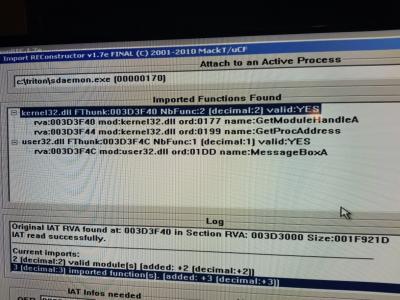
[](https://cdn.discordapp.com/attachments/438447915908726784/441710511567142912/20180503_162057.jpg)

Need that sylla

JECXZ**-**Yesterday at 2:29 PM

hrmm

ProAudioSoft**-**Yesterday at 2:29 PM

Prob have wrong oep also

JECXZ**-**Yesterday at 2:29 PM

are you sure you stopped at OEP?

yeah I really doubt the game only imports kernel32 and user32 man

I'm guessing too early

ProAudioSoft**-**Yesterday at 2:29 PM

Lol

JECXZ**-**Yesterday at 2:29 PM

or the import size you put is WAAAAAY too small

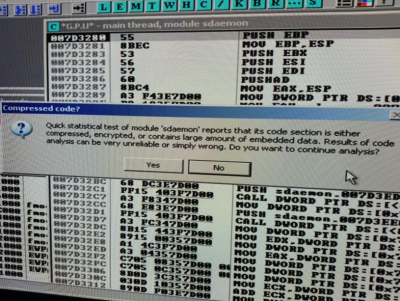
what did you set OEP at?

1F921D? from the output window?

holy fuck thats a huge IAT

that can't be right

lol

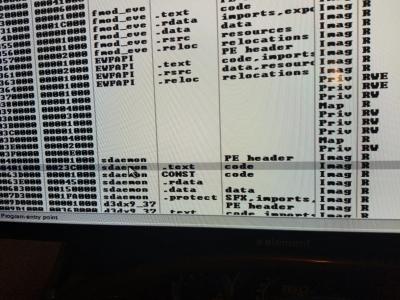
[](https://cdn.discordapp.com/attachments/438447915908726784/441713510876184596/20180503_161527.png)

did you set OEP to that highlighted value?

I mean I'm hoping no because that's the EP of the packer(edited)

but just checking

ProAudioSoft**-**Yesterday at 2:32 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441713745064886283/20180503_163348.jpg)

I set there

JECXZ**-**Yesterday at 2:32 PM

nope

that's not right

thats the base of your code section

but not necessarily OEP

generally not

ProAudioSoft**-**Yesterday at 2:33 PM

Ok

JECXZ**-**Yesterday at 2:33 PM

like for batman that value was 12D1000

but the OEP wasn't until like... 18something

ProAudioSoft**-**Yesterday at 2:33 PM

Wow ok

JECXZ**-**Yesterday at 2:33 PM

so one way to do it

that V2 crack exe you sent

that was the old protection I'm guessing?

because it had a const section too

my bet is it used the same vc compiler

ProAudioSoft**-**Yesterday at 2:34 PM

That wasn't even protected

JECXZ**-**Yesterday at 2:34 PM

oh thats fine

ok so open that shit up in ida

and look at its entry point

called \_\_start

chances are this is also vc7.1

so the entry point is gonna look a LOT like that

ProAudioSoft**-**Yesterday at 2:35 PM

Ok

JECXZ**-**Yesterday at 2:36 PM

one thing you might wanna do

GetStartupInfoW

search for that in all modules

set a breakpoint on that

the one from kernel32.dll | Export

let it run until it stops

because that's called pretty much at the top of \_\_\_tmainCRTStartup

find it once, note where the address is of that

set a memory breakpoint on execute

by that point the run will be too late to dump it

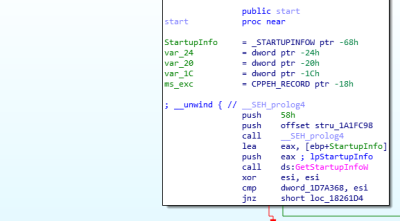
but you can always restart it with that hardware execute breakpoint set still

and just run it until it hits break on execute for that

and you'll be at oep

well the top of that function

it will look something like this (well in ida)

[](https://cdn.discordapp.com/attachments/438447915908726784/441715571478757376/unknown.png)

thats why breaking on getstartupinfo is helpful

probably getstartupinfow

chances are this sdaemon doesnt have ASLR enabled

so the breakpoint will be in the right spot on subsequent runs

yeah I checked , no ASLR

it might not be push 0x58

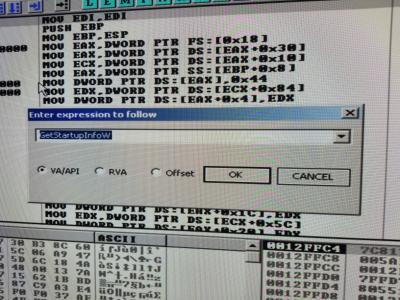
might be something else

but it will be a push push call to a prologue which you wont see in olly(edited)

anyway its a few instructions above that call to getstartupinfo

thats where you'll want to right click and set a hardware breakpoint on execute and rerun - when it hits that breakpoint you'll be at OEP

ProAudioSoft**-**Yesterday at 2:43 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441716352022216704/20180503_164344.jpg)

JECXZ**-**Yesterday at 2:43 PM

nope

go to uhh

search in all modules

name in all modules

and start typing getstartupinfow

and youll go to a list

find the one where it says kernel32.dll | export | GetStartupInfoW

and f2 on that line

ProAudioSoft**-**Yesterday at 2:45 PM

Trying to find search all modules

JECXZ**-**Yesterday at 2:45 PM

right click on the asm

go to "Search For"

and at the second from the top(edited)

"Name in all modules"

JECXZ**-**Yesterday at 2:36 PM

one thing you might wanna do

GetStartupInfoW

search for that in all modules

set a breakpoint on that

the one from kernel32.dll | Export

let it run until it stops

because that's called pretty much at the top of \_\_\_tmainCRTStartup

find it once, note where the address is of that

set a memory breakpoint on execute

by that point the run will be too late to dump it

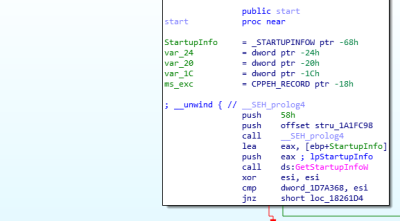
but you can always restart it with that hardware execute breakpoint set still

and just run it until it hits break on execute for that

and you'll be at oep

well the top of that function

it will look something like this (well in ida)

[](https://cdn.discordapp.com/attachments/438447915908726784/441715571478757376/unknown.png)

thats why breaking on getstartupinfo is helpful

probably getstartupinfow

chances are this sdaemon doesnt have ASLR enabled

so the breakpoint will be in the right spot on subsequent runs

yeah I checked , no ASLR

it might not be push 0x58

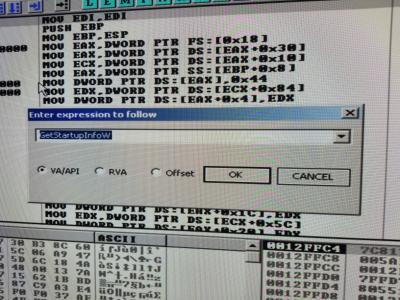
might be something else

but it will be a push push call to a prologue which you wont see in olly(edited)

anyway its a few instructions above that call to getstartupinfo

thats where you'll want to right click and set a hardware breakpoint on execute and rerun - when it hits that breakpoint you'll be at OEP

ProAudioSoft**-**Yesterday at 2:43 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441716352022216704/20180503_164344.jpg)

