Forum

FAQ   Calendar   Forum Actions ▾

Advanced Search

🏠 Forum ▹ CM 01/02 Updates ▹ Patches ▹ Tutorial: Using OllyDbg to patch your CM .exe

Thread: Tutorial: Using OllyDbg to patch your CM .exe

Thread Tools▾

📄 13-09-14,   11:15 PM   #1

bine ye ○
Hot Prospect for the Future

Join Date:	23-03-12
Location:	An Dún, Éire
Posts:	187

Tutorial: Using OllyDbg to patch your CM .exe

Here is a simple (I hope!) tutorial on how to make some basic changes to your CM .exe file.

EDIT: The example I used below is only available when your exe has been patched to 3.9.68 and then using a Tapani 2.xx patch. The following steps are just to show how any offset can be changed. (Cheers for the heads up CF!)

First, you will need to download OllyDbg from the following link:
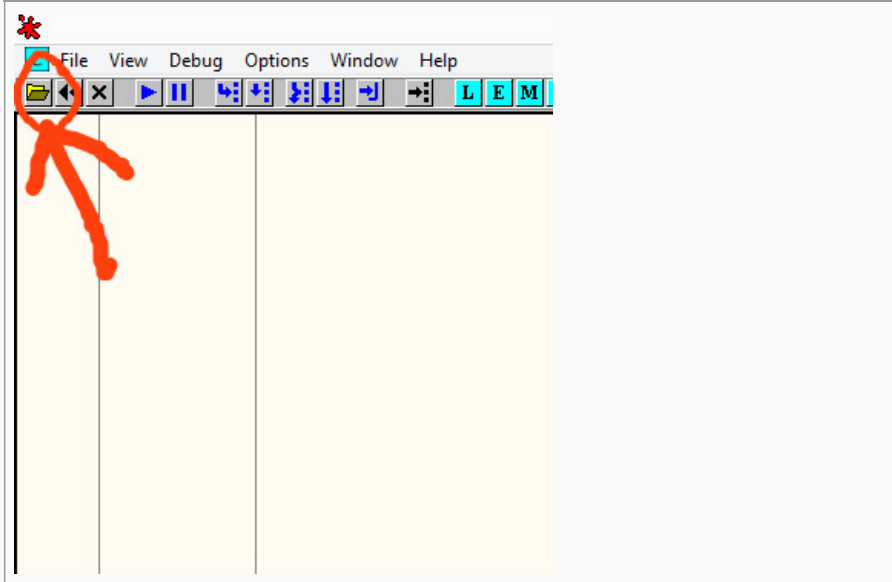http://www.ollydbg.de/download.htm

Now, we are ready to find a change to make to our CM executable. Oh look, I don't like the fact that the Premier League allows 7 subs, let's lower that amount.
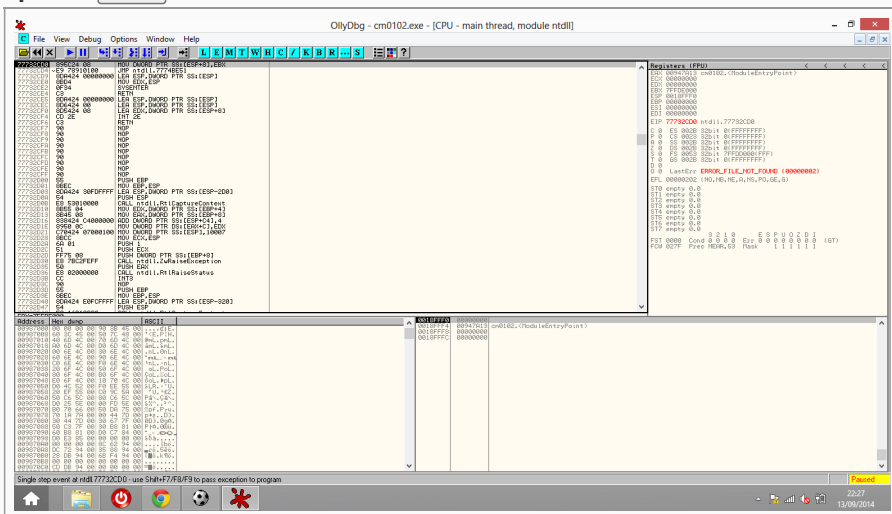
Spoiler! [Show]

Open your OllyDbg program and open your CM exe. This is normally located in your "C:\Program Files (x86)\Championship Manager 01-02" folder unless you have moved this.

Spoiler! [Show]

Now, you should see lines of scary looking nonsense! (Let's hope this makes sense later!)

Spoiler! Show

Next, find the offset you need from one of the numerous threads where the site's resident experts have already located this information for you. For example, we would find ours in the Offsets thread.

http://www.champman0102.co.uk/showthread.php?t=68

For this example, the number of subs offsets for all competitions are listed in a single post at the link below. How convenient! 🙂
http://www.champman0102.co.uk/showth...&p=131#post131

Spoiler! Show

Patinoz ○
Director
Manager
VIP

Mia san mia

Thanks.

