Results 1 to 25 of 26 Page 1 of 2 1 2 Last

Thread: Adding space to exe (not a question, but a reality!)

Thread Tools

05-02-19, 08:37 PM #1

mihaigrad
VIP

Join Date: 14-04-14
Location: Romania
Posts: 4

Adding space to exe (not a question, but a reality!)

Hi all, my first ever post to this forum which I've been following and using its resources for so many years...I am quite a fanatic of CM, you might all understand the feeling of assimilating it to a drug 🙂 I've modified the exe quite a lot, mostly just replicating the fabulous findings of this great community (I've discovered only a few on my own). I am usually patching the exe manually, I have almost zero coding experience, but I've come to understand the basics of assembly and, by modifying and checking the realtime results, gained that minimum level to allow me to discover new things.
Ok, enough with the intro, so... I've discovered the Holy Grail (actually, the Holy Grail would've been the source code, but I think what I describe below is the closest to what we need to go one level up in keeping the game alive). I just insisted in searching on how one can expand the code space in an exe to allow for adding code in assembly - and the answer, apparently, was quite easy to find and even easier to implement.
Go to https://ntcore.com/?tag=cff-explorer, download and run CFF Explorer, load the exe in it, on the left menu click on "Section Headers", on the top right window right click anywhere, select "Add Section (empty space)", for size enter a multiple of 2000, click OK. A new section appeared at the bottom of the list of sections, double click in the Name tab and give it a name (e.g. ".extra"). Then again in the same area right click and select "Rebuild Image Size", then again right click and "Rebuild PE Header".Now click on that row, the bottom half will show you that new section in HEX, right click in that area, "select all", then again right click and "Fill with", enter 90 (i.e. NOP). Save the exe.
Open the exe in olly, from the menu View/Memory Map. You will immediately identify the new section there, right click on it, "Dump in CPU", it will show up in the bottom left section - if it shows as HEX, right click and select "Disassemble", you will see the new section filled with NOPs. And now you are able to add code, all that's needed is to create jumps or calls from original code space to the code written here. Those of you who are much more used to coding and manipulating this exe will probably understand better what's happened here, tbh I wouldn't be able to provide too much support or explanations outside of this pure "follow the instructions step by step" approach. Main sources that I used: https://reverseengineering.stackexch...ile-on-windows and https://resources.infosecinstitute.c...-to-pe-binary/
I tested this by adding a 2000 byte section and adding the code described at https://champman0102.co.uk/showthrea...743#post346743, using Spain and Argentina and making a jump from the original code at 0053DA6E and then jumping back to 0053DA95. Works flawlessly!
Now...let's see what you skilled patchers are able to do!

Last edited by mihaigrad; 06-02-19 at 12:25 AM.

18-02-19, 06:20 PM #2

mihaigrad
VIP

Join Date: 14-04-14
Location: Romania
Posts: 4

So, as it appears that this hasn't quite generated to others the excitement that I felt when found out about this possibility, let me put here some gains that I believe can be achieved with additional space, by replicating blocks of existing competitions and changing references accordingly: African Nations Cup qualifications, U21 European and World Tournaments, new leagues (Austria, Serbia, Bulgaria, Romania, Uruguay, Columbia, China, UAE...), English full pyramid, French CFA, updated Champions League and Europa League structures, fictional regional/international leagues.
My goal, to work during my little spare time, is to add Austria Premier and FIrst divisions, plus the Cup and Supercup, as a replica of Netherlands's competitions, as this looks to be the most simple competition system to replicate and a way to learn by doing.
Happy to get your feedback on this whole new range of possibilities.

18-02-19, 06:49 PM #3

ebfatz
Social Media Bod
Former Holy Trinity Member
Stories Mod

Join Date: 02-03-12
Posts: 8,522

I think, and this is certainly true for me personally, is that you need to explain it in layman's terms.

Does this mean that essentially expanding the available space on the disk/iso?

So, I believe, the CM0102.iso is around 295MB (May be wrong).
So if you were able to double it for example and you had 600MB, you could add additional leagues and competitions or have more steps in a certain countries league pyramid?

