HOW TO BUILD AND RUN IDA PRO PLUGINS

MAKE IDA WORK FOR YOU!

PROF. BRENDAN SALTAFORMAGGIO

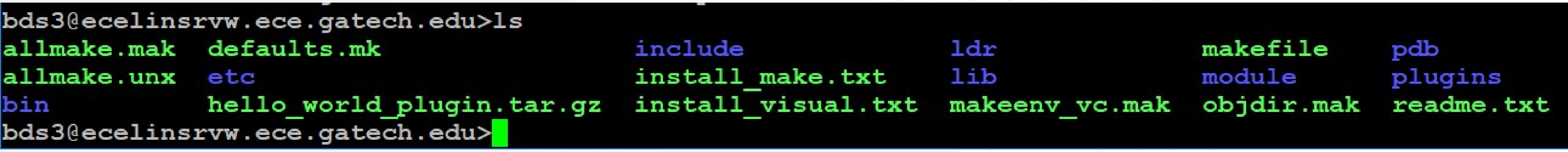
SCHOOL OF ECE

CREATING THE NEXT®

PLEASE CONSIDER THE ENVIRONMENT, AVOID PRINTING SLIDES!

EVERYTHING YOU NEED IS IN THE SDK

- **Run “source /tools/software/hex-rays/idapro.csh” first!**
- The IDA SDK is installed in the /tools/software/hex-rays directory
- Please check out the information in there!



```
bds3@ecelinsrvw.ece.gatech.edu>ls
allmake.mak  defaults.mk                  include              ldr               makefile      pdb
allmake.unx  etc                          install_make.txt     lib               module        plugins
bin          hello_world_plugin.tar.gz    install_visual.txt   makeenv_vc.mak    objdir.mak    readme.txt
bds3@ecelinsrvw.ece.gatech.edu>
```

- The doc directory has documentation on the SDK
  - But the web version may be easier (see the Additional Reading slide)
- The plugins directory has MANY sample plugins with source code
  - Check those out for code examples
  - **/tools/software/hex-rays/idasdk/lastest/plugins/readme.txt**
- The include directory has all the header files for the IDA SDK

- Google, Google, Google!! Many great IDA Plugins are available online!

3 VERSIONS OF PLUGINS!

- Just like IDA, plugins come in 32-bit and 64-bit versions
- The code is mostly identical for both versions

- 32-bit IDA can only run 32-bit plugins & 64-bit IDA can only run 64-bit plugins
  - You need to be careful not to load the wrong plugin version into IDA
  - This can cause IDA to crash

- Plugins written in C++ must be compiled to the specific version you will use
  - Or just compile both versions

- IDA Python plugins do not need to be compiled
- So they can be loaded by either IDA version
  - They can still crash at run time if your code is not careful about the 32-bit/64-bit target binary

GET THE HELLO WORLD PLUGIN!!