I have just written a short tool to scan the .exe file for all the substitute offsets, here is the definitive list of v

Code:

```
45bc12 - Brazilian Santa Catarina State Championship
51497a - Croatian A1
515e7c - Croatian A2A
516f9a - Croatian A2B
5174e9 - Croatian Cup
550a8c - Danish Cup *
5516d3 - Danish Cup *
552437 - Danish First
553a89 - Danish Premier
56aab5 - Englsih Auto Cup
56c317 - English Conference Cup
56d3e9 - English Charity Shield
56ee5a - English Conference
572e0d - English First (now Championship)
574c03 - English Premier
5767fe - English Second (now First)
578159 - English Third (now Second)
57a16e - European Super Cup
57b6b5 - European Championships
57e976 - European Champions League Qualifiers
58383f - European Championsn League
58be1b - Fifa Confederations Cup
5922b9 - Finnish Cup
593c06 - Finnish First
595cfa - Finnish Premier
5bc489 - French First
5bf134 - French Second
5d8c89 - German Cup
5db489 - German First
5dc1aa - German League Cup
5dcba3 - German Regional
```
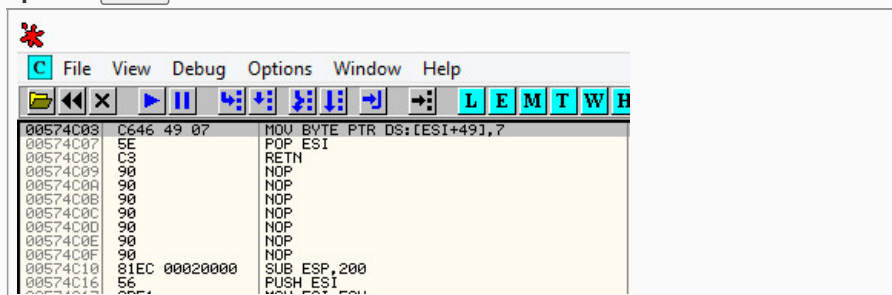
Our required offset as seen in the picture is 574C03.

Return to OllyDbg, click anywhere in the main panel and press Ctrl + G, entering your new found offset.
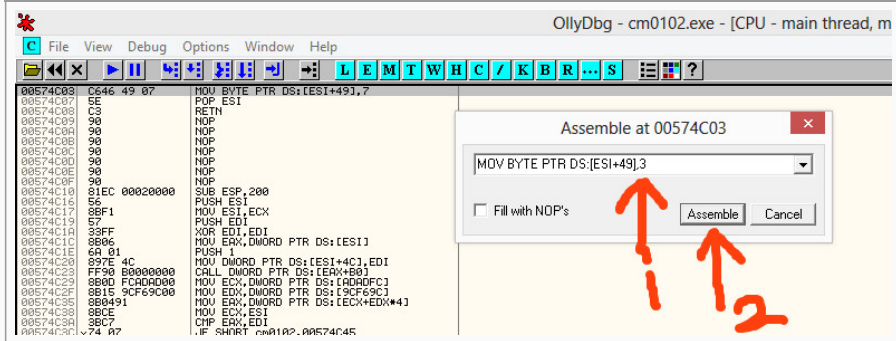
Spoiler! [Show]
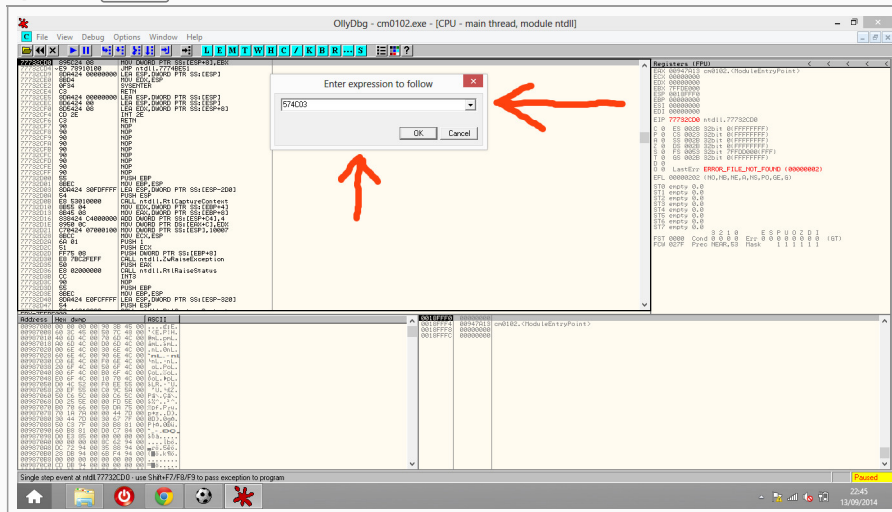
This will take you to the exact location of the information in the executable where the exe tells the game how many subs can be named in this competition. You should see the line as below:
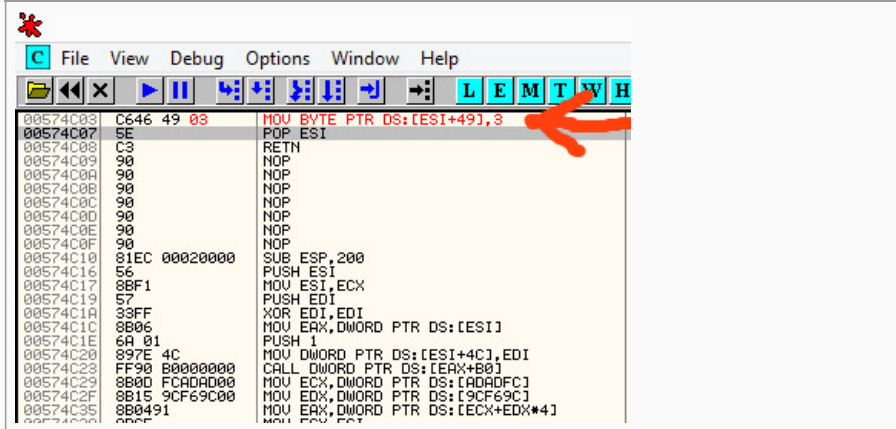
Spoiler! [Show]