Forgive me if I'm completely wrong on my example.

18-02-19, 07:06 PM #4

mihaigrad
VIP

Join Date: 14-04-14
Location: Romania
Posts: 4

I'm talking about the exe. it's always been the issue of only being able to change certain values, for example to change the number of subs or foreigners. When having to alter fixtures or competition structures, it was very diificult to add new features, or to make changes that required more code, as you only had a limited "code space". But it is now possible to add more such space, to add code in assembly and have additional "native" competitions, on top of those already available originally.

18-02-19, 09:01 PM #5

samsami
VIP

Join Date: 27-10-14
Location: The Netherlands
Posts: 8,159

> Originally Posted by **mihaigrad**
> *I'm talking about the exe. it's always been the issue of only being able to change certain values, for example to change the number of subs or foreigners. When having to alter fixtures or competition structures, it was very difficult to add new features, or to make changes that required more code, as you only had a limited "code space". But it is now possible to add more such space, to add code in assembly and have additional "native" competitions, on top of those already available originally.*

If that doesn't cause the game to crash after a season or so that would be marvelous. I hope Saturn can use this!!

Samsami Sungo's Career
Feyenoord after Koeman... The Golden Years Return for Spurs... His Last Bow & *Oh when the Saints... The Comeback of Samsami* & *The Return of the King...The Return of the Prodigal Sons*

18-02-19, 09:38 PM #6

ebfatz
Social Media Bod
Former Holy Trinity Member
Stories Mod

Join Date: 02-03-12
Posts: 8,522

> Originally Posted by **mihaigrad**
> *I'm talking about the exe. it's always been the issue of only being able to change certain values, for example to change the number of subs or foreigners. When having to alter fixtures or competition structures, it was very diificult to add new features, or to make changes that required more code, as you only had a limited "code space". But it is now possible to add more such space, to add code in assembly and have additional "native" competitions, on top of those already available originally.*

if it's workable then it sounds good but it's all over my head I'm afraid.

03-04-19, 08:27 PM #7

MadScientist
Director

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

@saturn how helpful do you think this can be for future patches?

04-04-19, 07:17 PM #8

mihaigrad
VIP

Join Date: 14-04-14
Location: Romania
Posts: 4

Brief update on the progress: I understood how to add nations to the first screen, where one chooses the countries where to play; to achieve this I had to add to the exe, beyond the already additional ""code"" section, also a new ""data"" section (i.e. similar to where text strings are stored, but also where temporary values are stored during game).
For the new code that adds, for example, Austria, I have to reference some new ""data"" locations, but because the game expected these to be at other addresses, I had to change all data references in some large areas of code to point to the new ""data"" section, for then to be able to redesign the sequences and let the code run the same loops, at the same location intervals, and maintaining the same relativity between addresses. So now I should be very close to add a new country - Austria - with a structure replicating the one of Holland's, for testing purposes for now (so using Austrian clubs, but on Holland's championship and cup formats) - I really hope to get a stable version by end of week. Once that works, only then we can really think big, though it appears to be not that simple to add workable code and features...

04-04-19, 07:42 PM #9

saturn
Programmer
VIP

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

> Originally Posted by **MadScientist**
> *@saturn how helpful do you think this can be for future patches?*

Yes, definitely has the potential to be very useful. For the moment a lot of new code can be added to the Credits section (quite a big section and all disabled by removing one CALL). But the addition of potenitally unlimited space would of course be great.

> Originally Posted by **mihaigrad**
> *Brief update on the progress: I understood how to add nations to the first screen, where one chooses the countries where to play; to achieve this I had to add to the exe, beyond the already additional ""code"" section, also a new ""data"" section (i.e. similar to where text strings are stored, but also where temporary values are stored during game).*
> *For the new code that adds, for example, Austria, I have to reference some new ""data"" locations, but because the game expected these to be at other addresses, I had to change all data references in some large areas of code to point to the new ""data"" section, for then to be able to redesign the sequences and let the code run the same loops, at the same location intervals, and maintaining the same relativity between addresses. So now I should be very close to add a new country - Austria - with a structure replicating the one of Holland's, for testing purposes for now (so using Austrian clubs, but on Holland's championship and cup formats) - I really hope to get a stable version by end of week. Once that works, only then we can really think big, though it appears to be not that simple to add workable code and features...*

Sounds promising! Perhaps try using South Korea's league structure, it's probably the most straightforward in the game.