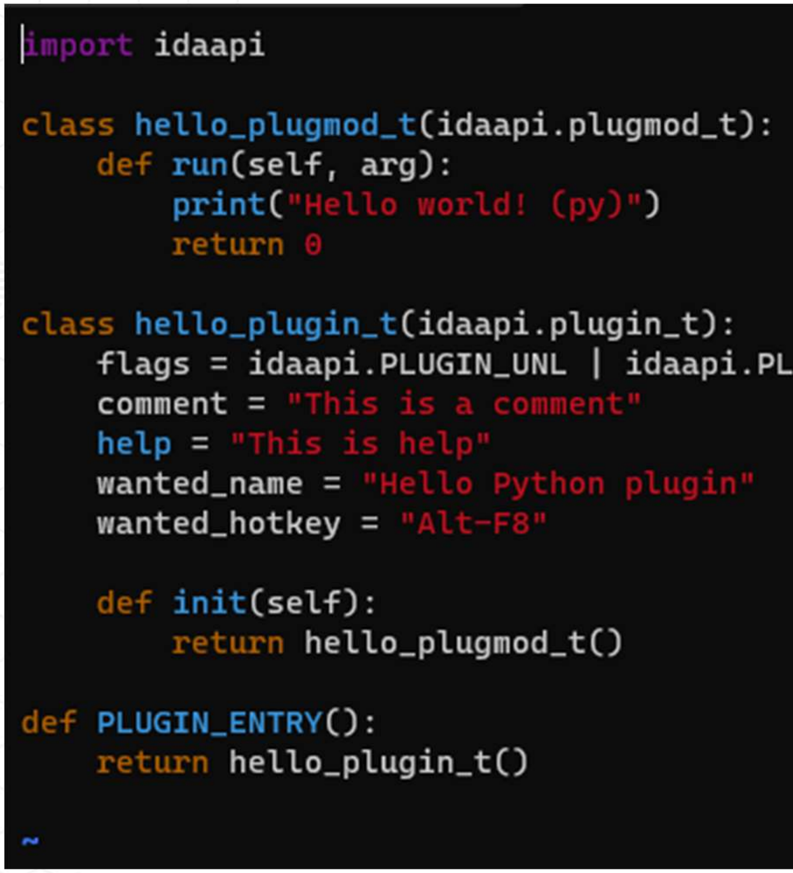
- The place to start is the Hellow World plugin!

/tools/software/hex-rays/idasdk/lastest/plugins/hello

- There is a python version and C++ version in there
- Copy that folder to your home directory and work from there

- If you want to use the C++ version, you'll need to patch the makefile because it includes a bunch of other makefiles from /tools/software/hex-rays/idasdk/lastest/plugins

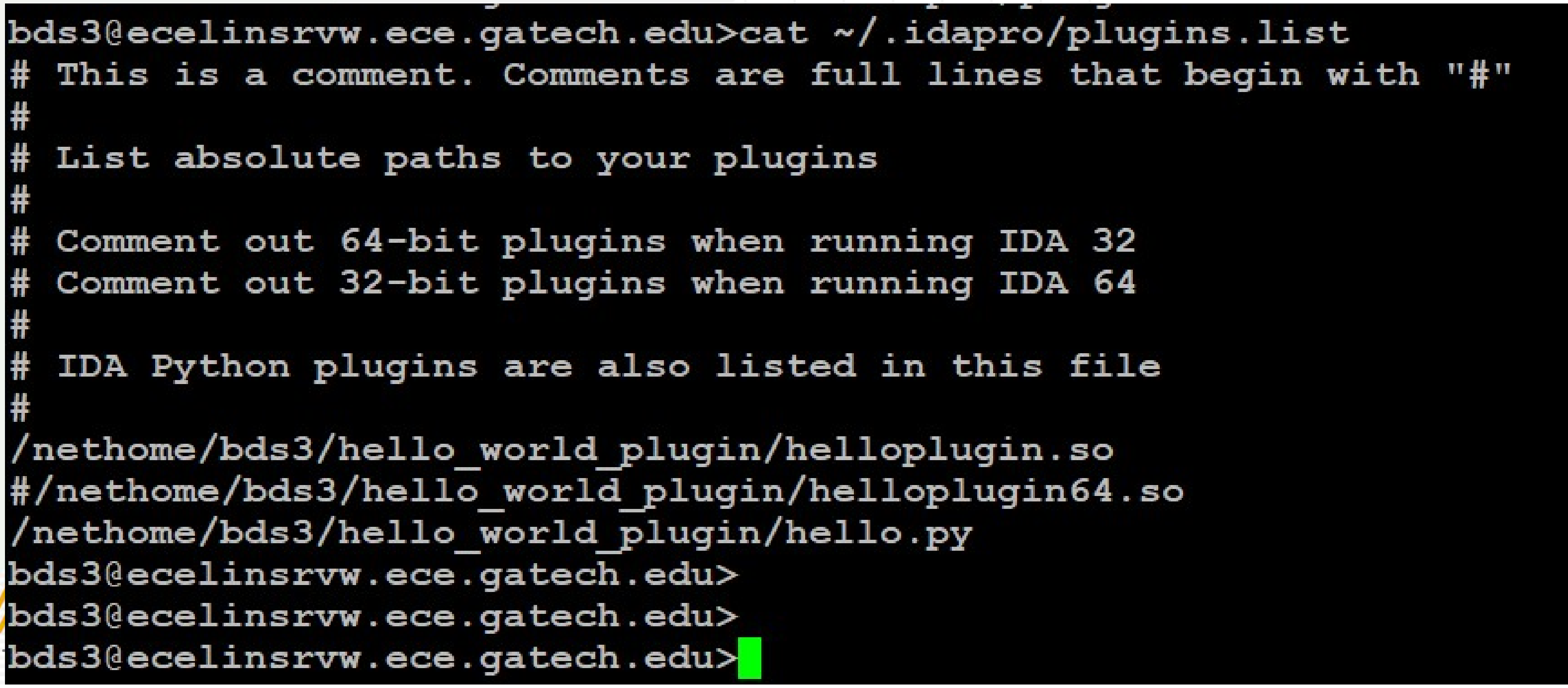
- Python version should work right away



```
import idaapi

class hello_plugmod_t(idaapi.plugmod_t):
    def run(self, arg):
        print("Hello world! (py)")
        return 0

class hello_plugin_t(idaapi.plugin_t):
    flags = idaapi.PLUGIN_UNL | idaapi.PL
    comment = "This is a comment"
    help = "This is help"
    wanted_name = "Hello Python plugin"
    wanted_hotkey = "Alt-F8"

    def init(self):
        return hello_plugmod_t()

def PLUGIN_ENTRY():
    return hello_plugin_t()

~
```

