How to dump LoL + get addresses: The guide

6th February 2019, 08:29 PM #1

shattter
h4x0!2

Join Date: Oct 2016
Location: mr worldwide
Posts: 118
Reputation: 7165
Rep Power: 148

Recognitions
Donator (1)

Points: 13,178, Level: 14
Level up: 68%, 422 Points needed
Activity: 2.5%

Last Achievements

How to dump LoL + get addresses: The guide

Hey guys,

As Matt is taking a step away due to IRL work, my inbox here and my Discord DM's have already been blowing up over the last week with questions regarding:

"How to get the latest addresses, none in megathread?!"
"You said before to use IDA, but how to get them?"
"I can't dump the game doesn't work help pls".

I do not mind **AT ALL** getting these multiple times a day, however instead of privately telling each of you having issues it's just going to make my life easier by writing this one time guide - as well as hopefully allowing some of you to not only rely on the offset thread, but also contribute

First things first, you will need 3 things:

- Tarekwiz' league dumper, I recommend this for beginners due to ease of use (https://github.com/tarekwiz/LeagueDumper)
- IDA Pro, most of you interested in this have it already so won't be providing info on how to get
- League, obviously..

Nice, with those 3 things you can now begin to find updated function addresses/offsets.

Step 1: Launching into a practice tool on league

You will need to launch a practice tool game - as this is where you will dump the game. Those of you that try to put the League of Legends.exe into IDA will know it is packed, and this is why you can't xref things / the exe is pretty useless without unpacking it. By running the game we are no longer totally limited by the packer as things have to be unpacked in order for the game to actually run.

https://vgy.me/FWiuUT.jpg

Step 2: Using the dumper

This step is pretty straightforward as well - however many people seem to get pretty stuck here. Those of you that tried dumping with scylla by suspending in process hacker etc will know it doesn't work as intended, and there are numerous posts on this in the AC thread from a while back so I won't regurgitate the info now, simply go back and read the thread.

With tareks modified process-dump, we can put the pd.exe into a directory (desktop/league stuff) etc, wherever you want to store your dumps each patch.

Next we open a CMD window, and navigate to our folder where we put the pd.exe, to do this type "cd /d d:\league" or wherever/whatever you decided to use.

Code:

```
1. C:\Users\shatter>cd /d C:\Users\shatter\Desktop\leageu work
```

(i know league is spelt wrong I just kinda left it cos why not lol)

Now you will want to type

Code:

```
1. pd.exe -pid 12345
```

where 12345 is your League of Legends.exe process ID. This can easily be found by opening Task Manager, navigating to Details tab and reading the process ID from there:

https://vgy.me/ujvbSG.png

In my case, that is 7652. This means I will use -pid 7652. Before we hit the return key, tab back into league and walk around for a second, cast a spell and then back to CMD and now hit the return key and let the dumper proceed to suspend the process and dump the files.

Some people say you should walk around and cast / others say don't but there's not harm for you to do it.

You will receive a "Finished running" after it is done, and maybe during the dump you got 100s of failed VirtualProtect spams in the console, ignore them. The game will now no longer be responding and is fine to just close via task manager or however you want.

Now in your folder you will see quite a few files produced during the dump, and the important thing is to notice the 2 different exe's. The way the game is packed will produce 2, but the important one is the one outlined in red, with the actual name of League of Legends.exe, rather than the hiddenmodule:

https://vgy.me/3QwRsu.png

Step 3: Moving into IDA

The last step is pretty simple too, just be sure to follow along. What we want to do now is to take the dumped exe and drag it into ida/onto the ida exe, whatever you prefer:

https://vgy.me/ueXel7.png

Take note of a part of the exe name too:

Code:

```
1. League of Legends_exe_PID1c94_League of Legends.exe_150000_x86.exe
```

The 150000 part tells us the game was at base address of 0x150000. This will be very useful now when it comes to finding addresses - those of you whom are used to rebasing I **HEAVILY** recommend not to do that in league, most who do end up with issues with correct addresses.

In IDA we will hit ok on the first window, and no when it asks to search for the symbol (won't find riots symbol on the microsoft server lol).

Now you wait until at the bottom left of IDA it says AU: idle
https://vgy.me/XAaQs6.png (superb image here no flame)

This means IDA has finished, can now go about looking for an address.

Hit Shift+F12 to generate all the strings, and when inside the string window press Ctrl+F to start a search for something. In this tutorial I will show you how to find the localplayer, the isHero function and the isTurret function.

