, digite então -> mov dword ptr [ebp-10], 2. E pressione OK. Você será "levado" para o offset 004695DB. No entanto, essa linha NÃO se refere ao anel de transformação, já que os comandos dos anéis ficam bem próximos.



2 - Assim, pressione novamente CTRL F e em seguida clique em OK (não escreva nada, pois continuaremos procurando pelo comando do anel de transformação). Repita esse processo quantas vezes for necessário, até localizar o comando correto. Repare na imagem abaixo como os comandos dos anéis de transformação estão próximos.



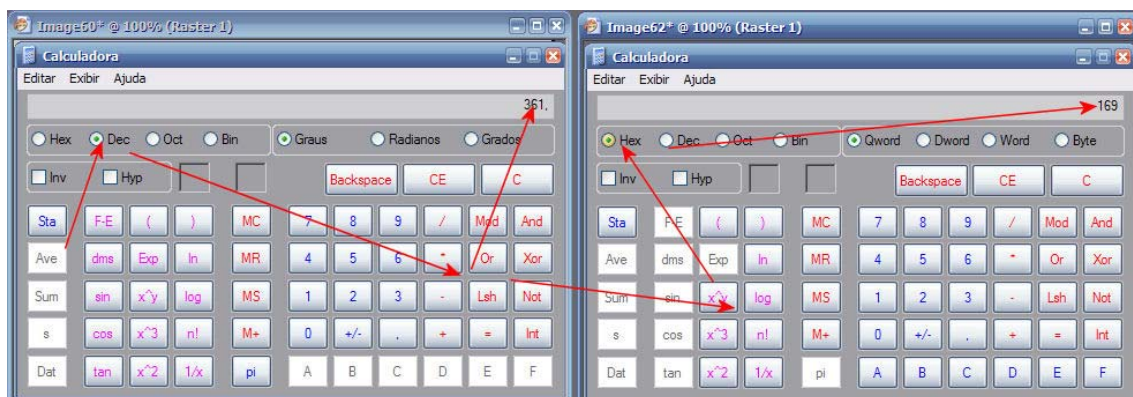
3 - Agora vamos então mudar o monstro do anel de transformação 1. Por padrão, o monstro do anel de transformação 1 é o Budge Dragon. Vamos então alterar o GS para que quando um personagem usar esse anel se transforme no Nightmare.

4 - Abra então o arquivo Monster.txt e procure por esse monstro e anote seu ID. No caso, o ID do Nightmare é 361. Agora, precisamos descobrir como transformar esse número, que está em número decimal, em número hexadecimal. Para isso,

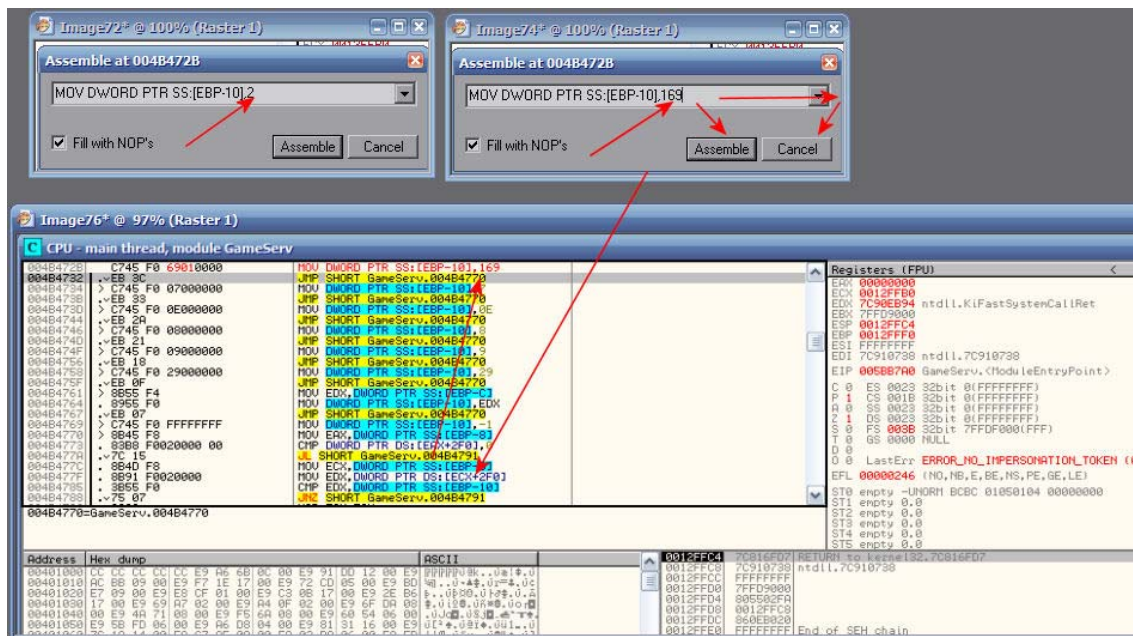
abra a Calculadora do Windows, certificando-se que ela está na opção Calculadora Científica (Exibir -> Científica).