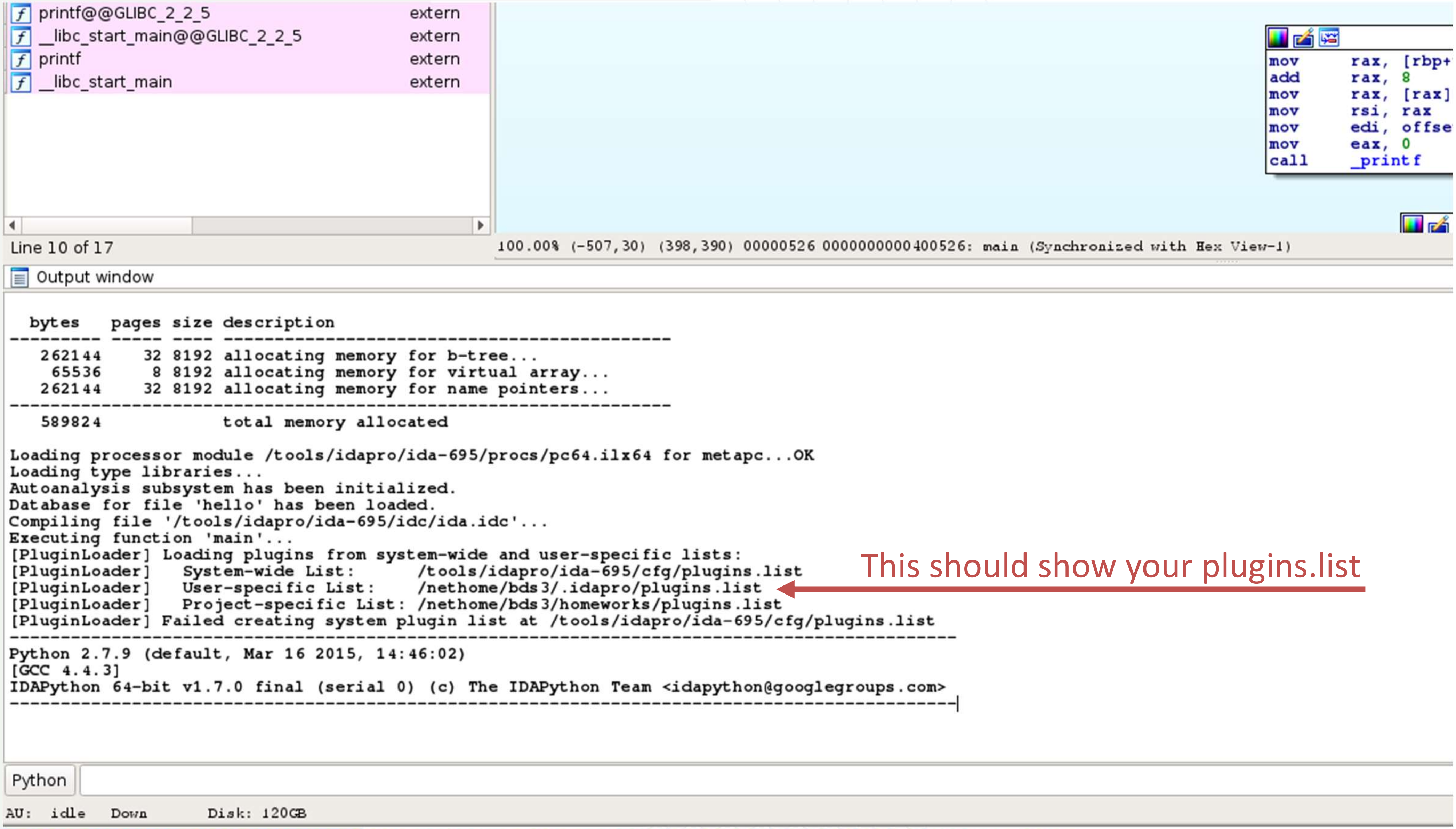
TELL IDA WHERE TO FIND YOUR PLUGIN

- Everyone has a directory called ".idapro" in their home directory on the IDA servers
  - /nethome/<username>/.idapro/   OR ~/.idapro/
- In that directory is a text file called "plugins.list"
  - You may need to create a blank one if it doesn't exist
- IDA reads this file during start-up and loads the plugins listed in it
- List the absolute paths to any plugins that you want IDA to load in this file
  - One plugin path per line, or use "#" to comment the entire line
  - List both Python and compiled plugins in this file
  - Comment out 64-bit plugins before you run 32-bit IDA!
  - Comment out 32-bit plugins before you run 64-bit IDA!



```
bds3@ecelinsrvw.ece.gatech.edu>cat ~/.idapro/plugins.list
# This is a comment. Comments are full lines that begin with "#"
#
# List absolute paths to your plugins
#
# Comment out 64-bit plugins when running IDA 32
# Comment out 32-bit plugins when running IDA 64
#
# IDA Python plugins are also listed in this file
#
/nethome/bds3/hello_world_plugin/helloplugin.so
#/nethome/bds3/hello_world_plugin/helloplugin64.so
/nethome/bds3/hello_world_plugin/hello.py
bds3@ecelinsrvw.ece.gatech.edu>
bds3@ecelinsrvw.ece.gatech.edu>
bds3@ecelinsrvw.ece.gatech.edu>
```

IDA WILL LOAD PLUGINS DURING START UP



```
mov     rax, [rbp+
add     rax, 8
mov     rax, [rax]
mov     rsi, rax
mov     edi, offse
mov     eax, 0
call    _printf
```

```