For 9.3 they are:

Code:

```
1. oIsHero = 0x227780
2. oIsTurret = 0x227950
3. oLocalPlayer = 0x2EC1870
```

Search for

Code:

```
1. blueHero
```

and it will look like this:
https://vgy.me/9ns1V0.png

Double click and it will take you here:
https://vgy.me/AFvjzT.png

Now u can press X while highlighting the blueHero, and hit Enter/return.
https://vgy.me/HB8uiK.png

You will now see something like this:

https://vgy.me/XINhp1.png

The red outline are my comments to show you what those actually are.
If you look at the top, above the "you" string you can see the

Code:

```
1.  dword_3011870
```

in my image, for you it will be different - this is due to our different **BASE ADDRESSES.**

Now without me even telling you that that is the localplayer, if we were attempting to work it out without any help, the string "you" is pretty helpful in showing us we must be dealing with "us" as in the localplayer.

The final stage is to just grab that address, subtract the base address of the dump and voila we will have the LocalPlayer for 9.3:

Code:

```
1. 0x3011870 - 0x150000 = 0x2EC1870
```

Now refer to the address above, oLocalPlayer was 0x2EC1870.

From here you can now build a signature (many tutorials on UC) and through a mix of sigs/string cross-references you can obtain all the addresses. An easy way for you beginners would be to wait for all the 9.3 to be posted, and then do the reverse.

- 9.3 Address for GetSpellState is 0x588970
- Add your base address and GetSpellState , so for me it will be 0x588970+ 0x150000 = 0x6D8970
- This is the address I can now jump to in IDA by pressing G and pasting the address into the form; and I will be at the GetSpellState function, from here can search for strings and make patterns.
- Do this for all the stuff you use, and on patch days you won't need to wait for someone to post them, can just run a python script in IDA to grab them all for you from the signatures

Hopefully this was helpful to you, and those with a 9.2 dump can easily update everything that you need to for 9.3, those without just wait for a complete offset list, if I have time I'll post one in a few hours. Sadly UC no longer allows game dumps so I can't upload the 9.2 for you.

I know this was very **VERY** simplified but isn't aimed at anyone that's used IDA or can actually understand the process of finding things from the disassembly, more as an introduction for all the new people that join this section each day

Enjoy - and if you need help don't stop PM'ing me I don't bite just this should clear up a lot of the confusion.

shatter

shattter is offline

QUOTE

6th February 2019, 08:31 PM

#2

Odysex
Senior Member

Join Date: Jan 2019

Posts: 83

Reputation: 191
Rep Power: 86

Points: 860, Level: 1
Level up: 92%, 40 Points needed
Activity: 7.7%

You're nuts, thaks for the tutorial budd. Much love <3

Odysex is offline

QUOTE

6th February 2019, 09:55 PM

#3

Catbert
n00bie

This is awesome, thankyou

Join Date: Jun 2006

Posts: 15

Reputation: 90
Rep Power: 392

Recognitions
Donator (1)

Points: 10,446, Level: 12
Level up: 54%, 554 Points needed
Activity: 6.7%

Last Achievements

Catbert is offline

QUOTE

6th February 2019, 10:03 PM

#4

shattter
h4x0!2

Quote:

> Originally Posted by **Odysex**
> *You're nuts, thaks for the tutorial budd. Much love <3*

Quote:

> Originally Posted by **Catbert**
> *This is awesome, thankyou*

You're welcome

Threadstarter

Join Date: Oct 2016

Location: mr worldwide

Posts: 118

Reputation: 7165
Rep Power: 148

Recognitions
Donator (1)

Points: 13,178, Level: 14
Level up: 68%, 422 Points needed
Activity: 2.5%

Last Achievements

shattter is offline

QUOTE

6th February 2019, 10:39 PM #5

themagicalgamer
n00bie

Join Date: May 2018

Posts: 6

Reputation: 68
Rep Power: 102

Points: 724, Level: 1
Level up: 65%, 176 Points needed
Activity: 1.3%

themagicalgamer is offline

Thank you

QUOTE

6th February 2019, 11:54 PM #6

munnkorn
UC Supporter

Join Date: Nov 2015

Posts: 303

Reputation: 1212
Rep Power: 166

Points: 7,673, Level: 10
Level up: 7%, 1,027 Points needed
Activity: 7.5%

Last Achievements

munnkorn is offline

Thanks, very helpfull!

QUOTE

7th February 2019, 03:37 AM #7

hawhawmatt
Supreme H4x0|2

Great post by a great guy. +rep
Btw, an important thing is that if you have offsets & exes before the anti-cheat patch, you can easily get the new offsets by just making patterns. Most of them haven't changed as far as what I've checked (9.2-)

Last edited by hawhawmatt; 7th February 2019 at 03:44 AM.