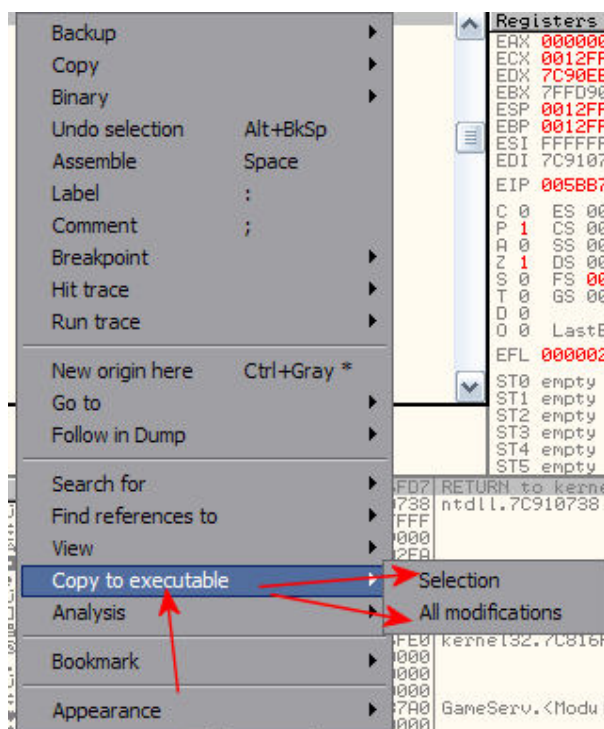
5 – Selecione então Dec e digite 361 (que é o ID em Dec do Nightmare). Em seguida, selecione Hex e verá o ID do monstro, que no caso é 169.



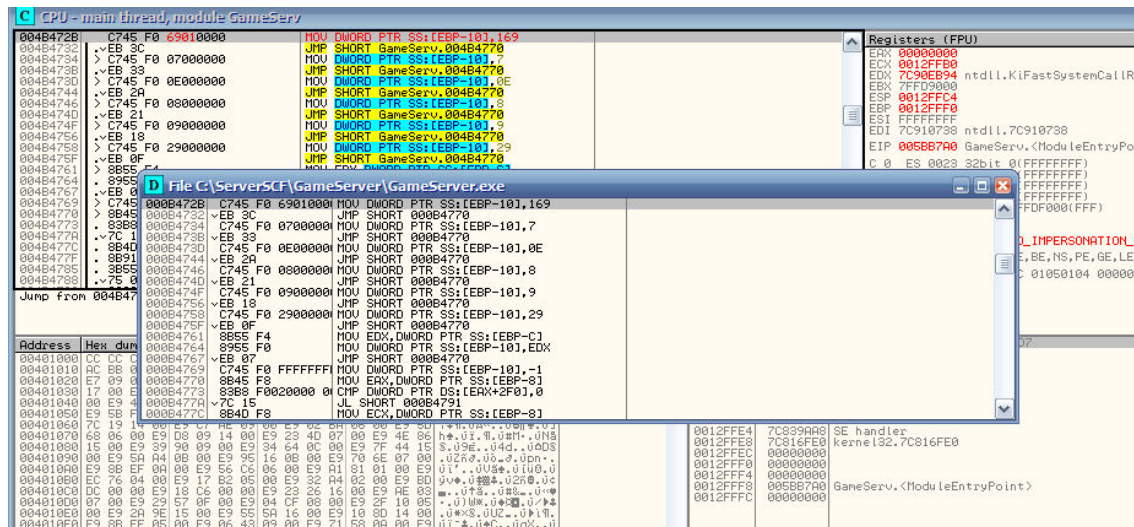
6 – Voltamos então para o OllyDBG e, já tendo localizado o comando, vamos fazer a alteração. Clique duas vezes então na linha do comando e será aberta a janela do Assemble. Substitua então o número 2 pelo 169. Clique em Assemble e em seguida em Cancel, para fechar a janela. Repare então que foi mudado o comando e que a linha está vermelha.