25-04-19, 04:00 PM #10

Anoxic
Youth Team Player

Join Date: 24-02-13
Posts: 16

Modifing main cm0102.exe is not nessesary.
I wrote wrapper as dll, is loaded on cm started.

Explaint: cm0102.exe load funtion DirectDrawCreate from ddraw.dll.
Orginal file (ddraw.dll) is in Windows/System32, but if add file named ddraw.dll in cm0102 working directory this will by loaded first.
My file wrap the oryginal function DirectDrawCreate and load the oryginal file from windows.
This way you can load any function writed in C/C++. (ASM is not nessasary more).

In example i redraw original "Web Sites" button text with my text.
Source code in C++ (Visual Studio Solution)

Link to file and source :
DOWNLOAD

The Following 2 Users Say Thank You to Anoxic For This Useful Post:

MadScientist, xeno

25-04-19, 05:47 PM #11

MadScientist
Director

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

> Originally Posted by **Anoxic**
>
> *Modifing main cm0102.exe is not nessesary.*
> *I wrote wrapper as dll, is loaded on cm started.*
>
> *Explaint: cm0102.exe load funtion DirectDrawCreate from ddraw.dll.*
> *Orginal file (ddraw.dll) is in Windows/System32, but if add file named ddraw.dll in cm0102 working directory this will by loaded first.*
> *My file wrap the oryginal function DirectDrawCreate and load the oryginal file from windows.*
> *This way you can load any function writed in C/C++. (ASM is not nessasary more).*
>
> *In example i redraw original "Web Sites" button text with my text.*
> *Source code in C++ (Visual Studio Solution)*
>
> *Link to file and source :*
> *DOWNLOAD*

This is great! And thanks for sharing VS project

I think tapani did something like that for the idle sensivity patch, or for something in his 3.xx patch. For sure it is promising if used with creativity

25-04-19, 06:37 PM #12

Ratio
Coach

Join Date: 03-03-12
Location: Italy
Posts: 484

> Originally Posted by **MadScientist**
>
> *This is great! And thanks for sharing VS project*
>
> *I think tapani did something like that for the idle sensivity patch, or for something in his 3.xx patch. For sure it is promising if used with creativity*

Mihaigrad wrote me saying he experienced 2 errors but he's working about!!! Obviously Anoxic gave us a magic touch!!

25-04-19, 06:59 PM #13

MadScientist
Director

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

> Originally Posted by **Ratio**
>
> *Mihaigrad wrote me saying he experienced 2 errors but he's working about!!! Obviously Anoxic gave us a magic touch!!*

yeah, each of the ideas are great and can be used differently.

I think mihaigrad's solution (add space to .exe) is more suited for when you want to increment something that already exists in the .exe (like create a new league as he is doing) as you would duplicate existing assembly league code and make adjusts to it.
And Anoxic's solution (.dll) is more suited for adding some new functionality different than already exists in the .exe (like the idle sensivity from tapani) because its easier to create new C++ code than assembly code.
And more uses can be invented with creativity for each solution.

24-09-19, 06:53 AM #14

probs
Youth Team Player

Join Date: 30-03-12
Location: Cracow , Poland
Posts: 32

I keep my fingers crossed for you guys. And for your work-life balance too

30-10-19, 06:30 AM #15

luisfrjgua
Youth Team Player

Join Date: 08-06-18
Posts: 41

I am curious, guys. Is it possible to duplicate the structure of a league or cup, making another league without replacing? Or not?
Anyone came close to do this?

