Subject: Extracting strings from the game
Posted by haxorsystem on Fri, 22 May 2015 00:47:09 GMT
View Forum Message <> Reply to Message

I'm not sure if anyone is still interested in this, but I use this way to dump strings out of the game using lua. This method doesn't require any complex skill to achieve a reasonable result.
All you need to know is:
1) How to run a lua script inside the game (I assume everyone here does)
2) Have Cheat Engine installed (Or any other means of accesing a heap of another running program)
3) Be able to parse a string (that's optional but recommended)

The thought is to make a long string containing everything you want to dump and a marker/debug symbol. You need the marker to find your string on the heap. Use the Cheat Engine or whatever you prefer, scan for your marker and extract the memory region where the string is saved. Then you can just parse it in a form of your choice.

Example:

```
local dump = ":"

-- Creating desired string
for key,value in pairs( GUI ) do
 dump = dump .. ( tostring( key ) .. "()\r\n" )
end

-- Adding primitive text marker to the beginning
dump = "ThisIsMyMarker" .. dump

-- Use some blocking call here to stay in the script so you can be sure GC will not free your string and something else will rewrite it.
-- There is a low probability of that happening though if you ALT-TAB and you won't be doing anything in the game.

-- And some indication the string is ready.
GUI.DisplayMessageBox( "Done" )
```

https://imgur.com/a/h5RmN

I checked out to not include the Cheat engine header and i already had braces and newlines from the lua script so i didn't even need any parsing. I only renamed it to GUI.txt

I was thinking redirecting the stdout of the process could be a more elegant way to do this,

because print(is still doing something, I'm just not sure what, but a simple 1>OUT.txt wasn't enough.

Feel free to share your solutions.

File Attachments

1) GUI.txt, downloaded 2111 times