You will need to change the '7' at the end of this line, as this is the number of subs allowed. But let's say we only want to allow 3 subs, because we are evil like that! 😈
So we change the 7 to 3, simply by double clicking on the line and editing as shown, then click assemble, followed by 'Cancel':

Spoiler! [Show]

Any changes will be highlighted in red:
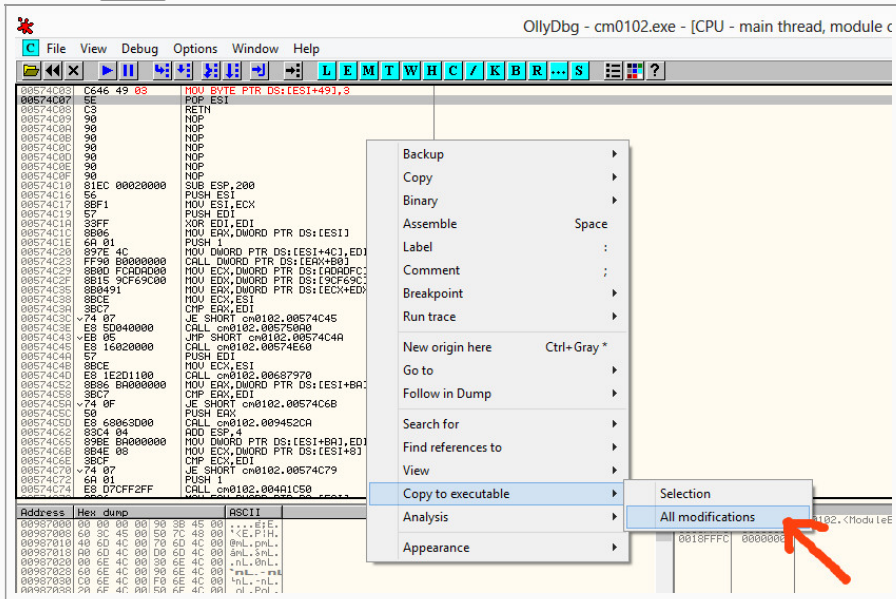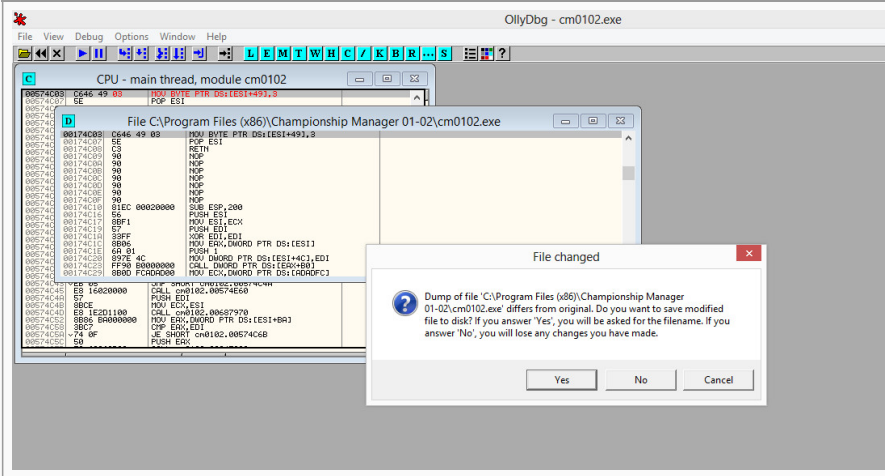
Spoiler! [Show]

Now, we are ready to test the changes. You will need to save your exe. Right click on the main panel, scroll down to 'Copy to executable', followed by 'All Modifications'. Then choose 'Copy all'.