30-10-19, 08:42 AM #16

saturn
Programmer
VIP

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

Tapani having both the Northern League Premier and Welsh league in his 3.xx patches is probably the closest anyone's got. I've thought about it before but never tried it. As well as creating the new league and cup code you'd also have to create things like the new nation's awards, discipline/ruling body, transfer rules, plus edit the following parts of the code (very likely to be more):
award_manager
discipline
hall_of_fame
key_nation
setup x3
transfer_manager

31-10-19, 04:16 AM #17

luisfrjgua
Youth Team Player

Join Date: 08-06-18
Posts: 41

> Originally Posted by **saturn**
> *Tapani having both the Northern League Premier and Welsh league in his 3.xx patches is probably the closest anyone's got. I've thought about it before but never tried it. As well as creating the new league and cup code you'd also have to create things like the new nation's awards, discipline/ruling body, transfer rules, plus edit the following parts of the code (very likely to be more):*
> *award_manager*
> *discipline*
> *hall_of_fame*
> *key_nation*
> *setup x3*
> *transfer_manager*

Thanks, saturn. So it's extremely dificult! rs
I make part of a brazilian community that helps to keep CM 01/02 alive in Brazil. I have done some substitutions of leagues that I don't used to play to other ones (sulamericans, such as Colombia, Chile, Uruguay...) based on the march update.
One easier thing that can be done (at least I think!), but I don't know how, is to make the correct teams of the two asian leagues that we have in the game participating in Asian Club Championship.
Actually if we choose to start a new game with these two leagues, only clubs of one of then go to the continental correctlly and not the other.
Is it possible and easy to fix this? With sulamerican leagues we don't have this problem!

Thanks to the oportunity and I'm sorry to my terrible english... 

31-10-19, 02:10 PM #18

saturn
Programmer
VIP

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

I know the bug you're talking about but unfortunately no, I don't know how to fix it.

02-11-19, 12:08 AM #19

luisfrjgua
Youth Team Player

Join Date: 08-06-18
Posts: 41

> Originally Posted by **saturn**
> *I know the bug you're talking about but unfortunately no, I don't know how to fix it.*

I imagined. Without the source code some modifications are almost impossible.
But one thing, if the guys make a comparison between the versions 3.90 and the 3.98 of CM 01/02 (in version 3.98 has been added the Korean league), wouldn't be possible to do the same in the code to make a new league?
And thanks to everyone here. What you have done with the game was amazing!

Last edited by luisfrjgua; 02-11-19 at 12:29 AM.

30-04-20, 12:11 PM #20

Nick+Co
Programmer

Join Date: 18-07-15
Posts: 795

Apologies for reviving an old thread, but I think mihaigrad had the right idea here. Applying this patch:

Code:

```
000000FE: 04 05
0000014A: 9E BE
000001F8: E5 00
000001F9: 50 60
00000220: CE 00
00000221: F1 00
00000222: 01 02
00000248: 3C 00
00000249: D6 E0
00000270: 38 00
00000271: 12 20
00000290: 00 2E
00000291: 00 6E
00000292: 00 69
00000293: 00 63
00000294: 00 6B
0000029A: 00 20
0000029D: 00 70
0000029E: 00 9E
000002A2: 00 20
000002A5: 00 C0
000002A6: 00 6D
000002B7: 00 C0
```

And then manually adding 0x200000 worth of zeroes to the end of the exe gives a load (2mb) of space that you can reference via 00DE7000 for any patches.
I'm going to make my patcher automate this expansion (just makes the exe 9mb instead of 7mb, so nothing too onerous) and start putting any patches in at DE7000 so that there are no clashes with any existing data/patches.
This is probably the future for anything new I come up with as I'm simply running out of space

EDIT: So doing the binary to memory conversion will be 006DC000 in the file will equal 00DE7000 in memory when loaded

Last edited by Nick+Co; 30-04-20 at 01:35 PM.

The Following 4 Users Say Thank You to Nick+Co For This Useful Post:

GFRay, Nick Valentine, tonytony, xeno

30-04-20, 02:52 PM #21

Bhaalspawn
Hot Prospect for the Future

Join Date: 05-02-17
Posts: 112

With that more space, is it possible to add leagues not just swap ? Like one nation loads 5-6 nations league(maybe it has flaws to shows under one nation). It should be haard work but im curious is it workable.