100.00% (-507,30) (398,390) 00000526 0000000000400526: main (Synchronized with Hex View-1)
```

```
  bytes   pages size description
--------- ----- ---- --------------------------------------------
   262144    32 8192 allocating memory for b-tree...
    65536     8 8192 allocating memory for virtual array...
   262144    32 8192 allocating memory for name pointers...
-----------------------------------------------------------------
   589824            total memory allocated

Loading processor module /tools/idapro/ida-695/procs/pc64.ilx64 for metapc...OK
Loading type libraries...
Autoanalysis subsystem has been initialized.
Database for file 'hello' has been loaded.
Compiling file '/tools/idapro/ida-695/idc/ida.idc'...
Executing function 'main'...
[PluginLoader] Loading plugins from system-wide and user-specific lists:
[PluginLoader]   System-wide List:      /tools/idapro/ida-695/cfg/plugins.list
[PluginLoader]   User-specific List:    /nethome/bds3/.idapro/plugins.list
[PluginLoader]   Project-specific List: /nethome/bds3/homeworks/plugins.list
[PluginLoader] Failed creating system plugin list at /tools/idapro/ida-695/cfg/plugins.list
---------------------------------------------------------------------------------------------
Python 2.7.9 (default, Mar 16 2015, 14:46:02)
[GCC 4.4.3]
IDAPython 64-bit v1.7.0 final (serial 0) (c) The IDAPython Team <idapython@googlegroups.com>
---------------------------------------------------------------------------------------------
```