Spoiler! [Show]

Now, click the 'X' to close the new window that appears, and a warning message appears asking you to save the changes.

Spoiler! [Show]

Click yes, and give your exe a DIFFERENT name to your current exe. (This is in case you have made any mistakes and you can revert back to before you made any changes!)

Spoiler! [Show]
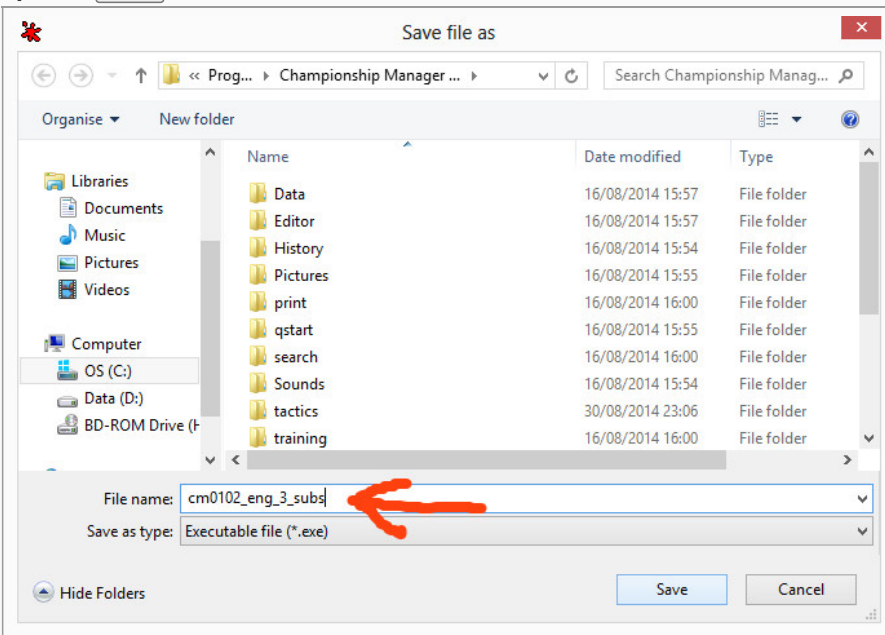
Now, load up the game through your new exe file. (Remember to set compatibility and 'Run as admin' on your new exe. You can do this by right clicking on your new file, choosing 'Properties' and the 'Compatibility' tab. Most computers will run the game in 'Windows 98 / ME' mode, and tick 'Run as administrator'. If you forget this, especially on Windows 8, the game may not load!)

Spoiler! [Show]
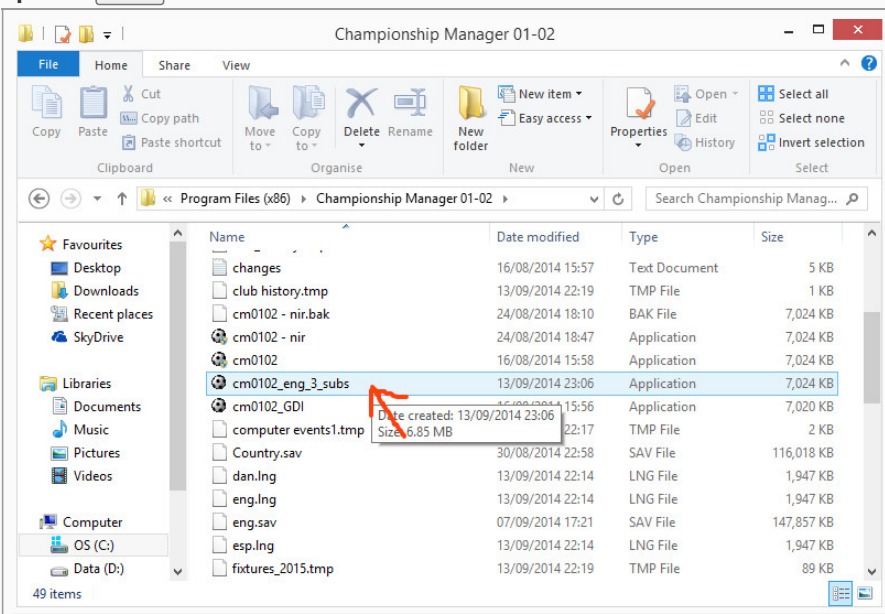
Then, we go load up the Premier League. Let's hope this works!