Join Date: Oct 2013

Location: 0xDEADBEEF

Posts: 691

Reputation: 6953
Rep Power: 226

Points: 25,362, Level: 22
Level up: 91%, 138 Points needed
Activity: 2.3%

Last Achievements

hawhawmatt is offline

QUOTE

7th February 2019, 04:03 AM

#8

shattter
h4x0!2

Threadstarter

Join Date: Oct 2016

Location: mr worldwide

Posts: 118

Reputation: 7165
Rep Power: 148

Recognitions
Donator (1)

Points: 13,178, Level: 14
Level up: 68%, 422 Points needed
Activity: 2.5%

Last Achievements

shattter is offline

Quote:

> Originally Posted by **hawhawmatt**
> *Great post by a great guy. +rep*
> *Btw, an important thing is that if you have offsets & exes before the anti-cheat patch, you can easily get the new offsets by just making patterns. Most of them haven't changed as far as what I've checked (9.2-)*

Thanks man, hope everything is well with you Great tip as well!

Last edited by shattter; 7th February 2019 at 04:08 AM.

QUOTE

7th February 2019, 04:17 AM

#9

xsm0o0tx
n00bie

Thanks for the tutorial

Join Date: Feb 2019

Posts: 16

Reputation: 10
Rep Power: 85

Points: 1,658, Level: 3
Level up: 37%, 442 Points needed
Activity: 6.1%

Last Achievements

xsm0o0tx is offline

QUOTE

7th February 2019, 04:41 AM

#10

synaxis
n00bie

Very nice
hope we can achieve more in League with this

Join Date: Nov 2017

Posts: 5

Reputation: 10
Rep Power: 113

Points: 894, Level: 1
Level up: 99%, 6 Points needed
Activity: 2.7%

synaxis is offline

QUOTE

7th February 2019, 09:16 AM

#11

hideinnull
n00bie

Very useful post thank you, is there a discord for people working on league at the moment?

Join Date: Jan 2019

Posts: 6

Reputation: 309
Rep Power: 85

Points: 385, Level: 1
Level up: 97%, 15 Points needed
Activity: 4.0%

hideinnull is offline

QUOTE

7th February 2019, 06:11 PM

#12

hackedhacker
Super l337

Join Date: Dec 2013

Posts: 205

Reputation: 1966
Rep Power: 212

Points: 10,149, Level: 12
Level up: 30%, 851 Points needed
Activity: 2.5%

Last Achievements

Elobuddy Rerevive 4.0, yes.

hackedhacker is offline

QUOTE

7th February 2019, 06:40 PM

#13

shattter
h4x0!2

Threadstarter

Join Date: Oct 2016

Location: mr worldwide

Posts: 118

Reputation: 7165
Rep Power: 148

Recognitions
Donator (1)

Points: 13,178, Level: 14
Level up: 68%, 422 Points needed
Activity: 2.5%

Last Achievements

Quote:

> Originally Posted by **hackedhacker**
> *Elobuddy Rerevive 4.0, yes.*

LMAO NOT HERE AS WELL

shattter is offline

QUOTE

7th February 2019, 08:05 PM #14

walangtayoexb
Super H4x0r

Join Date: Dec 2018

Posts: 309

Reputation: 439
Rep Power: 92

Points: 3,656, Level: 6
Level up: 7%, 844 Points needed
Activity: 19.4%

Last Achievements

THANK YOU VERY MUCH !!!!!!!!!!

;how do you find objmanager and aiheroclient? i tried searching networldobject for objmanager but it's empty(didn't find offset) and how about heroclient? i saw AIHeroClient in string but also empty im really bad at reversing i think

Last edited by walangtayoexb; 8th February 2019 at 07:25 AM.

walangtayoexb is offline

QUOTE

8th February 2019, 12:24 PM #15

Apple Man
A God

Join Date: Dec 2018

Posts: 175

Reputation: -739
Rep Power: 0

Points: 2,424, Level: 4
Level up: 47%, 376 Points needed
Activity: 3.0%

Last Achievements

This is great, thank you.

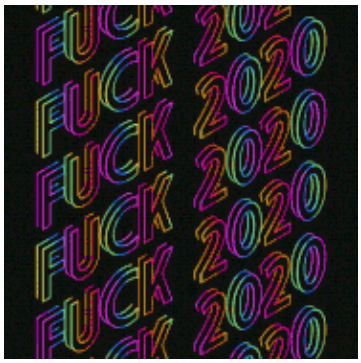
Apple Man is offline

QUOTE

9th February 2019, 12:16 AM #16

usafaqb
2020's Bitch

what a useful post! excellent write up. thank you!