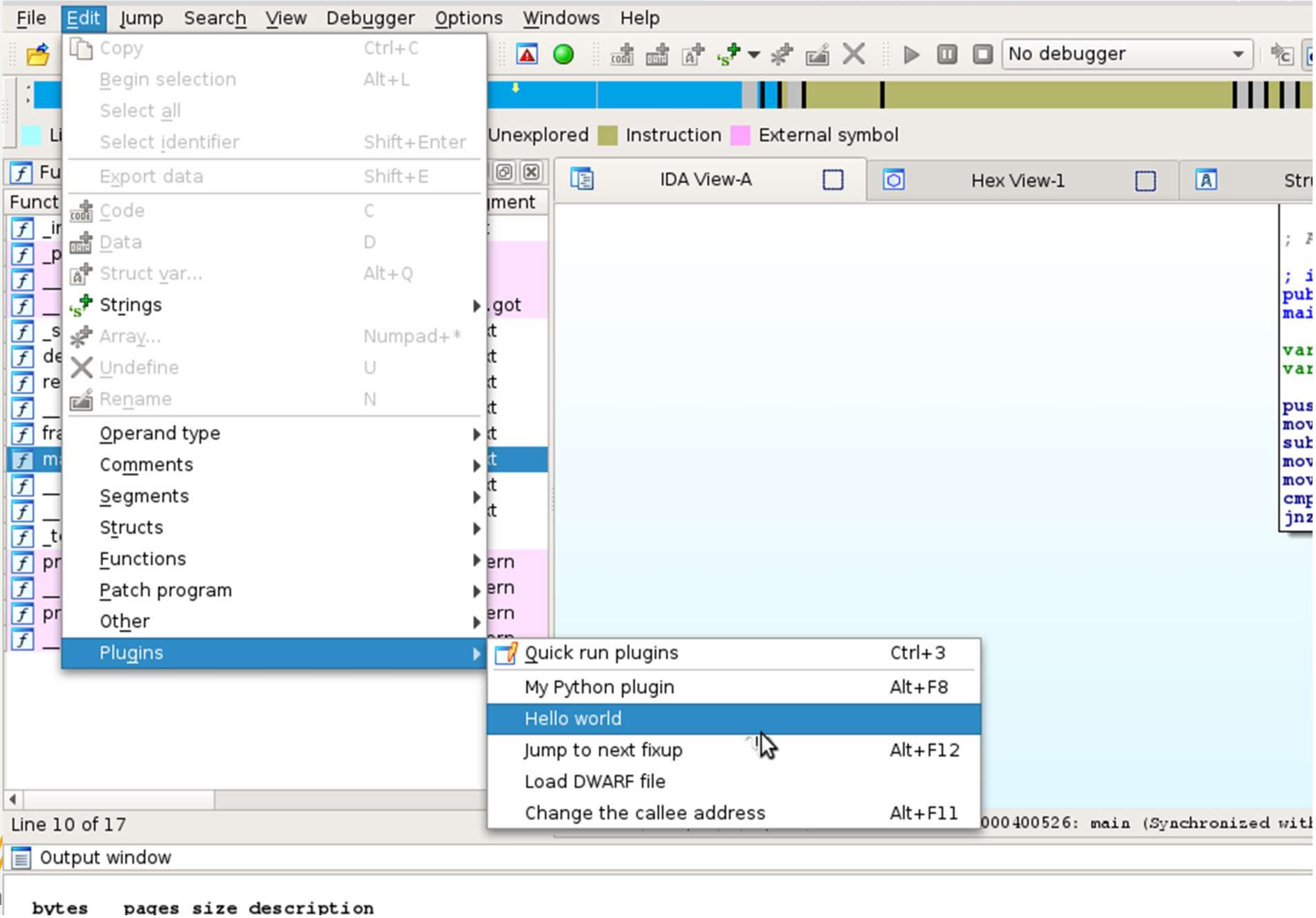
```
AU:  idle   Down      Disk: 120GB
```

