How to make nice search & replace patches...

Tools i used for this tutorial

- Ollydbg www.ollydbg.de
- dUP 2 www.diablo2oo2.cjb.net

Why search & replace?

The answear is simple: while usual offset patcher in most cases work only for a certain version of the target, a search & replace patch can work for all future versions if it’s made good.

Some rules...

There are just some rules you need to follow to make good s&r patch. You also need good assembler and coding knowledge.

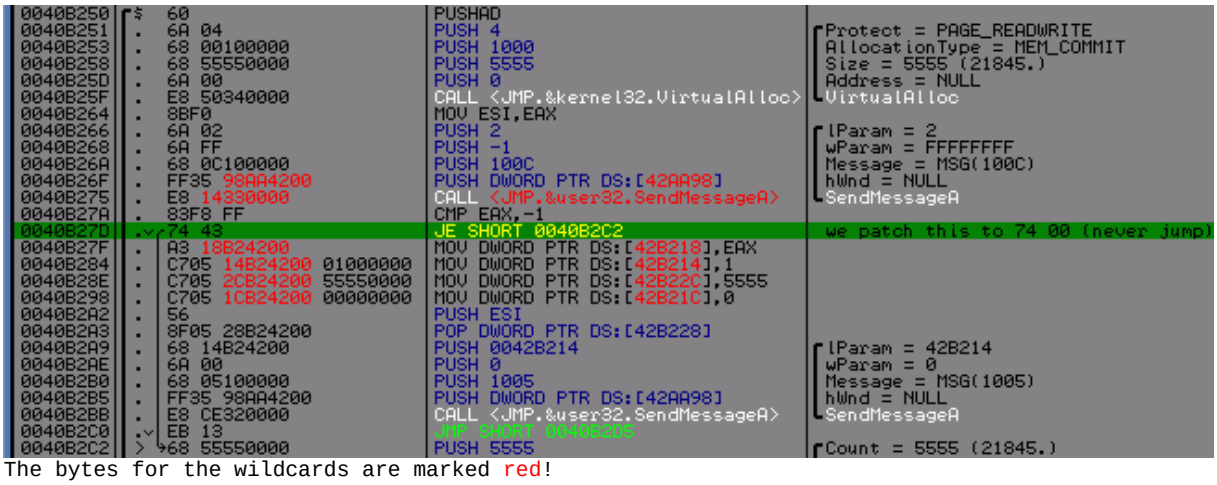
- the searchpattern is searching for a unique command sequence
- always use wildcards (??) for
  - **CALL’s**
    ASM Code : CALL ?? ?? ?? ??
    Searchpattern : E8 ?? ?? ?? ??

  - **Memory Addresses**
    ASM Code : CMP BYTE PTR [?? ?? ?? ??],1
    Searchpattern : 80 3D ?? ?? ?? ?? 01

  - **Long Jumps**
    ASM Code : JE LONG ?? ?? ?? ??
    Searchpattern : OF 84 ?? ?? ?? ??

  This are the most important examples for wildcard usage!

An Example...



The bytes for the wildcards are marked red!

You want to patch the jump @0040B27D so that it never jumps

```
0040B27D   |. /74 43                    JE SHORT 0040B2C2
```

↓

```
0040B27D   |. /74 00                    JE SHORT 0040B27F
```

We will search for this code sequence:

```
PUSH 2
PUSH -1
PUSH 100C
PUSH DWORD PTR DS:[?? ?? ?? ??]
CALL <?? ?? ?? ??>
CMP EAX,-1
JE SHORT ??
MOV DWORD PTR DS:[ ?? ?? ?? ?? ],EAX
MOV DWORD PTR DS:[ ?? ?? ?? ?? ],1
MOV DWORD PTR DS:[ ?? ?? ?? ?? ],5555
MOV DWORD PTR DS:[ ?? ?? ?? ?? ],0
```