JECXZ**-**Yesterday at 2:43 PM

nope

go to uhh

search in all modules

name in all modules

and start typing getstartupinfow

and youll go to a list

find the one where it says kernel32.dll | export | GetStartupInfoW

and f2 on that line

ProAudioSoft**-**Yesterday at 2:45 PM

Trying to find search all modules

JECXZ**-**Yesterday at 2:45 PM

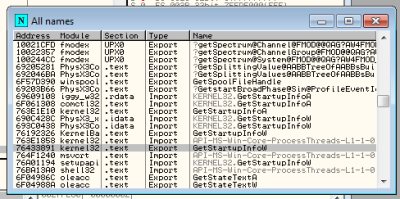
right click on the asm

go to "Search For"

and at the second from the top(edited)

"Name in all modules"

then you're looking for this guy

[](https://cdn.discordapp.com/attachments/438447915908726784/441717391664349203/unknown.png)

might want to do the "A" version as well

just in case

but try with just W first

no need to go bananas

now be aware , it might be called in the packer code too

not sure

so if the breakpoint for GetStartupInfoW is in a place that doesn't look kinda like that OEP up there

chances are it's not the place yet

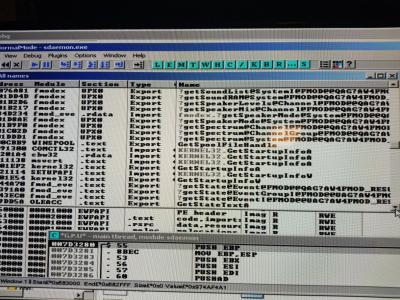
one way to know is if you scroll down slightly from the breakpoint where it hit, you might se HeapSetInformation or GetCommandLineA/W

that's how you'll know you're in the CRT startup

just remember that when you break you're breaking at the start of that function

you have to run until return to get back to the sdaemon code

ProAudioSoft**-**Yesterday at 2:51 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441718374255558656/20180503_165212.jpg)

JECXZ**-**Yesterday at 2:52 PM

yeah the one that ends in 01E54

F2 on that guy

after selecting it

then hit the play button and let it jam

ProAudioSoft**-**Yesterday at 2:54 PM

I set breakpoint. Game started

JECXZ**-**Yesterday at 2:54 PM

ok try again with GetStartupInfoA

ProAudioSoft**-**Yesterday at 2:54 PM

K

JECXZ**-**Yesterday at 2:54 PM

might have been compiled in multibyte mode instead of unicode

also don't run any scripts yet

not sure if you are but don't

we're doing this manually, the right way

ProAudioSoft**-**Yesterday at 2:56 PM

Ok, the export one right

JECXZ**-**Yesterday at 2:56 PM

yup

ProAudioSoft**-**Yesterday at 2:56 PM

K

JECXZ**-**Yesterday at 2:56 PM

what we're doing is breaking on the kernel32 address of the start of that function

as we can't be sure where it's called in the game

one thing we can be sure is that if it calls out to that function, it's gonna have to do it in the dll

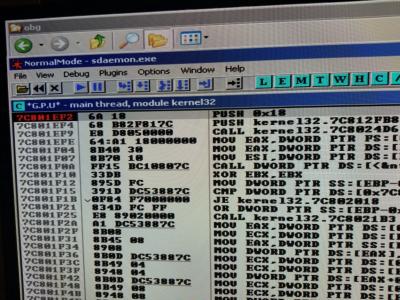
ProAudioSoft**-**Yesterday at 2:57 PM

Ok, it stopped

JECXZ**-**Yesterday at 2:57 PM

now run until return

ProAudioSoft**-**Yesterday at 2:57 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441720067596484638/20180503_165857.jpg)

JECXZ**-**Yesterday at 2:58 PM

ok so youre in kernel32

we want to go to debug

and then select run until return

and it will go near a retn function

hit f7 once after that and you'll see it change module name from kernel32 back to sdaemon

and we'll be back in the sdaemon code

JECXZ**-**Yesterday at 3:00 PM

once we're back to sdaemon look around... it's akin to poking your head out of the sand and checking if we're in the right spot

ProAudioSoft**-**Yesterday at 3:01 PM

Its scrolling like nuts

JECXZ**-**Yesterday at 3:01 PM

after hitting run until return?

ProAudioSoft**-**Yesterday at 3:02 PM

F7

Gonna have to stop it, prob reboot would be good idea

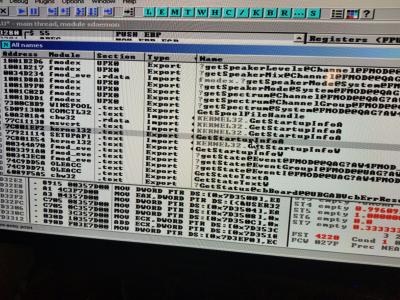
JECXZ**-**Yesterday at 3:03 PM

yeah

F7 does a single step so that's odd

it shouldn't keep going

ProAudioSoft**-**Yesterday at 3:12 PM

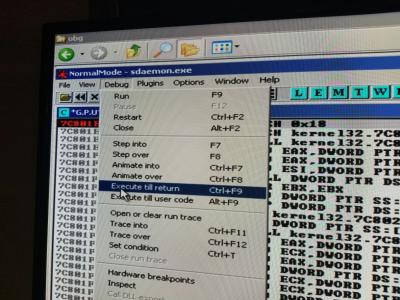
[](https://cdn.discordapp.com/attachments/438447915908726784/441723680536657920/20180503_171315.jpg)

Ok f2 on that

JECXZ**-**Yesterday at 3:12 PM

yup

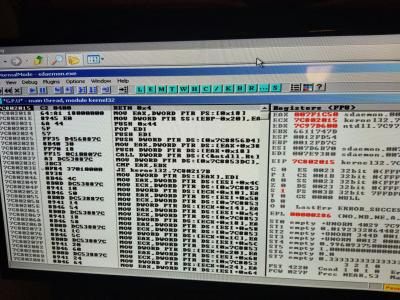
ProAudioSoft**-**Yesterday at 3:13 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441723925743796224/20180503_171417.jpg)

JECXZ**-**Yesterday at 3:13 PM

yup

ProAudioSoft**-**Yesterday at 3:13 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441724088835375107/20180503_171454.jpg)

JECXZ**-**Yesterday at 3:13 PM

now f7 once

ProAudioSoft**-**Yesterday at 3:13 PM

Now here, step

And it starts scrolling like mad (in video)

JECXZ**-**Yesterday at 3:14 PM

hrmm

ok

lets try breaking on GetCommandLineA

instead

so restart the application

and instead of GetStartupInfo

ProAudioSoft**-**Yesterday at 3:15 PM

Ok

JECXZ**-**Yesterday at 3:15 PM

kernel32.dll export GetCommandLineA

ProAudioSoft**-**Yesterday at 3:15 PM

K

I realized I was holding cntrl instead of fn on keyboard

JECXZ**-**Yesterday at 3:22 PM

LOL

ProAudioSoft**-**Yesterday at 3:22 PM

Get startup info A is ok

Lmao

JECXZ**-**Yesterday at 3:22 PM

goddammit

I was like wtf that shouldn't happen

ProAudioSoft**-**Yesterday at 3:22 PM

Haha

JECXZ**-**Yesterday at 3:22 PM

maybe theres some watchdog thread running around undoing breakpoints

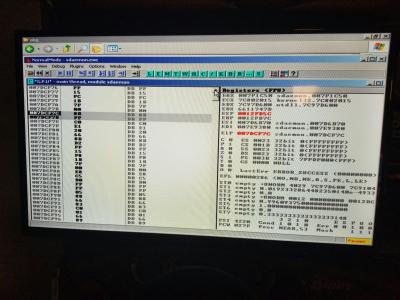
ProAudioSoft**-**Yesterday at 3:22 PM

Blaha

JECXZ**-**Yesterday at 3:23 PM

I hate function keys

ProAudioSoft**-**Yesterday at 3:23 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441726432570245141/20180503_172414.jpg)