Spoiler! [Show]

And there you have it! The damn Premier League going and changing the rules on us 35 days before the start of the season!

You can use the above steps to make many changes to the exe, the above was to show how a change can be made. There is many great changes that you can do to make your game easier, harder, or just more wackier and fun! Have a read at the offsets thread at the link above for more offsets that you can apply and use. 🙂

Last edited by bine ye; 14-09-14 at 12:43 AM.

Craig Forrest ○
Manager
Programmer
Forum Enforcer
Holy Trinity Member

Join Date: 02-03-12
Location: The Great White
North
Posts: 4,502

Just an FYI though..... you can only change the subs in England if you've applied a Tapani patch.... the vanilla EXE does not have that line of code 😄👎

---

bine ye ○
Hot Prospect for the Future

Join Date: 23-03-12
Location: An Dún, Éire
Posts: 187

I was hoping people weren't going to use it as a 'Change England subs' tutorial, but instead as a 'Change any offset' tutorial 🙂

Craig Forrest ○
Manager
Programmer
Forum Enforcer
Holy Trinity Member

Join Date: 02-03-12
Location: The Great White
North
Posts: 4,502

no I get it.... but if a n00b tries that for the first time using Olly and can't find the offset then it might put them off....

---

bine ye ○
Hot Prospect for the Future

Join Date: 23-03-12
Location: An Dún, Éire
Posts: 187

Updated OP. Cheers 😄👎

eddieC ○
Reserve Team Player

Join Date: 27-08-14
Posts: 308

This is brilliant exactly what I was asking for in the offest thread!!! 😎

So glaad this has finally been done....

please if anyone can give another examples for doing differnt offset's... please do so

This was explained so well for begginers, thanks
bine ye

VERY VERY greatful! 🔥

Craig Forrest ○
Manager
Programmer
Forum Enforcer
Holy Trinity Member

Join Date: 02-03-12
Location: The Great White
North
Posts: 4,502

the other offsets follow the same principle... value 'a' needs to be changed to value 'b' in order to alter the exe in some way

JohnLocke ○
Programmer
VIP

Join Date: 05-06-12
Posts: 1,032

> 📖 Originally Posted by **Craig Forrest** ▶
>
> *Just an FYI though..... you can only change the subs in England if you've applied a Tapani patch.... the vanilla EXE does not have that line of code* 😊👍

Or you could add the missing line yourself...
Original exe:
00574C03 POP ESI
00574C04 RETN

To modify thism double-click on 'POP ESI' and type in 'MOV BYTE PTR DS:[ESI+49],7' (change the 7 if you want more or less subs). This will overwrite the above two lines - so you'll need to puth them back. So double-click the 'NOP' which is now below the line you've just added and enter 'POP ESI' then repeat and enter 'RETN'.

You can do the same thing with subs you can use - just add the following line as well 'MOV BYTE PTR DS:[ESI+4A],7'.

Note - NOP is the code for 'No Operation', overwriting any other code would almost certainly have negative conseqeunces.

eddieC ○
Reserve Team Player

Join Date: 27-08-14
Posts: 308

Thanks John

Any chance you could upload some scrrenshots on how this is done, just until newbs like myself get to grips with the procedure...... it would be greatly appreciated 🙂

I mean, I think the whole point of this thread, is to familiarize people with the ollydb program, and screenshots of how each step is done would make all these numbers and codes, make alot more sense for people like myself, unfamiliar with ollydb... I understand this may be time consuming, so if you cant find the time, i totally understand.

cheers dude

*Last edited by eddieC; 14-09-14 at 12:57 PM. **Reason:** ammendment*

You shouldn't need screenshots for this, if you are running the stock 3.9.68. It is as the OP, except when you search for 574C03, you should have POP ESI highlighted. Double click this, and add the lines JL mentioned and click assemble. To clarify what JL was saying, the NOP is free space in the exe and is in most cases here you can overwrite. It will not always be the case as the game needs some of these free spaces to write to during the game run time.

To break this down:
* Find 574C03 - POP ESI, and double click on this to write your new line.
* Write out "MOV BYTE PTR DS:[ESI+49],VALUE"
(Where VALUE is your number of subs to be named, between 0-9)
* Click assemble.
* Write out "MOV BYTE PTR DS:[ESI+4A],VALUE"
(Where VALUE is your number of subs to be used, between 0-9, should be same or lower as the above to be named, not higher)
* Click assemble.
* Write "POP ESI"
* Click assemble.
* Write "RETN".
* Click assemble.

Then return to the OP and continue from the steps about testing your changes.