30-04-20, 04:15 PM #22

tonytony
Youth Team Player

Join Date: 29-07-19
Posts: 41

> Originally Posted by **Nick+Co**
> *I'm going to make my patcher automate this expansion (just makes the exe 9mb instead of 7mb, so nothing too onerous) and start putting any patches in at DE7000 so that there are no clashes with any existing data/patches.*
> *This is probably the future for anything new I come up with as I'm simply running out of space*

I wonder if it would be worth coming up with a header format like index.dat so new mods could define their size and then with a patcher it can be applied without over writing existing content as you know from the patches header you can place it safely after existing mods.

> Originally Posted by **Bhaalspawn**
> *With that more space, is it possible to add leagues not just swap ? Like one nation loads 5-6 nations league(maybe it has flaws to shows under one nation). It should be haard work but im curious is it workable.*

I think it would be possible but as **Saturn** mentioned it would be a lot of work. Someones first job would be to make a proof of concept of a new league and everything it needs to be used a template for future leagues.

> *As well as creating the new league and cup code you'd also have to create things like the new nation's awards, discipline/ruling body, transfer rules, plus edit the following parts of the code (very likely to be more):*
> *award_manager*
> *discipline*
> *hall_of_fame*
> *key_nation*
> *setup x3*
> *transfer_manager*

30-04-20, 08:05 PM #23

Nick+Co
Programmer

Join Date: 18-07-15
Posts: 795

> *I wonder if it would be worth coming up with a header format like index.dat so new mods could define their size and then with a patcher it can be applied without over writing existing content as you know from the patches header you can place it safely after existing mods.*

If we had a whole plethora of patchers, maybe. But as it's a limited number it's not necessary. With this approach you could just post in here and claim some of the 2mb as yours and warn others to leave it alone
Also, if a patch is built against a certain offset, it's not always trivial to shift it to another - so it would be kind of set in stone any way.

05-05-20, 12:25 AM #24

John Locke
Decent Young Player

Join Date: 04-05-20
Posts: 89

> Originally Posted by **Nick+Co**
>
> *Apologies for reviving an old thread, but I think mihaigrad had the right idea here. Applying this patch:*
>
> *Code:*

```
000000FE: 04 05
0000014A: 9E BE
000001F8: E5 00
000001F9: 50 60
00000220: CE 00
00000221: F1 00
00000222: 01 02
00000248: 3C 00
00000249: D6 E0
00000270: 38 00
00000271: 12 20
00000290: 00 2E
00000291: 00 6E
00000292: 00 69
00000293: 00 63
00000294: 00 6B
0000029A: 00 20
0000029D: 00 70
0000029E: 00 9E
000002A2: 00 20
000002A5: 00 C0
000002A6: 00 6D
000002B7: 00 C0
```

> *And then manually adding 0x200000 worth of zeroes to the end of the exe gives a load (2mb) of space that you can reference via 00DE7000 for any patches.*
> *I'm going to make my patcher automate this expansion (just makes the exe 9mb instead of 7mb, so nothing too onerous) and start putting any patches in at DE7000 so that there are no clashes with any existing data/patches.*
> *This is probably the future for anything new I come up with as I'm simply running out of space*
>
> *EDIT: So doing the binary to memory conversion will be 006DC000 in the file will equal 00DE7000 in memory when loaded*

Just checking... this actually means we can now JMP / CALL from within the body of the original exe into the newly created space and then JMP / RETN back?

05-05-20, 08:41 AM #25

MarcoVanBast
Reserve Team Player

Join Date: 17-06-12
Posts: 455

> Originally Posted by **John Locke**
>
> *Just checking... this actually means we can now JMP / CALL from within the body of the original exe into the newly created space and then JMP / RETN back?*

tried OP method - it works.

Results 26 to 26 of 26 Page 2 of 2 First 1 2

Thread: Adding space to exe (not a question, but a reality!)

Thread Tools

05-05-20, 08:45 AM #26

Nick+Co
Programmer

Join Date: 18-07-15
Posts: 795

@JL: Yep - would be pointless if we couldn't!

Page 2 of 2 First 1 2

« how to save whole exe in olly | Renaming Competitions, e.g. UEFA Cup / Europa League »

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