JECXZ**-**Yesterday at 3:23 PM

especially on lenovo laptops

ok right click

choose

analysis or some shit

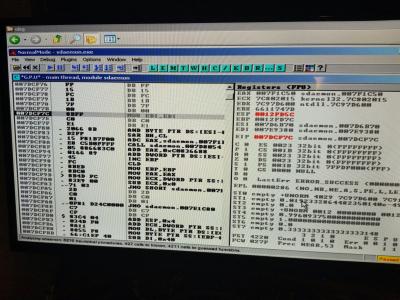
to analyze the code

unless you like reading one byte at a time

Analysis->Analyze Code

ProAudioSoft**-**Yesterday at 3:24 PM

K

[](https://cdn.discordapp.com/attachments/438447915908726784/441726808019435520/20180503_172543.jpg)

JECXZ**-**Yesterday at 3:25 PM

ok so that doesn't look right yet?

or wait

did you analyze all the code?

the ff 15 above it should be a jump

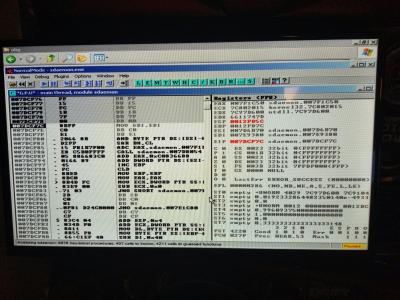
click on that FF

then right click

and hit analyze

ProAudioSoft**-**Yesterday at 3:26 PM

No change

[](https://cdn.discordapp.com/attachments/438447915908726784/441727397578932225/20180503_172755.jpg)

JECXZ**-**Yesterday at 3:27 PM

ok

dont click and drag

just left click

once on a line

ProAudioSoft**-**Yesterday at 3:27 PM

Ok, shit thought I did

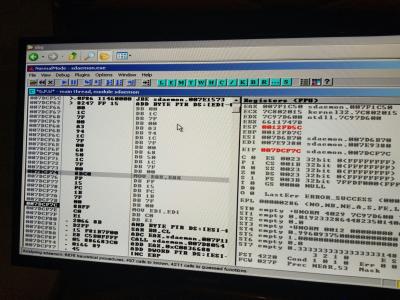
JECXZ**-**Yesterday at 3:27 PM

thats why its fucked up lol it thought you just meant to analyze that one selection(edited)

thats why that asm makes no sense lol

ProAudioSoft**-**Yesterday at 3:30 PM

Mouse acting strange, highlighting all, not accurate either. When I click where cursor sits, it highlights where you see

[](https://cdn.discordapp.com/attachments/438447915908726784/441728304442245120/20180503_173138.jpg)

JECXZ**-**Yesterday at 3:30 PM

left click once

then hit CTRL+A

make sure it's not function :3

ProAudioSoft**-**Yesterday at 3:32 PM

They all highlight together as a group no matter

JECXZ**-**Yesterday at 3:32 PM

something is effed with your mouse

can you plug in a new mouse or switch to another window and switch back?

ProAudioSoft**-**Yesterday at 3:35 PM

Yes, I switched windows no help, will get Seperate mouse

Same behaviour

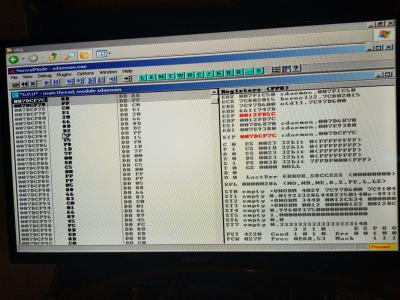
Maybe should reboot since I started prog a few times

Can redo quick

Machine on internet too, had to set static ip

USB gate installed. Win XPE

Right when I press f7 is when shit starts double highlighting

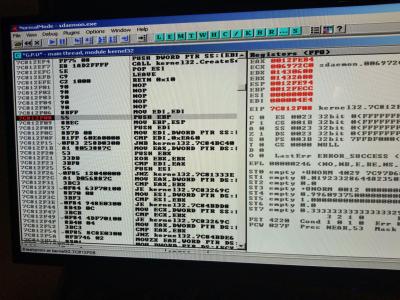
[](https://cdn.discordapp.com/attachments/438447915908726784/441731825476435968/20180503_174536.jpg)

Code analysis just does not work here.

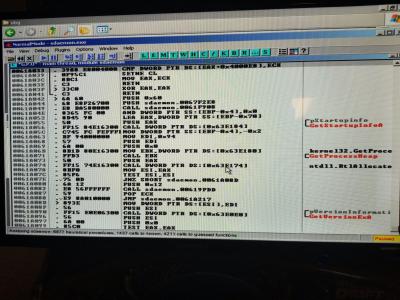
[](https://cdn.discordapp.com/attachments/438447915908726784/441732215982915595/20180503_174654.jpg)

Should we try GetCommandWindowA?

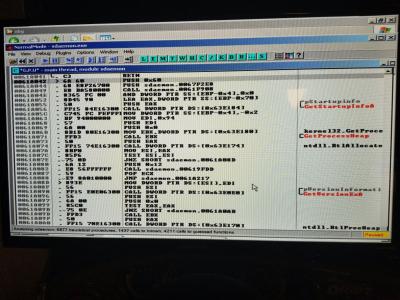
Can this be oep?

[](https://cdn.discordapp.com/attachments/438447915908726784/441735288327503884/20180503_175911.jpg)

ProAudioSoft**-**Yesterday at 4:06 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441737398653681664/20180503_180748.jpg)

Is that oep?

[](https://cdn.discordapp.com/attachments/438447915908726784/441744481054621716/20180503_183553.jpg)

Look at, and let me know...

JECXZ**-**Yesterday at 4:41 PM

6a 60

61a042

it looks like

yeah that's OEP

congratulations

so what you'd wanna do is right click that guy

go to breakpoint

then click "Hardware, on execution"

and then click play

let it go until it hits the hardware breakpoint

youll know because it will say hardware breakpoint at blah blah at the bottom

its to make sure everything is unpacked

if the game starts thats ok

just use the rewind looking button to reload and rerun it

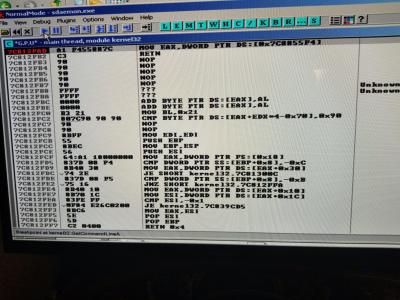
that hardware breakpoint should still be set

and it will be in that same location

you no longer need the kernel32 breakpoints at this point

ProAudioSoft**-**Yesterday at 5:06 PM

Ok, back, great!

[](https://cdn.discordapp.com/attachments/438447915908726784/441752758865887264/20180503_190850.jpg)

It stopped here

Oh, prob other break

JECXZ**-**Yesterday at 5:10 PM

yeah below it says breakpoint at getcommandlinea

just hit the play button again

but chances are you're going to have to hit the << button

with that hardware breakpoint still on

and let it go through again

because its probably after it already

ProAudioSoft**-**Yesterday at 5:19 PM

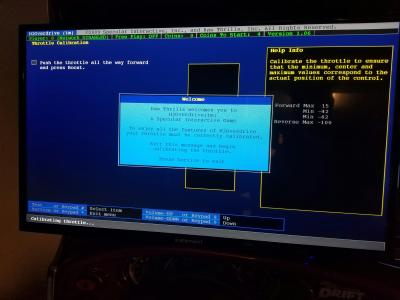
[](https://cdn.discordapp.com/attachments/438447915908726784/441755733705621505/20180503_192025.jpg)

That's right correct? Will remove other break

JECXZ**-**Yesterday at 5:20 PM

yeah

ProAudioSoft**-**Yesterday at 5:20 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441756083657113611/20180503_192205.jpg)