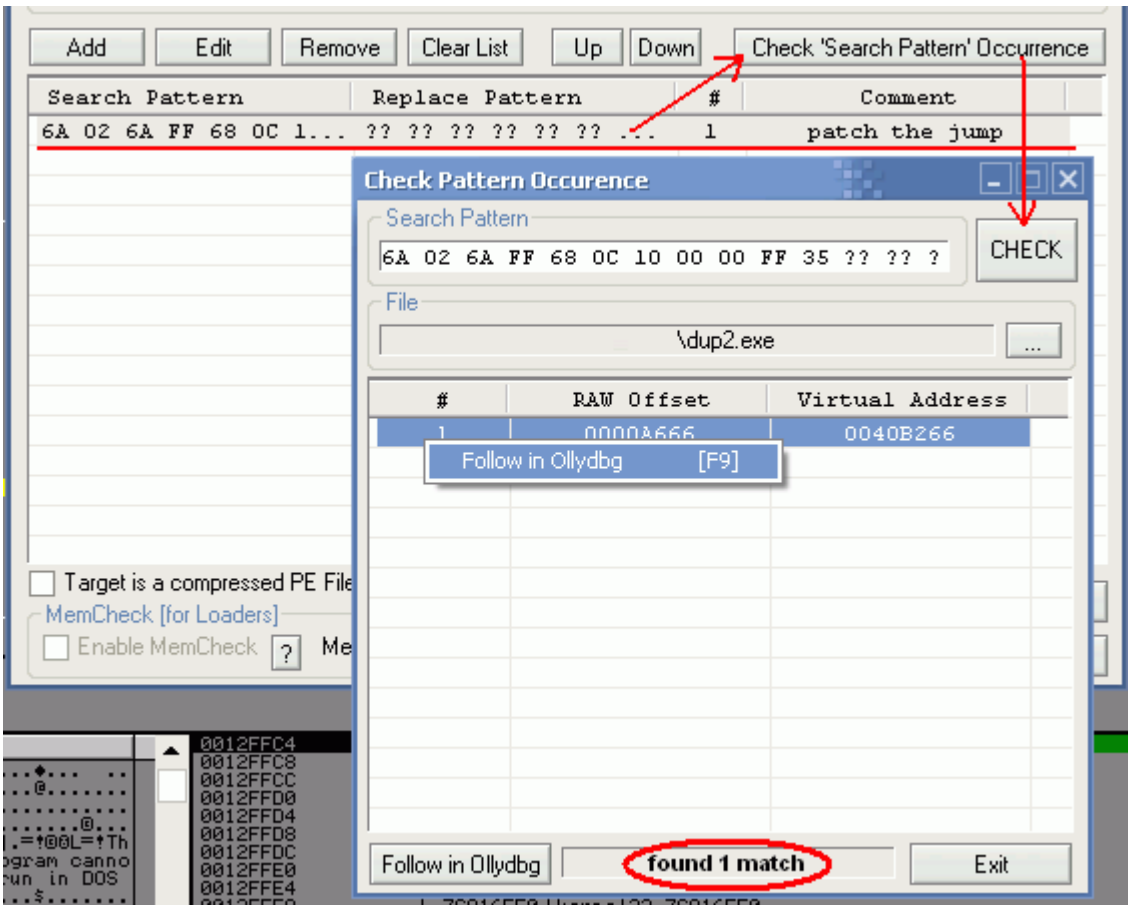
The searchpattern would look like this:

```
6A 02 6A FF 68 0C 10 00 00 FF 35 ?? ?? ?? ?? E8 ?? ?? ?? ?? 83 F8 FF 74 ?? A3 ?? ??
?? ?? C7 05 ?? ?? ?? ?? 01 00 00 00 C7 05 ?? ?? ?? ?? 55 55 00 00 C7 05 ?? ?? ?? ??
00 00 00 00
```

And the replacepattern:

```
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? 00 ?? ?? ??
?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ?? ??
?? ?? ?? ??
```

Now start dUP 2 and enter the search- and replacepattern. Then use the function “Check occurrence”:



dUP 2 will check how often it can find our searchpattern. The result should be **one match** only! After the check you can use the function “Follow in Ollydbg” to be sure that it’s the right pattern.

What to do if there is more than one match?

- Use a longer pattern
- Use less wildcards (but carefully!)

I hope it wasn’t too hard to understand. ;D