I appreciate that mate, I really do but let me try to expalin this better... when you say:

"* Find 574C03 - POP ESI, and double click on this to write your new line.
* Write out "MOV BYTE PTR DS:[ESI+49],VALUE"
(Where VALUE is your number of subs to be named, between 0-9)
* Click assemble.
* Write out "MOV BYTE PTR DS:[ESI+4A],VALUE"
(Where VALUE is your number of subs to be used, between 0-9, should be same or lower as the above to be named, not higher)
* Click assemble.
* Write "POP ESI"
* Click assemble.
* Write "RETN".
* Click assemble."

All I see is... "789072365780bf3460n8cv0gn6f-935827fm-023876md9-823749tb87234tc69-8 Click assemble"

ha ha ha

In all fairness tho... I haven't actually attempted to do this yet... so I might be able to do it once I try it a few times....

Thanks for the Instruction mate.. 🙂

> 🗩 Originally Posted by **edcrowley100** ▸
> when you say:
> All I see is... "789072365780bf3460n8cv0gn6f-935827fm-023876md9-823749tb87234tc69-8 Click assemble"
> ha ha ha

Look we are only trying to help. How can you say that when you haven't even opened the program to see what we are explaining? I have given you 4 lines to change, and told you exactly what changes need to be made to modify the subs named and subs used for the English Premier League. Why don't you go and try it first before posting stuff like that?

wonderful tutorial bine ye 🔧

now, question time 😁

do i need a fresh install or is it fine having two exe's in the same folder? i mean, if i create the second modified exe, am i still able to use the clean one without problems?

also, this is for everyone, some months ago i was trying to create a full ordered (by nation & by subject) list of all the offsets found out so far, would it be helpful?

#15

JohnLocke ○
Programmer
VIP

Join Date: 05-06-12
Posts: 1,032

Two exes is fine - my CM folder currently has 18 different exes in it.

#16

bine ye ○
Hot Prospect for the Future

Join Date: 23-03-12
Location: An Dún, Éire
Posts: 187

No, you can have as many exe files in one folder as you wish. It's only when you have 2 or more data folders together that problems start! Sure when you install the game, you have 2 exes by default, 'cm0102.exe' and 'cm0102_GDI.exe'. 🙂

And your other point, JL has started something like that already, it is stickied in the Patches thread under 'The Offsets Index'.

#17

eddieC ○
Reserve Team Player

Join Date: 27-08-14
Posts: 308

I see my humor doesn't translate on here too well...

Sorry Bin, i was only joking dude.... didn't mean to come acrossy as being a bit arsey, believe me i'm not.... I'm extremely greatful for any advice you guys have to give

Sorry for the misunderstanding mate

#18

Jesus ○
First Team Player

Join Date: 04-03-12
Posts: 3,459

> 👀 Originally Posted by **edcrowley100** ▷
>
> *I see my humor doesn't translate on here too well...*
>
> *Sorry Bin, i was only joking dude.... didn't mean to come acrossy as being a bit arsey, believe me i'm not.... I'm extremely greatful for any advice you guys have to give*
>
> *Sorry for the misunderstanding mate*

The internet and humour don't like to get along together sometimes.

#19

eddieC ○
Reserve Team Player

Join Date: 27-08-14
Posts: 308

ha ha tell me about it! It's why I left Facebook! ha

Jesus, you're very wise

Craig Forrest ○
Manager
Programmer
Forum Enforcer
Holy Trinity Member

Join Date: 02-03-12
Location: The Great White
North
Posts: 4,502

He IS Jesus you know....

---

eddieC ○
Reserve Team Player

Join Date: 27-08-14
Posts: 308

---

ivicamlacko ○
Youth Team Player

Join Date: 01-10-12
Posts: 5

hi,why I cant open offsets? I want to make some changes in Croatia league

---

saturn ○
Programmer
VIP

Join Date: 18-03-14
Posts: 1,240

A lot of times when wanting to change one line in the middle of a block of code, the new line is a couple of bytes larger. This results in us having to do some tedious copying and pasting of the lines that the new line of code has overwritten, all the way down to the end of the block of code, line by line. Here's how to copy and paste large chunks of lines in one go.

I'm going to use the Italian Cup team selection code as an example. I wanted to revert Tapani's code in 2.21.1 to see whether .68's original code worked with my 20/22 Italian league structure. The new team selection code begins at 0063FAF0 in 2.21.1 and lasts until 0063FCB9 (or at least the code stops looking like gibberish in Olly then). So this is what we'll be NOPing and replacing with the original .68 code.

Next we've to get the original code, so open up the vanilla .68 exe in Olly. Go to 0063FAF0 again and click on the line. Scroll down to 0063FCB**6** (don't CTRL+G) and, holding Shift, click that line too. All the lines between those two addresses should now be grey. Right click on any of the lines and go to Binary -> Binary copy.

Open up a text editor (Notepad etc) and paste in the contents. You should see "81 EC 8C...20 7D 79". This is what we'll be pasting back into Olly. When pasting we can enter a maximum of 256 bytes at a time. In your text editor your pasted content should be in rows of 32. Count down eight rows and hit enter, which will give you the maximum of 256 (32x8). The first block should end in "...00 00 00" while the second block should begin with "85 C9 74...".