After play, io stuff starts

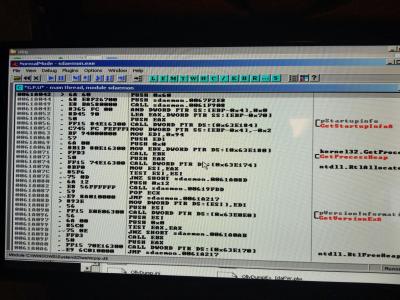
JECXZ**-**Yesterday at 5:21 PM

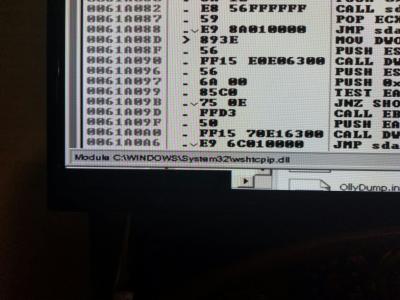
ok so go back to olly

hit the << button

ProAudioSoft**-**Yesterday at 5:21 PM

Will alt tab

[](https://cdn.discordapp.com/attachments/438447915908726784/441756342160457728/20180503_192301.jpg)

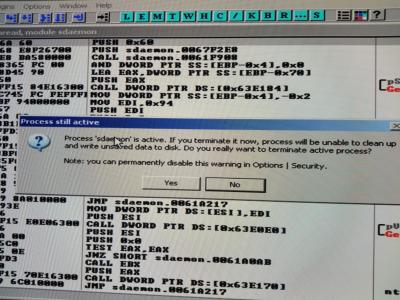
[](https://cdn.discordapp.com/attachments/438447915908726784/441756364063375390/20180503_192305.jpg)

Back at olly, didn't rewind

JECXZ**-**Yesterday at 5:22 PM

ok hit the rewind

ProAudioSoft**-**Yesterday at 5:23 PM

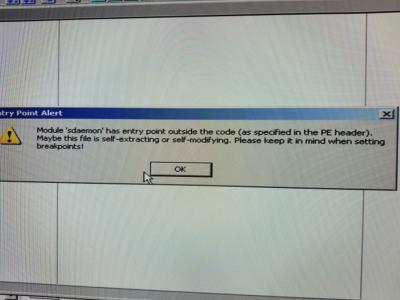
[](https://cdn.discordapp.com/attachments/438447915908726784/441756705295171584/20180503_192432.jpg)

Get that with rewind

JECXZ**-**Yesterday at 5:23 PM

hit yes

ProAudioSoft**-**Yesterday at 5:24 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441756966683934720/20180503_192534.jpg)

Then this

JECXZ**-**Yesterday at 5:24 PM

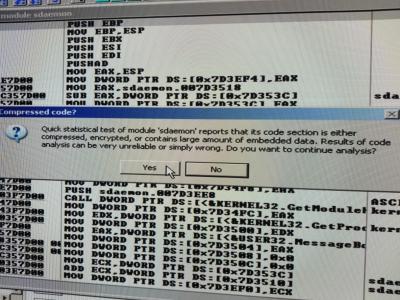
hit ok

then on the top menu

go to debug->hardware breakpoints

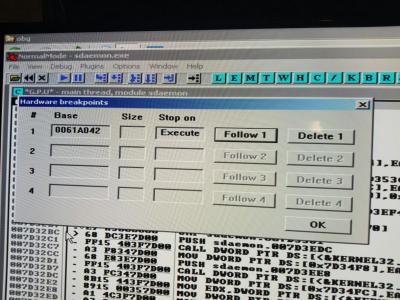
the top one should be set still

ProAudioSoft**-**Yesterday at 5:25 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441757160062320652/20180503_192618.jpg)

I know yes

Ok

[](https://cdn.discordapp.com/attachments/438447915908726784/441757405219651584/20180503_192719.jpg)

JECXZ**-**Yesterday at 5:26 PM

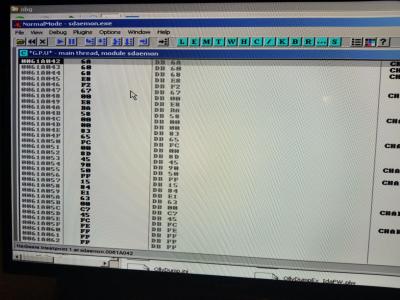
yup

ok hit play

and on the bottom you should see where it hits the hardware breakpoint

ProAudioSoft**-**Yesterday at 5:27 PM

It did, click analyze right

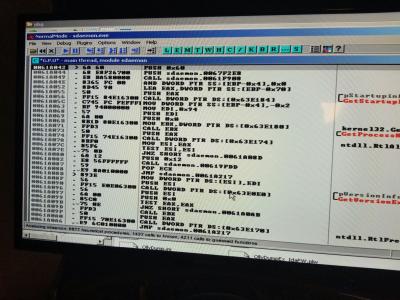
[](https://cdn.discordapp.com/attachments/438447915908726784/441757745507729418/20180503_192827.jpg)

Analyze, or no

JECXZ**-**Yesterday at 5:29 PM

yeah

ProAudioSoft**-**Yesterday at 5:29 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441758139549745152/20180503_193000.jpg)

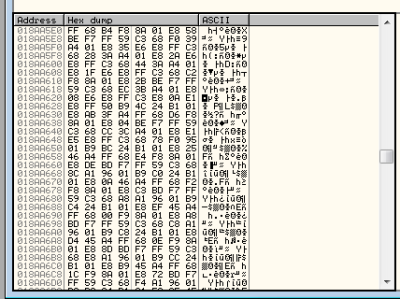
JECXZ**-**Yesterday at 5:29 PM

nice

ok so you're legit at ebp now

ok so now

youll see something like this below the asm

[](https://cdn.discordapp.com/attachments/438447915908726784/441758346966597663/unknown.png)

ProAudioSoft**-**Yesterday at 5:30 PM

The hex, lemme try to bring up

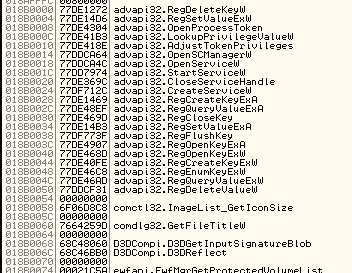
JECXZ**-**Yesterday at 5:30 PM

what youre gonna want to do is right click

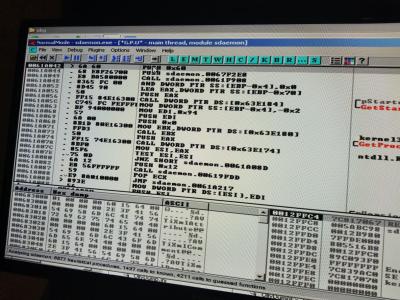
on it whne you have that window

and under the right click menu find Long->Address

the area you're going to look for in there looks like this:

[](https://cdn.discordapp.com/attachments/438447915908726784/441758883741040651/unknown.png)

ProAudioSoft**-**Yesterday at 5:32 PM

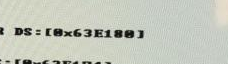
[](https://cdn.discordapp.com/attachments/438447915908726784/441758993124163584/20180503_193323.jpg)

Ok, lemme recheck

JECXZ**-**Yesterday at 5:32 PM

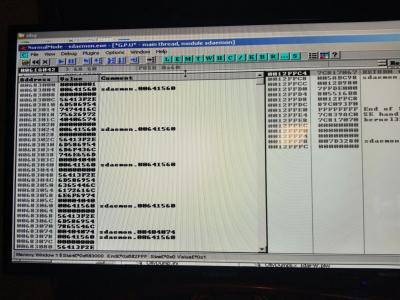
ok so that lower left window

you need to get that address to where the iat is

[](https://cdn.discordapp.com/attachments/438447915908726784/441759102545166347/unknown.png)

one hint are those DS:[Addr] calls to kernel32 functions

those offsets are in the IAT

[](https://cdn.discordapp.com/attachments/438447915908726784/441759303599259648/20180503_193452.jpg)

JECXZ**-**Yesterday at 5:34 PM

ok so in that window

you want to scroll up to 0x63E180

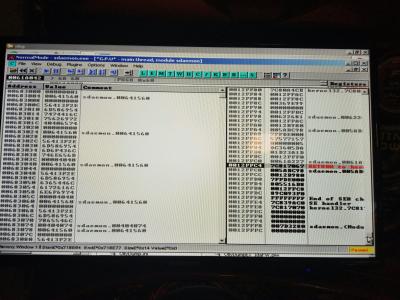
thats not the beginning of the IAT but it will be in the IAT

once you get there you'll have to scroll up a bit

youll know youre at the top of the IAT when you stop seeing DLL names

ProAudioSoft**-**Yesterday at 5:36 PM

In

[](https://cdn.discordapp.com/attachments/438447915908726784/441759944375795722/20180503_193720.jpg)

In right window?