Join Date: Feb 2018

Posts: 47

Reputation: 1056
Rep Power: 109

Recognitions
Donator (2)

Points: 3,923, Level: 6
Level up: 36%, 577 Points needed
Activity: 2.6%

Last Achievements

usafaqb is offline

QUOTE

10th February 2019, 06:20 AM #17

Enelx
Junior Member

Really nice tutorial, but your examples seems to be the only ones i can find with strings, how to find objectmanager for example ?

Join Date: Mar 2018

Posts: 54

Reputation: -101
Rep Power: 0

Points: 2,311, Level: 4
Level up: 31%, 489 Points needed
Activity: 2.2%

Last Achievements

Enelx is offline

QUOTE

10th February 2019, 02:19 PM #18

shattter

Quote:

h4x0!2

Threadstarter

Join Date: Oct 2016

Location: mr worldwide

Posts: 118

Reputation: 7165
Rep Power: 148

Recognitions
Donator (1)

Points: 13,178, Level: 14
Level up: 68%, 422 Points needed
Activity: 2.5%

Last Achievements

shattter is offline

> Originally Posted by **Enelx**
> *Really nice tutorial, but your examples seems to be the only ones i can find with strings, how to find objectmanager for example ?*

I did explain how to in the post. Here's the 9.3 ObjectManager: 0x2EC0510

Add your base address to it, go to that address in IDA, search for strings / cross reference the ObjManager anyway and look around the functions and make a pattern/use strings.

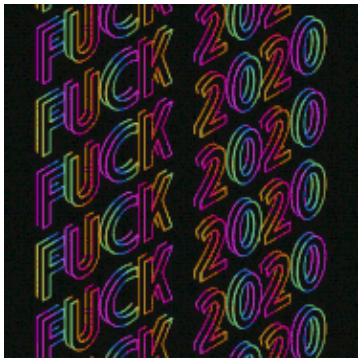
The post is meant to help u find addresses once you have them for a patch. So u use the 9.3 addresses to build your method of finding them, FOR 9.4 onwards

QUOTE

10th February 2019, 05:51 PM

#19

usafaqb
2020's Bitch



Join Date: Feb 2018

Posts: 47

Reputation: 1056
Rep Power: 109

Recognitions
Donator (2)

Points: 3,923, Level: 6
Level up: 36%, 577 Points needed
Activity: 2.6%

Last Achievements

usafaqb is offline

Quote:

> Originally Posted by **shattter**
> *I did explain how to in the post. Here's the 9.3 ObjectManager: 0x2EC0510*
>
> *Add your base address to it, go to that address in IDA, search for strings / cross reference the ObjManager anyway and look around the functions and make a pattern/use strings.*
>
> *The post is meant to help u find addresses once you have them for a patch. So u use the 9.3 addresses to build your method of finding them, FOR 9.4 onwards*

Could 0x2EC0508 possibly be the offset for ObjectManager? matt's base crashes with 0x2EC0510 but runs fine when i put 0x2EC0508

QUOTE

10th February 2019, 07:54 PM #20

shattter
h4x0!2

Threadstarter

Join Date: Oct 2016

Location: mr worldwide

Posts: 118

Reputation: 7165
Rep Power: 148

Recognitions
Donator (1)

Points: 13,178, Level: 14
Level up: 68%, 422 Points needed
Activity: 2.5%

Last Achievements

shattter is offline

Quote:

> Originally Posted by **usafaqb**
> *Could 0x2EC0508 possibly be the offset for ObjectManager? matt's base crashes with 0x2EC0510 but runs fine when i put 0x2EC0508*

Yep Matt's base will use that one, as he directly accesses the object manager, some people use the previous address and subtract the 0x8. Just totally depends on how u find it easier to do when updating via IDA

QUOTE

POST REPLY

Page 1 of 7 **1** 2 3 4 5 > Last »

Similar Threads

Thread	Thread Starter	Forum	Replies	Last Post
[Question] The problem of converting physical addresses to linear addresses	shixiaoyi	C and C++	32	8th March 2020 05:04 AM
[Help] How to get pointer LoL since recent patch preven debugger	iamvip987	League of Legends	3	29th June 2017 06:05 AM
[Release] [Dump] AVA.exe latest dump	Geecko	Alliance of Valiant Arms	10	12th April 2014 01:09 PM

Tags

ida, league, game, address, dump, step, addresses, hit, process, pretty

« Previous Thread | Next Thread »

Forum Jump
League of Legends Go

All times are GMT. The time now is 02:31 PM.