Open up a patched 2.21.1 exe in Olly and go to 0063FAF0 again. Like earlier, select that line and scroll down to 0063FCB6, hold Shift and click that line too. Now right click on any of the lines and go to Binary -> Fill with NOPs. CTRL+G back up to 0063FAF0. Copy the first block of 256 bytes in your text editor and right click on the 0063FAF0 line. Go to Binary -> Edit, right click in the HEX +00 box and select Paste. About half the original code should now be entered. Select the second block in your text editor and paste into the next line in Olly like before. Now the code should all be fully entered, and be identical to the .68 version.

A couple of things to be aware of. Firstly, the first block in the example above happened to end on a "full" command (JL 0063FCA5). I'm not sure what happens if the first block ends in the middle of a command: perhaps the second block will make things look fine when it's entered, or perhaps you'll have to copy and paste that in-between line yourself like we always had to before. Secondly, you'll have to check and make sure that any JMP commands are pointing towards the correct line in your newly pasted code. Everything's fine in my example as it's a true copy and paste job. But if your reason for copying and pasting is because you've wanted to change something like PUSH EAX to PUSH 1 in the middle of the code, be wary that all the code beneath that will be one line off, so things like JMP/JE/JNZ commands will have to be edited accordingly.

Edit: Watch out for the CALL xxx commands not appearing correctly too, you'll have to double-check them aswell.

Last edited by saturn; 25-05-16 at 10:48 PM. **Reason:** *CALL command warning.*

📄 27-07-17,　05:48 PM | #24

Balthazor ○
Youth Team Player

Join Date: 04-06-17
Location: Estonia
Posts: 8

If there were something like Olly for CM97/98 too... it would be possible to change starting day, promotions-relegations and much more easily.

📄 27-07-17,　06:29 PM | #25

Dermotron ○
Sir Mergements
Director
Manager
VIP
Captain

Join Date: 15-12-11
Location: Your Mother
Posts: 29,995

It should work since its just editing an executable (.exe)

Champman0102.co.uk Facebook Page
13000 followers and rising
November 2020 Data Update Out Now

▼ Page 1 of 2　**1**　2　▶　Last ▶▶

« Patch +v5 | Patch +v7 (+v8 in Post #377) »

-- Default Style

Archive　Web Hosting　Top

🏠 Forum ▸ CM 01/02 Updates ▸ Patches ▸ Tutorial: Using OllyDbg to patch your CM .exe

Results 26 to 41 of 41 | ▾ Page 2 of 2 | ◀◀First | ◀ | 1 | **2**

Thread: Tutorial: Using OllyDbg to patch your CM .exe

Thread Tools▾

📄 28-07-17,   03:38 PM   #26

Balthazor ⚬
Youth Team Player

Join Date: 04-06-17
Location: Estonia
Posts: 8

Maybe problem is that CM97/98 can be opened in Win10 only through emulators like
DosBox? I have to try it in some older computer...

edit: and it says Can't open file...

Last edited by Balthazor; 28-07-17 at 03:57 PM.

📄 28-07-17,   03:53 PM   #27

Dermotron ⚬
Sir Mergements
Director
Manager
VIP
Captain

Join Date: 15-12-11
Location: Your Mother
Posts: 29,995

What format are the files in? There are a lot of Hex Editors that might work

Champman0102.co.uk Facebook Page
13000 followers and rising
November 2020 Data Update Out Now

📄 28-07-17,   07:33 PM   #28

Craig Forrest ⚬
Manager
Programmer
Forum Enforcer
Holy Trinity Member

Join Date: 02-03-12
Location: The Great White
North
Posts: 4,502

I wonder if it has to do with the programming language 97/98 was written in

---

📄 31-07-17,   11:09 PM   #29

Balthazor ⚬
Youth Team Player

Join Date: 04-06-17

Interestingly CM96/97 and CM1 generation were readable with Olly in old computer. Newer one is moaning about 16-bit program and can't open it as being 64-bit. That's different topic that my zerowise programming skills don't let me find almost anything. Their structure is probably different as I couldn't find any offsets connected to certain clubs(but they are mentioned in exe as I see wit hex editor.. About current one...it would be cool to find offsets which allow promotion-relegation from Irish and Northern Irish second level to amateur leagues. They would be good base for Austrian, Swiss and Estonian leagues with 10+10, bu it's annoying when no new teams will be promoted. I read that something is done with Scotland to get 2 more teams., so there might be hope?