JECXZ**-**Yesterday at 5:36 PM

no

right click on the left window

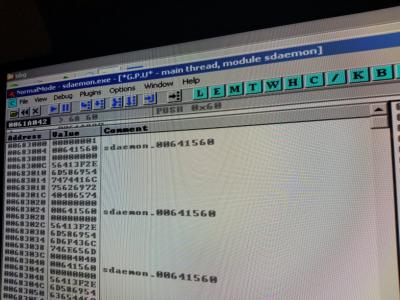
ProAudioSoft**-**Yesterday at 5:36 PM

Can't scroll any further in left

JECXZ**-**Yesterday at 5:37 PM

one second

ProAudioSoft**-**Yesterday at 5:37 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441760321066237953/20180503_193844.jpg)

Ok

JECXZ**-**Yesterday at 5:39 PM

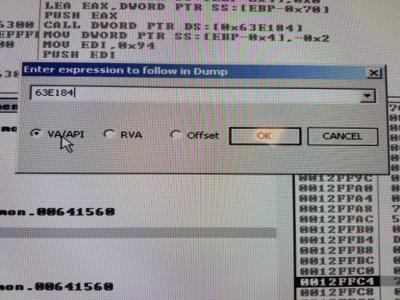
right click on the left window

the lower left window yeah

and put goto->expression

and type 63E184

ProAudioSoft**-**Yesterday at 5:42 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441761472897613824/20180503_194328.jpg)

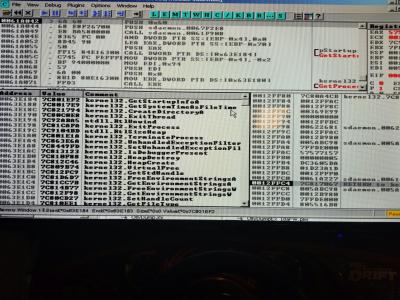
Good?

JECXZ**-**Yesterday at 5:42 PM

yup

ProAudioSoft**-**Yesterday at 5:42 PM

Ok

[](https://cdn.discordapp.com/attachments/438447915908726784/441761664887422983/20180503_194416.jpg)

Puts me here

JECXZ**-**Yesterday at 5:43 PM

yup

thats in the iat

now scroll up until you stop seeing dll names

why does your scrolling not work ?

thats some weird shit

do the goto think again and type 63E000

see where that takes you(edited)

or actually

do 62E000

it should be before the iat I'm guessing

then you can scroll down

ProAudioSoft**-**Yesterday at 5:45 PM

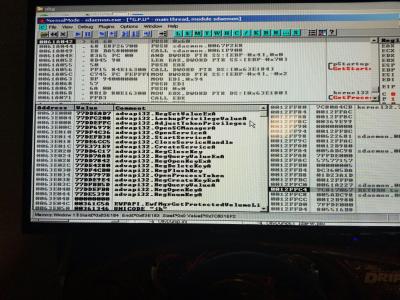
Already scrolled there, that's at top

JECXZ**-**Yesterday at 5:45 PM

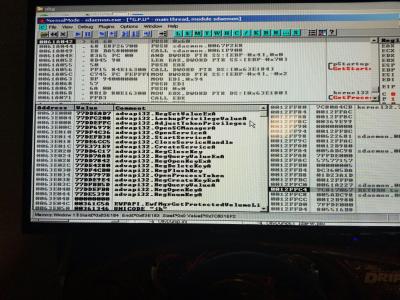
yeah its not supposed to be

idk why its doing that

ProAudioSoft**-**Yesterday at 5:45 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441762240383680543/20180503_194632.jpg)

ProAudioSoft**-**Yesterday at 5:45 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441762240383680543/20180503_194632.jpg)

JECXZ**-**Yesterday at 5:45 PM

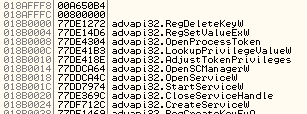
ok thats "probably" the top but lets be sure

go to 62E5000 or something

and scroll down until you start seeing those dll names

JECXZ**-**Yesterday at 5:46 PM

like the top of batmans looked like this

[](https://cdn.discordapp.com/attachments/438447915908726784/441762606798340096/unknown.png)

ProAudioSoft**-**Yesterday at 5:46 PM

No memory on specified address

JECXZ**-**Yesterday at 5:47 PM

oh I added a zero

62E500

ProAudioSoft**-**Yesterday at 5:47 PM

Ok, let me see

JECXZ**-**Yesterday at 5:47 PM

note that for batmans the start of the IAT is at 18B0000 where you see the first advapi32 reference

yours more than likely wont be the same entry/name but thats to give you an idea about what it looks like

ProAudioSoft**-**Yesterday at 5:48 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441763097728909322/20180503_194955.jpg)

Looks pretty similar at top, I can go above to address if you want though

JECXZ**-**Yesterday at 5:49 PM

yeah

just to be sure

JECXZ**-**Yesterday at 5:49 PM

if you fuck up where it starts we have to do it over

lol

so lets make sure

ProAudioSoft**-**Yesterday at 5:55 PM

Man I think its right. Easy to do over now that I know how lol

On this one anyway, know its not one size fits all

JECXZ**-**Yesterday at 5:56 PM

actually that first part

yeah

thats how you do it on both versions of the envelope

but theres still more shit to do

ProAudioSoft**-**Yesterday at 5:56 PM

I know

Grrr

JECXZ**-**Yesterday at 5:56 PM

this is actually the easy part haha

ProAudioSoft**-**Yesterday at 5:56 PM

Cool

JECXZ**-**Yesterday at 5:56 PM

now we have to reconstruct the imports that the envelope stole

if you scroll down that list

you'll see some entries sandwiched between dll names

with sdaemon.#######

those are ones we have to fix

ProAudioSoft**-**Yesterday at 5:57 PM

Ah

JECXZ**-**Yesterday at 5:57 PM

and using imprec at this point isn't a good idea

so we need to figure out what those functions are supposed to be

'most' of them will be kernel32 functions

but sometimes ws2\_32 functions too

one thing to note

JECXZ**-**Yesterday at 5:58 PM

when you see 00000000 00000000

that's the end of the IAT

two blank entries are how the pe format denotes the end of a section

ProAudioSoft**-**Yesterday at 5:59 PM

Sdaemon.00000000?

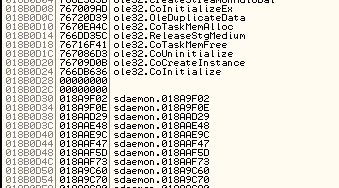
JECXZ**-**Yesterday at 5:59 PM

no youll just see 00000000 00000000

ProAudioSoft**-**Yesterday at 5:59 PM

Ok

JECXZ**-**Yesterday at 5:59 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441765875373047819/unknown.png)

like that

ProAudioSoft**-**Yesterday at 6:00 PM

Ah

JECXZ**-**Yesterday at 6:00 PM

anything after that is in .rdata and doesn't matter for the import stuff

ProAudioSoft**-**Yesterday at 6:00 PM

Cool

JECXZ**-**Yesterday at 6:00 PM

so in batmans case above

the IAT is of size 0xD30

because it started at 0x18B0000 and ends at 0x18B0D30

ProAudioSoft**-**Yesterday at 6:01 PM

Ok

JECXZ**-**Yesterday at 6:01 PM

where that first sdaemon whatever entry in rdata is after the 8 bytes of NULL(edited)

so in that list, if you see anything with sdaemon.########

that's an import that has to be fixed

the pdf guide that I sent over before will explain how to do that

most of those can be found by looking at the guide

what you'll want to do is right click on them in that lower left window and select 'follow in disassembler'

and look at the assembly and compare it to the pictures in the guide

it will tell you what those functions are supposed to be

THEN what you do is ... remember that window we used to set the breakpoint on kernel32?

we go to that, look up the name of the function, find the dll and export line

and look at the address on the left hand column

make a note of it

go back to the entry in the lower left window, right click and hit "Modify"

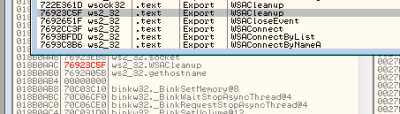
and enter that address

ProAudioSoft**-**Yesterday at 6:04 PM

This sounds like the hard part lol

Haha

JECXZ**-**Yesterday at 6:04 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441767115440128021/unknown.png)

see what I did?

