Subject: ASM Addresses
Posted by QoQn00b on Tue, 20 Feb 2007 04:51:05 GMT
View Forum Message <> Reply to Message

I've been modding C++ and CS for about 4 weeks now and I want to move on to editing the ASM... and I understand how for the most part, enough to get going, but I need to know how to get the Address (i.e. 0x0040F0D0) of the function I'm trying to make. Is there a list or something somewhere? oO

Subject: Re: ASM Addresses
Posted by Cat998 on Tue, 20 Feb 2007 09:34:07 GMT
View Forum Message <> Reply to Message

use the adress operator: &

Subject: Re: ASM Addresses
Posted by jnz on Tue, 20 Feb 2007 16:54:10 GMT
View Forum Message <> Reply to Message

```
#include <iostream>
using namespace std;

int myfunct(int myparam)
{
    return myparam+10;
}

int main()
{

    cout << "Call the function: " << myfunct(2) << endl << "Function address: " << &myfunct <<
endl;
    system("pause");
    return 0;
}
```

for my own interest, how do you get the function in bhs.dll and how would you make such an application IE: stop the message from showing? the only way i know how to hack is to:

```
#include <iostream>
using namespace std;
```

```
typedef int (*_myfunctptr)(int param);
int main()
{
 _myfunctptr myfunctptr = (_myfunctptr)12423574; //some funct address

 cout << myfunctptr(2) << endl;

 system("pause");
      return 0;
}
```

how do i get the addresses of the functions i want to hack?

Subject: Re: ASM Addresses
Posted by QoQn00b on Tue, 20 Feb 2007 23:03:22 GMT
View Forum Message <> Reply to Message

Quote:use the adress operator: &

Nein, I mean how to find the names of the ASM commands. Like, 0x0040F0D0 is the SetScore or SetMoney (I cant remember which) address in the ASM release. How can I get a key to the list of these address names?

Subject: Re: ASM Addresses
Posted by jnz on Tue, 20 Feb 2007 23:29:54 GMT
View Forum Message <> Reply to Message

you mean this?

Number of Exported Functions = 115 (decimal)

Addr:45018390 Ord: 1 (0001h) Name: AddCRCHook
Addr:45018900 Ord: 2 (0002h) Name: AddCharacterPurchaseHook
Addr:45018990 Ord: 3 (0003h) Name: AddCharacterPurchaseMonHook
Addr:450170E0 Ord: 4 (0004h) Name: AddChatHook
Addr:45017EE0 Ord: 5 (0005h) Name: AddConsoleOutputHook
Addr:450185D0 Ord: 6 (0006h) Name: AddDataHook
Addr:45017130 Ord: 7 (0007h) Name: AddGameOverHook
Addr:450170F0 Ord: 8 (0008h) Name: AddHostHook
Addr:45018830 Ord: 9 (0009h) Name: AddKeyHook
Addr:45017120 Ord: 10 (000Ah) Name: AddLoadLevelHook
Addr:45017100 Ord: 11 (000Bh) Name: AddPlayerJoinHook
Addr:450185E0 Ord: 12 (000Ch) Name: AddPlayerLeaveHook