This should show your plugins.list

CREATING THE NEXT®

RUN YOUR PLUGIN

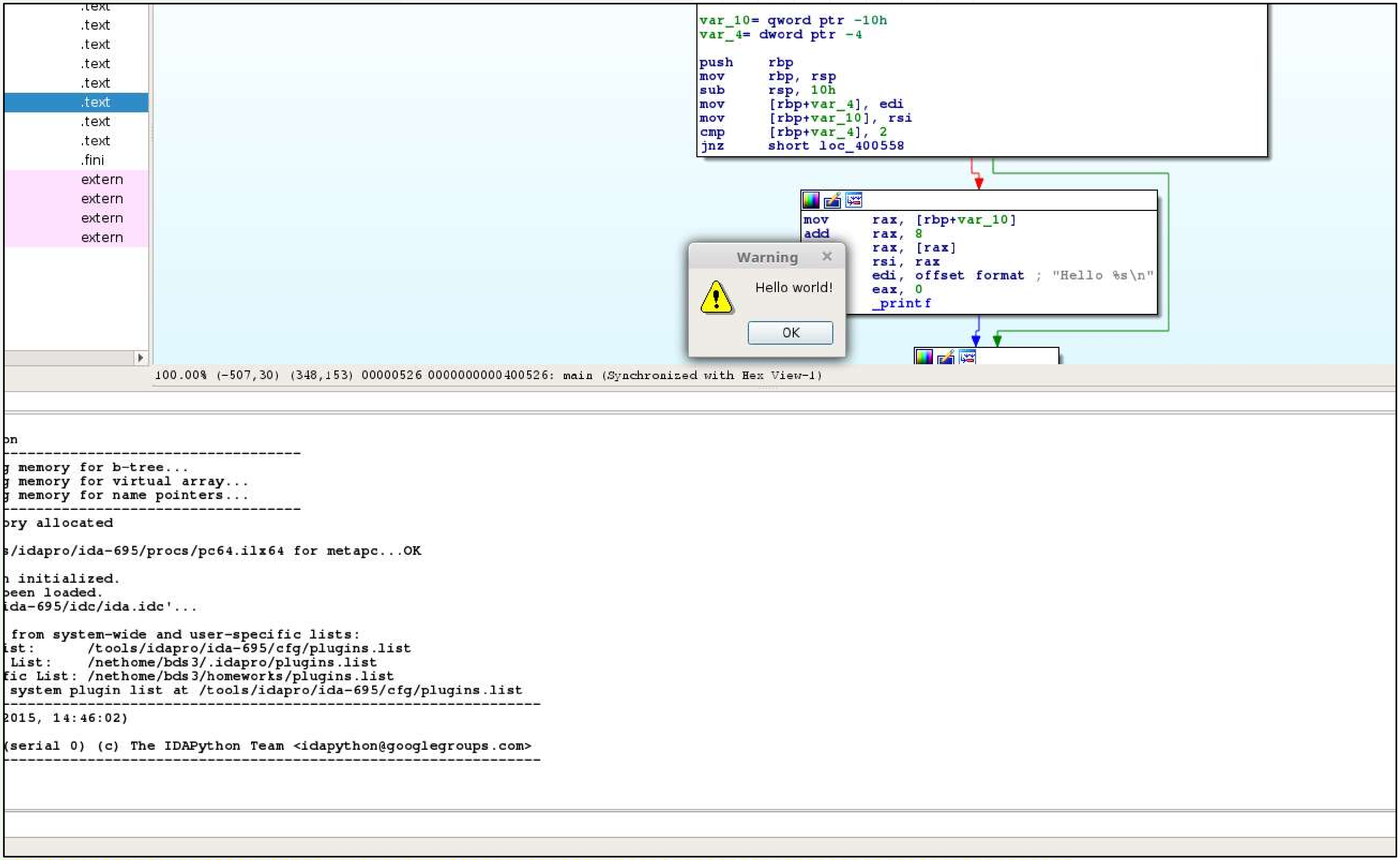
- Most plugins are listed in the Edit->Plugins menu
- Plugins can also be designed to run automatically or be linked to keyboard shortcuts



```
000400526: main (Synchronized with
```

```
bytes   pages size description
```