I found that entry, then modified where it said sdaemon.xxxxxxxx

and wrote that address in there and olly automatically updated it to say "ws2\_32.WSACleanup"

once you fix all those the IAT will be fixed

then we can talk about the next step

ProAudioSoft**-**Yesterday at 6:06 PM

Its all done in olly?

JECXZ**-**Yesterday at 6:06 PM

yes

we're doing it the right way

other tools will just fuck this up

it's easier to fix it here first

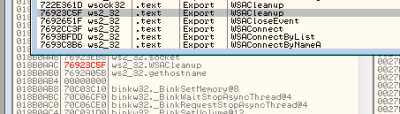
ProAudioSoft**-**Yesterday at 6:06 PM

Ok

So what's first thing I should do

One step at a time lol

JECXZ**-**Yesterday at 6:06 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441767644551577608/unknown.png)

whoops

so go back to your window

the one with the advapi32 names

and scroll down until you find an entry that says sdaemon.xxxxxxxx

the x's will be numbers of course

ProAudioSoft**-**Yesterday at 6:07 PM

Right

JECXZ**-**Yesterday at 6:07 PM

and show me

ProAudioSoft**-**Yesterday at 6:07 PM

Ok, appreciate your patience :)

JECXZ**-**Yesterday at 6:07 PM

hey no problem

I don't do this often enough so it's good to help someone else understand it

maybe I'll remember it better this time

ProAudioSoft**-**Yesterday at 6:08 PM

Don't look at right window shit right?

JECXZ**-**Yesterday at 6:08 PM

yeah thats the stack view

ignore that

ProAudioSoft**-**Yesterday at 6:08 PM

Ok, stack right

JECXZ**-**Yesterday at 6:09 PM

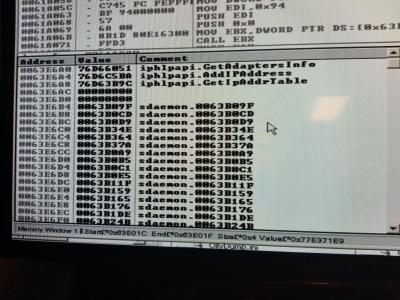
we don't really need to worry about the stack right now because we're just gonna stay at oep forever

JECXZ**-**Yesterday at 6:09 PM

which is oddly enough where batman still is right now lol

I just left olly running lol

ProAudioSoft**-**Yesterday at 6:10 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441768442333495296/20180503_201111.jpg)

JECXZ**-**Yesterday at 6:10 PM

so thats the end

scroll back up

ProAudioSoft**-**Yesterday at 6:10 PM

No

JECXZ**-**Yesterday at 6:10 PM

yeah

0000000000000000

ProAudioSoft**-**Yesterday at 6:10 PM

Many more

Oh right

JECXZ**-**Yesterday at 6:10 PM

3E6B4 is the end of the IAT

and between there and the top

you didn't see 'any' entries that were sdaemon.xxxxxxxx

ProAudioSoft**-**Yesterday at 6:11 PM

Lemme check

Is ac b0 or b4 end

JECXZ**-**Yesterday at 6:12 PM

for your notes your iat size is 63E6B4 - 63E000 = 6B4

ProAudioSoft**-**Yesterday at 6:12 PM

Ok

Is ac b0 or b4 end

JECXZ**-**Yesterday at 6:13 PM

b4 is the end

the first line of not zeroes

is considered the end

technically the first line of the new section

ProAudioSoft**-**Yesterday at 6:13 PM

Ok

JECXZ**-**Yesterday at 6:13 PM

yeah that's confusing

lol

ProAudioSoft**-**Yesterday at 6:15 PM

I do not see any sdaemon.######## before end

JECXZ**-**Yesterday at 6:15 PM

really?

hrmm

and you checked through all the kernel32 ones?

double check the kernel32 ones

those are the most likely

and if you have any ws2\_32 ones

ProAudioSoft**-**Yesterday at 6:17 PM

Lemme check more

JECXZ**-**Yesterday at 6:18 PM

it's "possible" that this older version didn't play the emulated function game

although we should make sure first

if that's truly the case and we're sure they arent there

the next step involves this script

[section\_fixer.txt](https://cdn.discordapp.com/attachments/438447915908726784/441770942495064065/section_fixer.txt)

but we need to figure out where section boundaries are first before we run it(edited)

chiefly where the data section starts

as we know where .rdata starts (where the IAT starts)(edited)

ProAudioSoft**-**Yesterday at 6:22 PM

Yeah, nothing sdaemon there

JECXZ**-**Yesterday at 6:22 PM

ok good

then we don't have to do that part lol

ok so now

we need to scroll down in that lower left window

until you see something like

ProAudioSoft**-**Yesterday at 6:22 PM

Should I put script on external drive?

JECXZ**-**Yesterday at 6:22 PM

yeah

we'll need it in a sec

you can also right click that lower left view

and select Hex->ASCII 8 bytes

ProAudioSoft**-**Yesterday at 6:23 PM

Done

JECXZ**-**Yesterday at 6:23 PM

so we need to figure out how big this rdata section is by finding out where the data section starts

we'll want to look where it starts doing this shit

?AV

?AVSomeclassName@Decorator stuff

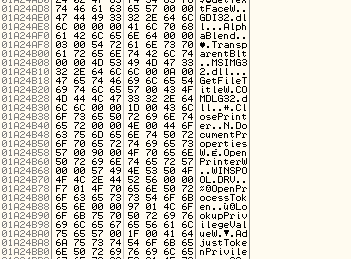
ProAudioSoft**-**Yesterday at 6:24 PM

Lost me

Ha

JECXZ**-**Yesterday at 6:25 PM

ok so scroll down in the hex view

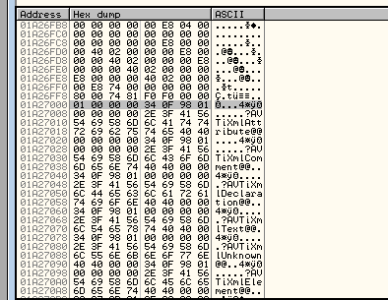
[](https://cdn.discordapp.com/attachments/438447915908726784/441772262157189122/unknown.png)

until you start seeing the function names

like this

then after that you might see some offsets that arent text

keep going a bit until you get to something that looks like this

[](https://cdn.discordapp.com/attachments/438447915908726784/441772517590302730/unknown.png)

thats actually the start of the .data section in batman

find something that looks like that and show me

I generally look for class names which start with ?AVblahblah

oh nvm

we don't even have to fix these

man this older envelope was stupid lol

they didn't pack the sections

ok fine we won't have to use the script

ok so ... next step hrmm

we should just be able to dump it now that we know some of the stuff

do you have the ollydump plugin?