04-12-18, 09:51 PM   #30

juanpsno ○
Youth Team Player

Join Date: 03-01-17
Posts: 27

Hello! I followed all the steps to the letter. When selecting the option "copy to excecutable-> all modifications -> copy all" the window to save the new exe does not appear

---

05-12-18, 12:03 AM   #31

MadScientist ○
Director

Join Date: 26-09-18
Location: Brazil
Posts: 882

> **Originally Posted by juanpsno** ▶
>
> *Hello! I followed all the steps to the letter. When selecting the option "copy to excecutable-> all modifications -> copy all" the window to save the new exe does not appear*

When u click 'copy all' a small window appear with olly code. Close that small window and the window to save the exe will appear. Then click YES and choose the file name.

05-12-18, 07:21 PM   #32

juanpsno ○
Youth Team Player

Join Date: 03-01-17
Posts: 27

Thanks so much for the help!

02-02-20, 12:00 PM   #33

Bhaalspawn ○
Hot Prospect for the Future

Join Date: 05-02-17
Posts: 112

Hi there! I need your help. I try to using olly again but after open the exe, the olly loads the game and everything freeze. Can i somewherw stops olly to load the game ?

Edit: i found the answer 🙂

Last edited by Bhaalspawn; 02-02-20 at 12:40 PM.

26-03-20, 12:04 PM   #34

Ronaldo07 ○
Youth Team Player

Join Date: 08-03-12
Location: Manchester
Posts: 22

Can someone help please, im trying to test the olly debugger on the new Saturn v9 patch, when I go to open the CM0102 exe file, I select in on click ok, it then goes to the CPU screen with nothing in any of the columns, and just says "running" in the bottom corner this just stays like this and nothing else happens, when I then go to close Olly down it comes up with the following message

Unable to termiate process 'cm002'. Operating system reports error ERROR_\INVALID_HANDLE

Any help on this would be great as id like to run the v9+ Saturn patch through it to see if that helps my screen resolution problems.

28-03-20, 06:28 PM   #35

MadScientist ○
Director

Join Date: 26-09-18

> **Originally Posted by Ronaldo07** ▶
>
> *Can someone help please, im trying to test the olly debugger on the new Saturn v9 patch, when I go to open the CM0102 exe file, I select in on click ok, it then goes to the CPU screen with nothing in any of the columns, and just says "running" in the bottom corner this just stays like this and nothing else happens, when I then go to close Olly down it comes up with the following message*
>
> *Unable to termiate process 'cm002'. Operating system reports error ERROR_\INVALID_HANDLE*
>
> *Any help on this would be great as id like to run the v9+ Saturn patch through it to see if that helps my screen resolution problems.*

as far as i remember you need to run olly as admin to be able to run the debugger

---

📄 09-07-20, 09:04 PM   #36

AndyCM0102 ○
Youth Team Player

Hi,I've got to the 31st of July 2008 but can't get any further.

I did have the Argentine second division in the game as a background league, but even now I've removed it, it still doesn't seem to work.

For clarification the leagues I had as playable were Scotland,Spain,France,Germany,Italy,Greece,England and Holland. And the background leagues are Argentina,Brazil,Belgium,Sweden and Turkey.

I had the 3.9.68 patch installed and used nick's patcher,but not a tapani or saturn patch.

Is there any potential suggestions as to what else it could be on those leagues, or is it likely to be corrupted at this point?.

📄 12-07-20, 08:44 AM   #37

Nick+Co ○
Programmer

@Andy: Upload your save somewhere and I'll take a look

📄 12-07-20, 08:30 PM   #38

AndyCM0102 ○
Youth Team Player

> **Originally Posted by Nick+Co** ▶
>
> *@Andy: Upload your save somewhere and I'll take a look*

Hi

It should be uploaded here https://easyupload.io/xdk2tx

Any problems with the link please let me know and I'll try and upload somewhere else.

📄 12-07-20, 08:32 PM   #39

AndyCM0102 ○
Youth Team Player

> **Originally Posted by Nick+Co** ▶
>
> *@Andy: Upload your save somewhere and I'll take a look*

https://easyupload.io/xdk2tx

It should be here Nick, if not please get back to me and I'll try uploading somewhere else

---

📄 12-07-20, 10:06 PM   #40

AndyCM0102 ○

Youth Team Player

Posts: 6

Hi Nick, I've sent a PM as it won't let me respond with the link through here.

📄 05-08-20, 10:08 AM

#41

yokofoxes ○
Youth Team Player

Join Date: 17-11-19
Posts: 8

Late to the game here, but I have followed all the instructions and have changed 3rd/4th place bugs and the Aussie league bug on the .68 version but when I go to save I get: Error- Unable to Create File.

Posting Permissions 🔼

You may not post new threads	**BB code** is On
You may not post replies	**Smilies** are On
You may not post attachments	**[IMG]** code is On
You may not edit your posts	**[VIDEO]** code is On
	HTML code is Off
	Forum Rules

-- Default Style ▾

Archive Web Hosting Top