HELLO WORLD!



```
.text
.text
.text
.text
.text
.text
.text
.text
.fini
extern
extern
extern
extern
```

```
var_10= qword ptr -10h
var_4= dword ptr -4

push    rbp
mov     rbp, rsp
sub     rsp, 10h
mov     [rbp+var_4], edi
mov     [rbp+var_10], rsi
cmp     [rbp+var_4], 2
jnz     short loc_400558
```

```
mov     rax, [rbp+var_10]
add     rax, 8
        rax, [rax]
        rsi, rax
        edi, offset format ; "Hello %s\n"
        eax, 0
        _printf
```

Hello world!

```
100.00% (-507,30) (348,153) 00000526 0000000000400526: main (Synchronized with Hex View-1)
```

```
on
-----------------------------------
g memory for b-tree...
g memory for virtual array...
g memory for name pointers...
-----------------------------------
ory allocated

s/idapro/ida-695/procs/pc64.ilx64 for metapc...OK

n initialized.
been loaded.
ida-695/idc/ida.idc'...

 from system-wide and user-specific lists:
ist:      /tools/idapro/ida-695/cfg/plugins.list
 List:    /nethome/bds3/.idapro/plugins.list
fic List: /nethome/bds3/homeworks/plugins.list
 system plugin list at /tools/idapro/ida-695/cfg/plugins.list
----------------------------------------------------------------
2015, 14:46:02)

(serial 0) (c) The IDAPython Team <idapython@googlegroups.com>
----------------------------------------------------------------
```

CREATING THE NEXT®

ANNUAL IDA PLUGIN CONTEST!

- So you built a really great plugin?
- Hex-Rays (the company that makes IDA) runs an annual plugin contest
- https://www.hex-rays.com/contests/
- The best plugins from that year compete for huge respect among the reverse engineering community
- AND CASH PRIZES!! 🤑 💰 💸

ADDITIONAL READINGS (OPTIONAL)

- https://www.hex-rays.com/products/ida/tech/plugin.shtml
- Chris Eagle. The IDA Pro Book. No Starch Press (2nd Edition), 2011. ISBN: 978-1593272890
  - You can probably find the PDF version online!
  - The IDA Pro Book describes many aspects of plugin writing
  - Note that the API listings in the book may be outdated!
- IDA SDK Docs:
  - https://www.hex-rays.com/products/ida/support/sdkdoc/
  - https://www.hex-rays.com/products/ida/support/idapython_docs/
- RE StackExchange. For example:
  - https://reverseengineering.stackexchange.com/questions/14430/how-is-idapython-api-structured
  - https://reverseengineering.stackexchange.com/questions/1899/creating-ida-pro-debugger-plugins-api-documentation-and-examples
- The OLD Guide Book: http://www.openrce.org/reference_library/files/ida/idapw.pdf
- Google!! There are many great resources online for IDA Plugin development!

Georgia Tech

QUESTIONS?

CREATING THE NEXT®