ProAudioSoft**-**Yesterday at 6:30 PM

Yes

Don't I have to find that info in hex

JECXZ**-**Yesterday at 6:30 PM

ok so bring that up and show me the options

nope

ProAudioSoft**-**Yesterday at 6:31 PM

Ok

JECXZ**-**Yesterday at 6:31 PM

they didn't pack the sections

they are exactly where they're supposed to be

in your memory map screenshot from before

ProAudioSoft**-**Yesterday at 6:31 PM

Ha

JECXZ**-**Yesterday at 6:31 PM

you'll see that rdata starts exactly where we found it

and data is after that

ProAudioSoft**-**Yesterday at 6:31 PM

Ok

JECXZ**-**Yesterday at 6:31 PM

so we just cut about 80% of the work on this out

lol

ProAudioSoft**-**Yesterday at 6:31 PM

Sweet

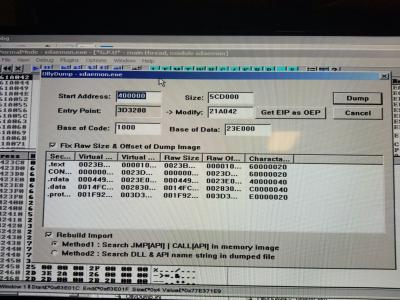
JECXZ**-**Yesterday at 6:31 PM

like I said this old envelope was terrible lol

no wonder they changed it

ok so bring up the ollydump window

ProAudioSoft**-**Yesterday at 6:32 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441774109374939136/20180503_203339.jpg)

JECXZ**-**Yesterday at 6:33 PM

so click get EIP as OEP

ProAudioSoft**-**Yesterday at 6:33 PM

K

JECXZ**-**Yesterday at 6:33 PM

ok

now hit dump

and send me the result and I'll check to see if we need to use imprec to fix the section

we might not

we might be lucky in this case

but I'll be able to pretty easily tell if we need to do more

ProAudioSoft**-**Yesterday at 6:34 PM

Ok

JECXZ**-**Yesterday at 6:35 PM

ida is pretty good about pissing and fuckin moaning if something is wrong

so it's a good acid test

lol

ProAudioSoft**-**Yesterday at 6:37 PM

[H20-jecxz.exe](https://cdn.discordapp.com/attachments/438447915908726784/441775396070096896/H20-jecxz.exe)

5.80 MB

JECXZ**-**Yesterday at 6:38 PM

ok lets see how you did

ProAudioSoft**-**Yesterday at 6:38 PM

ok

JECXZ**-**Yesterday at 6:39 PM

this looks pretty good

olly made a new import section and technically we could take out .protect and the old section

if we wanted to be super anal about it but this looks good

looks like it should run

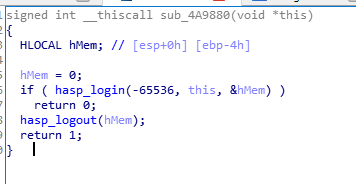
now of course the game uses the dongle

sub\_5A3260 is hasp\_login

so lets see what they did with the dongle

maybe its just a stupid like... is it plugged in thing

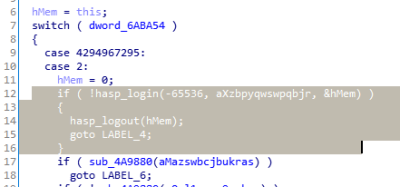
well

[](https://cdn.discordapp.com/attachments/438447915908726784/441776429504659457/unknown.png)

theres one stupid is it plugged in thing

lol

there was another hasp call - lets see what that does

[](https://cdn.discordapp.com/attachments/438447915908726784/441776644814929930/unknown.png)

and theres another stupid is it plugged in thing

ok so we could build a dll for this but honestly

going the cheap shitty route of patching this is faster

one second

[H20\_patched.exe](https://cdn.discordapp.com/attachments/438447915908726784/441777651087048714/H20_patched.exe)

5.80 MB

easy breezy beautiful, covergirl

JECXZ**-**Yesterday at 6:48 PM

im gonna try running it although I suspect that this doesnt support the newer IO

so its going to hit an illegal opcode because of the in,out calls

let's see

ProAudioSoft**-**Yesterday at 6:49 PM

curious

JECXZ**-**Yesterday at 6:50 PM

hrmm

it exits because it reads from my registry and something

but it doesnt crash

so theres probably more stuff but hey run it on the real machine

see what happens

chances are it should work

JECXZ**-**Yesterday at 6:51 PM

oh yeah this doesnt use the rio... guess I have to emulate the fuckin "JammaUSB"); now

lol

ProAudioSoft**-**Yesterday at 6:51 PM

oh shit

JECXZ**-**Yesterday at 6:51 PM

ahh whatever I was going to have to anyway eventually lol

ProAudioSoft**-**Yesterday at 6:51 PM

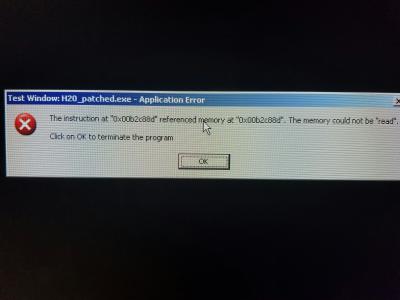
ha

JECXZ**-**Yesterday at 6:52 PM

I mean it looks sane to me man

lemme know if it boots

ProAudioSoft**-**Yesterday at 6:55 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441779849187557387/20180503_205630.jpg)

JECXZ**-**Yesterday at 7:02 PM

hrmm... I can't get that message... for some reason mine starts and then closes

did you run sdaemon directly?

with like no command line parameters?

ProAudioSoft**-**Yesterday at 7:03 PM

yes, directly, as named from you

usb gate is installed and running

didnt think that would matter

JECXZ**-**Yesterday at 7:05 PM

I dont think it has anything to do with that

those were the only two dongle login calls

so they don't really do much

ProAudioSoft**-**Yesterday at 7:09 PM

this one has motion dongle option too, cool

unpatched dump with dongle, same error

JECXZ**-**Yesterday at 7:20 PM

ok so I figured out why mine was closing

the game is 1360/768

so I had to patch it to something dx9 could fullscreen

now its crashing, lets see why

JECXZ**-**Yesterday at 7:29 PM

ok its missing a directx import

that's why

do you still have olly open?

ProAudioSoft**-**Yesterday at 7:30 PM

no, but I can bring it back up

JECXZ**-**Yesterday at 7:30 PM

ok

get back to oep and then dump it but this time uncheck the import box

we'll have to fix it in imprec

it's possible that you can just hardware execute breakpoint the same spot

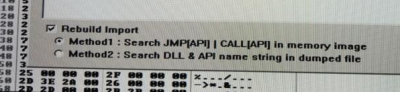
it might load in the same address if you havent rebooted

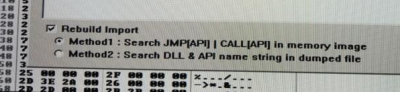
ProAudioSoft**-**Yesterday at 7:31 PM

Ok

JECXZ**-**Yesterday at 7:31 PM

yeah so we're gonna uncheck this guy

[](https://cdn.discordapp.com/attachments/438447915908726784/441788956842131456/unknown.png)

[](https://cdn.discordapp.com/attachments/438447915908726784/441788956842131456/unknown.png)

because fuck ollydump's import rebuilding

lol

ProAudioSoft**-**Yesterday at 7:32 PM

Ha

JECXZ**-**Yesterday at 7:32 PM

what we'll do is we'll stick the new IAT where .protect is

might as well

not like any of that is useful

ProAudioSoft**-**Yesterday at 7:33 PM

Broke at same spot

Uncheck and redump?

JECXZ**-**Yesterday at 7:34 PM

yes

then fire up imprec

JECXZ**-**Yesterday at 7:34 PM

im using 1.7e final

that was the last version made iirc

then of course we'll want to set the oep which is that eip address in olly minus 400000

well essentially what it says in ollydump... that 21a042 thing

ProAudioSoft**-**Yesterday at 7:36 PM

Imprec loaded

JECXZ**-**Yesterday at 7:36 PM

then the iat is the same thing - the start of rdata - 400000

63e000 - 400000

23E000

then the size was what I said before

6b4

and hit get imports

they should all load up

scroll down the list and make sure every single one says valid

I missed the step where you select the sdaemon process but I figured you already knew that

ProAudioSoft**-**Yesterday at 7:38 PM

In left section right

JECXZ**-**Yesterday at 7:38 PM

yeah

ProAudioSoft**-**Yesterday at 7:38 PM

Change oep to?