Addr:450188A0 Ord: 13 (000Dh) Name: AddPowerupPurchaseHook
Addr:45018930 Ord: 14 (000Eh) Name: AddPowerupPurchaseMonHook
Addr:450188D0 Ord: 15 (000Fh) Name: AddVehiclePurchaseHook
Addr:45018960 Ord: 16 (0010h) Name: AddVehiclePurchaseMonHook
Addr:45017110 Ord: 17 (0011h) Name: AddVersionHook
Addr:45017E10 Ord: 18 (0012h) Name: Change_Radar_Map
Addr:450178A0 Ord: 19 (0013h) Name: Clear_Info_Texture
Addr:450183C0 Ord: 20 (0014h) Name: Display_GDI_Sidebar
Addr:45018470 Ord: 21 (0015h) Name: Display_NOD_Sidebar
Addr:45018520 Ord: 22 (0016h) Name: Display_Security_Dialog
Addr:450174B0 Ord: 23 (0017h) Name: GetBHSVersion
Addr:450174A0 Ord: 24 (0018h) Name: GetCurrentMusicTrack
Addr:45017DF0 Ord: 25 (0019h) Name: Get_Build_Time_Multiplier
Addr:45017AE0 Ord: 26 (001Ah) Name: Get_Vehicle_Limit
Addr:45017ED0 Ord: 27 (001Bh) Name: Is_Currently_Building
Addr:45017CF0 Ord: 28 (001Ch) Name: Load_New_HUD_INI
Addr:450187D0 Ord: 29 (001Dh) Name: NewAddObjectCreateHook
Addr:450187F0 Ord: 30 (001Eh) Name: NewRemoveObjectCreateHook
Addr:450183B0 Ord: 31 (001Fh) Name: New_Change_Time_Limit
Addr:450183A0 Ord: 32 (0020h) Name: New_Change_Time_Remaining
Addr:45016450 Ord: 33 (0021h) Name: New_Clear_Weapons
Addr:45015BF0 Ord: 34 (0022h) Name: New_Create_2D_Sound
Addr:45017030 Ord: 35 (0023h) Name: New_Create_2D_Sound_Player
Addr:45015C40 Ord: 36 (0024h) Name: New_Create_2D_WAV_Sound
Addr:450171F0 Ord: 37 (0025h) Name: New_Create_2D_WAV_Sound_Player
Addr:45015D20 Ord: 38 (0026h) Name: New_Create_3D_Sound_At_Bone
Addr:450173A0 Ord: 39 (0027h) Name: New_Create_3D_Sound_At_Bone_Player
Addr:45015C90 Ord: 40 (0028h) Name: New_Create_3D_WAV_Sound_At_Bone
Addr:450172A0 Ord: 41 (0029h) Name: New_Create_3D_WAV_Sound_At_Bone_Player
Addr:45015620 Ord: 42 (002Ah) Name: New_Create_Explosion
Addr:45015690 Ord: 43 (002Bh) Name: New_Create_Explosion_At_Bone
Addr:45015B50 Ord: 44 (002Ch) Name: New_Create_Sound
Addr:45016F10 Ord: 45 (002Dh) Name: New_Create_Sound_Player
Addr:45017BA0 Ord: 46 (002Eh) Name: New_Disable_All_Collisions
Addr:45017C10 Ord: 47 (002Fh) Name: New_Disable_Physical_Collisions
Addr:45016820 Ord: 48 (0030h) Name: New_Display_Float
Addr:45016C80 Ord: 49 (0031h) Name: New_Display_Float_Player
Addr:45016110 Ord: 50 (0032h) Name: New_Display_GDI_Player_Terminal_Player
Addr:45017AF0 Ord: 51 (0033h) Name: New_Display_Health_Bar
Addr:45016880 Ord: 52 (0034h) Name: New_Display_Int
Addr:45016D50 Ord: 53 (0035h) Name: New_Display_Int_Player
Addr:450161B0 Ord: 54 (0036h) Name: New_Display_NOD_Player_Terminal_Player
Addr:450167D0 Ord: 55 (0037h) Name: New_Display_Text
Addr:45016BD0 Ord: 56 (0038h) Name: New_Display_Text_Player
Addr:45017C80 Ord: 57 (0039h) Name: New_Enable_Collisions
Addr:45016A30 Ord: 58 (003Ah) Name: New_Enable_HUD_Player
Addr:45016050 Ord: 59 (003Bh) Name: New_Enable_Radar_Player
Addr:450155A0 Ord: 60 (003Ch) Name: New_Enable_Stealth