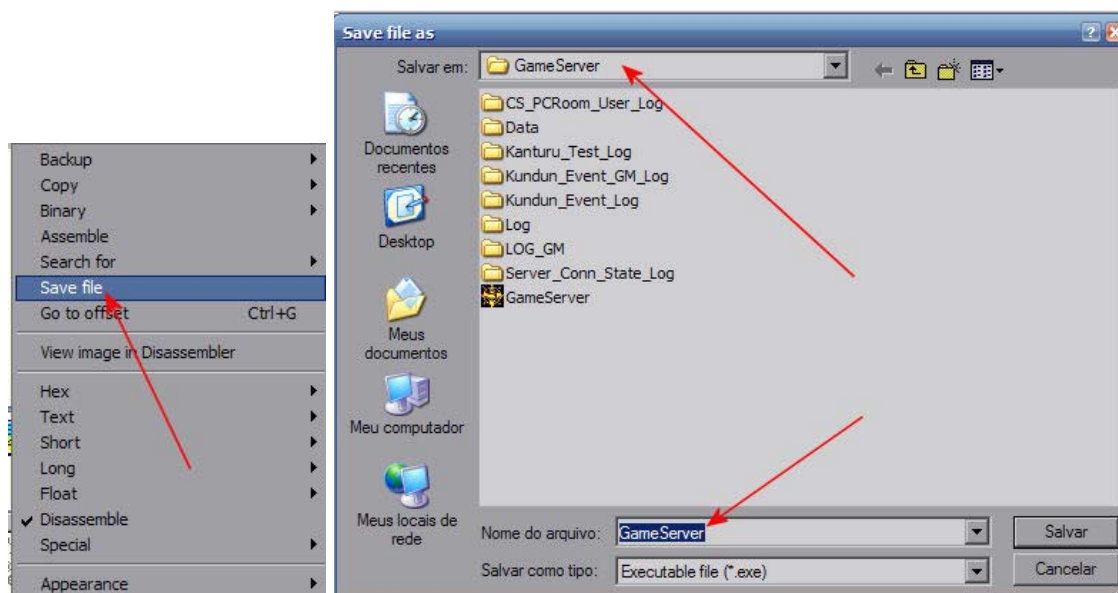
7 – Antes de continuar com as alterações, vamos verificar se podemos fazer todas as alterações antes de salvá-las ou se precisaremos salvar individualmente cada alteração feita... Para isso, clique com o botão direito e selecione a opção Copy to executable. Se aparecem as opções Selection (salva apenas a linha alterada) e All modifications (salva todas as alterações feitas), você pode continuar fazendo as alterações e salvar tudo no final. Caso só apareça a opção Selection, você terá de salvar individualmente cada alteração. Mas o processo é basicamente o mesmo.



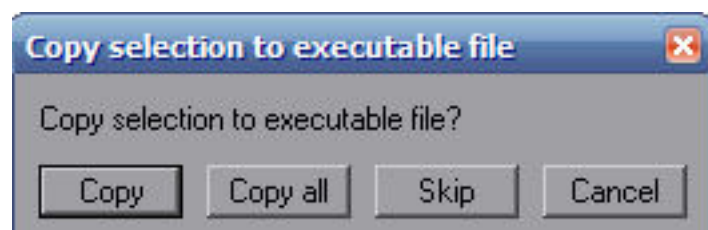
8 – Ao selecionar qualquer uma dessas opções, será aberta uma nova janela, onde irão aparecer as alterações (uma alteração, se for selecionada a opção Selection, ou várias se for selecionada a opção All modifications).



9 – Clique nessa nova janela com o botão direito e selecione a opção Save File. Caso você tenha selecionado anteriormente a opção Selection, ao clicar em Save File será aberta uma janela onde você poderá escolher o diretório e o nome do arquivo a ser salvo.



10 – Caso faça mais de uma alteração e selecione a opção All modifications, será aberta uma janela onde deverá ser selecionada a opção Copy all. Na janela seguinte, clique com o botão direito e selecione Save file, escolhendo então o diretório e o nome do arquivo a ser salvo.



ATENÇÃO: Não importa se salvar uma alteração por vez ou todas as alterações de uma só vez, depois que terminar o processo, abra novamente o GS no OllyDBG.

Observações importantes

1 – Sempre que for alterar um arquivo, faça antes uma cópia para o caso se errar e precisar restaurar o arquivo original.

2 – Teste sempre o arquivo para verificar se as alterações não causou nenhum bug.

3 – É importante ressaltar que alguns códigos (comandos/funções) podem variar de um GS para outro. Assim, antes de fazer uma alteração, certifique-se que vai alterar o comando correto.

4 – Quando encontrar nos fóruns algum fix em hex, procure por ele no GS pelo Olly e anote o offset do comando. Em seguida, faça a alteração usando um Editor de Hex e abra novamente o GS com o Olly e procure o offset anotado anteriormente. Assim, você saberá o que foi mudado e poderá fazer a alteração em outro GS usando o Olly.

Tutorial elaborado por chris05 – DSTeam.

Agradecimentos especiais a rodrigobmg, testando e welcomevoce, que me ensinaram a mexer com o Olly.

SP – 09/10/2007