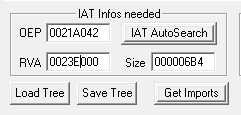
JECXZ**-**Yesterday at 7:38 PM

21a042

ProAudioSoft**-**Yesterday at 7:39 PM

And rva

JECXZ**-**Yesterday at 7:39 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441790990077132810/unknown.png)

should be this

then click get imports

and it should populate the top list

ProAudioSoft**-**Yesterday at 7:40 PM

Just wanted to make sure

It did

JECXZ**-**Yesterday at 7:40 PM

ok scroll through it

ProAudioSoft**-**Yesterday at 7:40 PM

Will check

JECXZ**-**Yesterday at 7:40 PM

make sure every one says valid YES

ProAudioSoft**-**Yesterday at 7:40 PM

All valid

JECXZ**-**Yesterday at 7:41 PM

ok good

how many entries are under d3d9 btw

also is it the last one in the list

ProAudioSoft**-**Yesterday at 7:42 PM

One

X9 has many

JECXZ**-**Yesterday at 7:43 PM

ok good

is the d3d9 one the last in the list?

ProAudioSoft**-**Yesterday at 7:43 PM

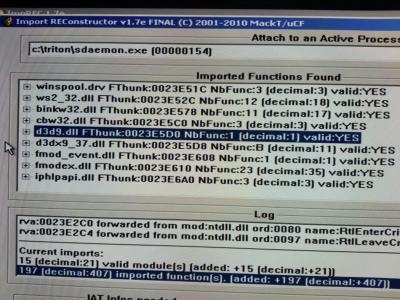
No

JECXZ**-**Yesterday at 7:43 PM

ok so now

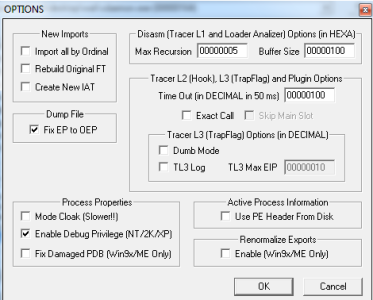
we're going to write the iat to the head of the protect section

ProAudioSoft**-**Yesterday at 7:43 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441792063776751616/20180503_214504.jpg)

JECXZ**-**Yesterday at 7:44 PM

click options

[](https://cdn.discordapp.com/attachments/438447915908726784/441792150150053888/unknown.png)

make sure it looks like this

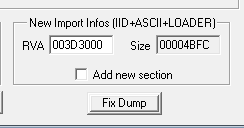
ProAudioSoft**-**Yesterday at 7:45 PM

Done

JECXZ**-**Yesterday at 7:45 PM

ok

last step

[](https://cdn.discordapp.com/attachments/438447915908726784/441792459379572754/unknown.png)

that section

uncheck that box

the add new section box

ProAudioSoft**-**Yesterday at 7:45 PM

K

JECXZ**-**Yesterday at 7:45 PM

and write 3d3000 in it

the size wont be the same

its auto calculated

nbd

once you change the rva to 3d3000 after unchecking that box, click fix dump

and make sure to fix the dump exe you just made with olly

and send that

ProAudioSoft**-**Yesterday at 7:46 PM

Ok cool!

JECXZ**-**Yesterday at 7:46 PM

ill patch out the hasp shit and we'll try this again

there's a possibility it might fuck up if something references protect but I really doubt it

pretty sure that added section is just for the envelope

ProAudioSoft**-**Yesterday at 7:49 PM

[H20-Rebuild\_.exe](https://cdn.discordapp.com/attachments/438447915908726784/441793426057592832/H20-Rebuild_.exe)

5.80 MB

JECXZ**-**Yesterday at 7:50 PM

[H20-Rebuild\_patched.exe](https://cdn.discordapp.com/attachments/438447915908726784/441793729343389716/H20-Rebuild_patched.exe)

5.80 MB

ProAudioSoft**-**Yesterday at 7:54 PM

cool, will test

JECXZ**-**Yesterday at 7:55 PM

oh also

if you still have imprec open

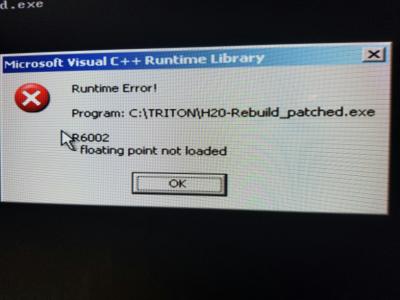
make another version but check the add new section box

just in case it fucks up

and send that one

I can fix that one if need be

ProAudioSoft**-**Yesterday at 7:57 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441795530050502676/20180503_215847.jpg)

JECXZ**-**Yesterday at 7:57 PM

yeah

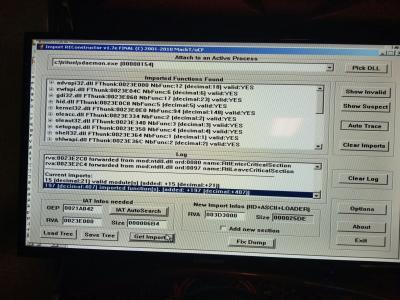
thats a section issue

ok do the imprec thing

JECXZ**-**Yesterday at 7:58 PM

but add a new section this time

ProAudioSoft**-**Yesterday at 8:01 PM

[](https://cdn.discordapp.com/attachments/438447915908726784/441796479225430047/20180503_220236.jpg)

Sitting there

JECXZ**-**Yesterday at 8:01 PM

ok check the add new section box

and click fix dump

ProAudioSoft**-**Yesterday at 8:02 PM

Fix olly dump right?

JECXZ**-**Yesterday at 8:02 PM

yes

the one you dumped from olly last

ProAudioSoft**-**Yesterday at 8:02 PM

Haha

[H20-Rebuild\_.exe](https://cdn.discordapp.com/attachments/438447915908726784/441797310486282245/H20-Rebuild_.exe)

5.81 MB

JECXZ**-**Yesterday at 8:06 PM

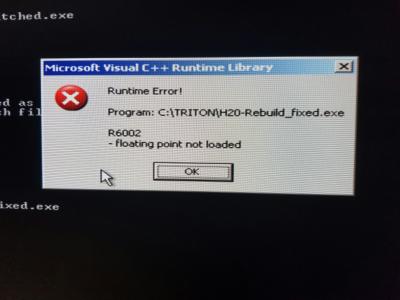
[H20-Rebuild\_fixed.exe](https://cdn.discordapp.com/attachments/438447915908726784/441797771725373445/H20-Rebuild_fixed.exe)

5.81 MB

try this one

ProAudioSoft**-**Yesterday at 8:06 PM

k

[](https://cdn.discordapp.com/attachments/438447915908726784/441800195542614017/20180503_221253.jpg)

JECXZ**-**Yesterday at 8:30 PM

[H20-Rebuild\_take4.exe](https://cdn.discordapp.com/attachments/438447915908726784/441803760365469716/H20-Rebuild_take4.exe)

5.81 MB

shit wrong window

lol deleted it though

but yeah

that should do it

my system restarted while testing

but that should fix it

ProAudioSoft**-**Yesterday at 9:04 PM

Great work!!!!!

JECXZ**-**Yesterday at 9:10 PM

hey you did it not me lol

great work to you sir

that was a good one to do I think

less steps

now we'll just have to do another one with the new envelope and you'll know how to do both variants

ProAudioSoft**-**Yesterday at 9:22 PM

Thanks! Couldnt have without your help!

Have superbikes 2 dongle in now lol

JECXZ**-**Yesterday at 9:22 PM

that was fun, we should do that again sometime xD

nice

does that also use the envelope?

ProAudioSoft**-**Yesterday at 9:23 PM

yes

I can send torrent

have latest version

JECXZ**-**Yesterday at 9:24 PM

nice