Addr:45016E10 Ord: 61 (003Dh) Name: New_Enable_Stealth_Player
Addr:450164D0 Ord: 62 (003Eh) Name: New_Enable_Vehicle_Transitions
Addr:45015A30 Ord: 63 (003Fh) Name: New_Fade_Background_Music
Addr:45015E30 Ord: 64 (0040h) Name: New_Fade_Background_Music_Player
Addr:45016960 Ord: 65 (0041h) Name: New_Force_Camera_Look_Player
Addr:45015DB0 Ord: 66 (0042h) Name: New_Play_Building_Announcement
Addr:450168D0 Ord: 67 (0043h) Name: New_Select_Weapon
Addr:45015AB0 Ord: 68 (0044h) Name: New_Set_Background_Music
Addr:45015F00 Ord: 69 (0045h) Name: New_Set_Background_Music_Player
Addr:45016760 Ord: 70 (0046h) Name: New_Set_Display_Color
Addr:45016AF0 Ord: 71 (0047h) Name: New_Set_Display_Color_Player
Addr:45018050 Ord: 72 (0048h) Name: New_Set_Fog_Color
Addr:45018280 Ord: 73 (0049h) Name: New_Set_Fog_Density
Addr:45015700 Ord: 74 (004Ah) Name: New_Set_Fog_Enable
Addr:450157D0 Ord: 75 (004Bh) Name: New_Set_Fog_Enable_Player
Addr:45018180 Ord: 76 (004Ch) Name: New_Set_Fog_Mode
Addr:45015750 Ord: 77 (004Dh) Name: New_Set_Fog_Range
Addr:45015890 Ord: 78 (004Eh) Name: New_Set_Fog_Range_Player
Addr:45018740 Ord: 79 (004Fh) Name: New_Set_Model
Addr:45017520 Ord: 80 (0050h) Name: New_Set_Obj_Radar_Blip_Color
Addr:45017660 Ord: 81 (0051h) Name: New_Set_Obj_Radar_Blip_Color_Player
Addr:450174C0 Ord: 82 (0052h) Name: New_Set_Obj_Radar_Blip_Shape
Addr:45017580 Ord: 83 (0053h) Name: New_Set_Obj_Radar_Blip_Shape_Player
Addr:45016550 Ord: 84 (0054h) Name: New_Set_Player_Type
Addr:450165D0 Ord: 85 (0055h) Name: New_Set_Screen_Fade_Color
Addr:45016250 Ord: 86 (0056h) Name: New_Set_Screen_Fade_Color_Player
Addr:45016660 Ord: 87 (0057h) Name: New_Set_Screen_Fade_Opacity
Addr:45016370 Ord: 88 (0058h) Name: New_Set_Screen_Fade_Opacity_Player
Addr:45015990 Ord: 89 (0059h) Name: New_Set_War_Blitz
Addr:450166D0 Ord: 90 (005Ah) Name: New_Shake_Camera
Addr:45015B10 Ord: 91 (005Bh) Name: New_Stop_Background_Music
Addr:45015FB0 Ord: 92 (005Ch) Name: New_Stop_Background_Music_Player
Addr:45018A00 Ord: 93 (005Dh) Name: RemoveCharacterPurchaseHook
Addr:45018A60 Ord: 94 (005Eh) Name: RemoveCharacterPurchaseMonHook
Addr:45018810 Ord: 95 (005Fh) Name: RemoveKeyHook
Addr:450189C0 Ord: 96 (0060h) Name: RemovePowerupPurchaseHook
Addr:45018A20 Ord: 97 (0061h) Name: RemovePowerupPurchaseMonHook
Addr:450189E0 Ord: 98 (0062h) Name: RemoveVehiclePurchaseHook
Addr:45018A40 Ord: 99 (0063h) Name: RemoveVehiclePurchaseMonHook
Addr:45017D60 Ord: 100 (0064h) Name: Remove_Weapon
Addr:45017A20 Ord: 101 (0065h) Name: Send_Message
Addr:45017940 Ord: 102 (0066h) Name: Send_Message_Player
Addr:45017EC0 Ord: 103 (0067h) Name: Set_Currently_Building
Addr:450180B0 Ord: 104 (0068h) Name: Set_Fog_Color_Player
Addr:450182D0 Ord: 105 (0069h) Name: Set_Fog_Density_Player
Addr:450181D0 Ord: 106 (006Ah) Name: Set_Fog_Mode_Player
Addr:45017740 Ord: 107 (006Bh) Name: Set_HUD_Texture
Addr:450177F0 Ord: 108 (006Ch) Name: Set_Info_Texture

Addr:45017EF0 Ord: 109 (006Dh) Name: Set_Reticle_Texture1
Addr:45017FA0 Ord: 110 (006Eh) Name: Set_Reticle_Texture2
Addr:45017140 Ord: 111 (006Fh) Name: Set_Scope
Addr:450185F0 Ord: 112 (0070h) Name: Set_Shader_Number
Addr:45017A90 Ord: 113 (0071h) Name: Set_Vehicle_Limit
Addr:45017B50 Ord: 114 (0072h) Name: Set_Wireframe_Mode
Addr:45017DE0 Ord: 115 (0073h) Name: Update_PT_Data

Subject: Re: ASM Addresses
Posted by 0x90 on Wed, 21 Feb 2007 01:11:48 GMT
View Forum Message <> Reply to Message

QoQn00b wrote on Wed, 21 February 2007 00:03
Nein, I mean how to find the names of the ASM commands. Like, 0x0040F0D0 is the SetScore or SetMoney (I cant remember which) address in the ASM release. How can I get a key to the list of these address names?

gamemodding wrotehow do i get the addresses of the functions i want to hack?

im pretty sure youre talking about the same: getting the function pointer of an (engine) function. so the address of the first instruction of any function not available in source (so only in asm).
im afraid you would have to debug/trace them yourself if not already done like by jonwil@scriptsdll.
so i think funcptr of renegade engine is pretty good covered.

regards
0x90

Subject: Re: ASM Addresses
Posted by QoQn00b on Wed, 21 Feb 2007 05:41:33 GMT
View Forum Message <> Reply to Message

Thanks for the replies.

Yes, gamemodding, that is EXACTLY what I'm looking for. Where'd you get that list? Is there more?

Subject: Re: ASM Addresses
Posted by jnz on Wed, 21 Feb 2007 08:04:28 GMT
View Forum Message <> Reply to Message

with this handy little tool.

File Attachments
1) dsassm01.zip, downloaded 124 times

Subject: Re: ASM Addresses
Posted by 0x90 on Wed, 21 Feb 2007 10:14:41 GMT
View Forum Message <> Reply to Message

but that are just the exported functions of a dll (in this case the bhs.dll i guess?!)

this is useless if youre looking for engine pointers in a closed-source "exe" file like you will find them in jonwils scripts.dll source. dont have the sources here right now but i think it was InitEngine()@Engine.c

oh and btw, just to do some smalltalk, instead of using typedefs for all those funcptr calls i wrote myself a small function:

pCall(ptraddress,argcount,arguments...)

for example: if there was a function in the renegade engine to set some players money at 0x12345678 and it needs two arguments (playerid and moneyamount) you would call it that way:

pCall(0x12345678,2,playerid,moneyamount);

of course a typedef is more failsafe/nicer but if you have to call many funcptr's randomly, this is a quick'n'dirty, asm-based solution to do it. the contra: it has of course some (code)overhead.

regards
0x90

Subject: Re: ASM Addresses
Posted by jnz on Wed, 21 Feb 2007 16:40:06 GMT
View Forum Message <> Reply to Message

i never thought it was possible to call a non-exported function in a dll. so, how do i get the address of the non-exported funcion? if you try to call a invalid address, it will throw a generic error.