

# WELCOME TO IDA PRO

PROF. BRENDAN SALTAFORMAGGIO

SCHOOL OF ECE

CREATING THE NEXT®

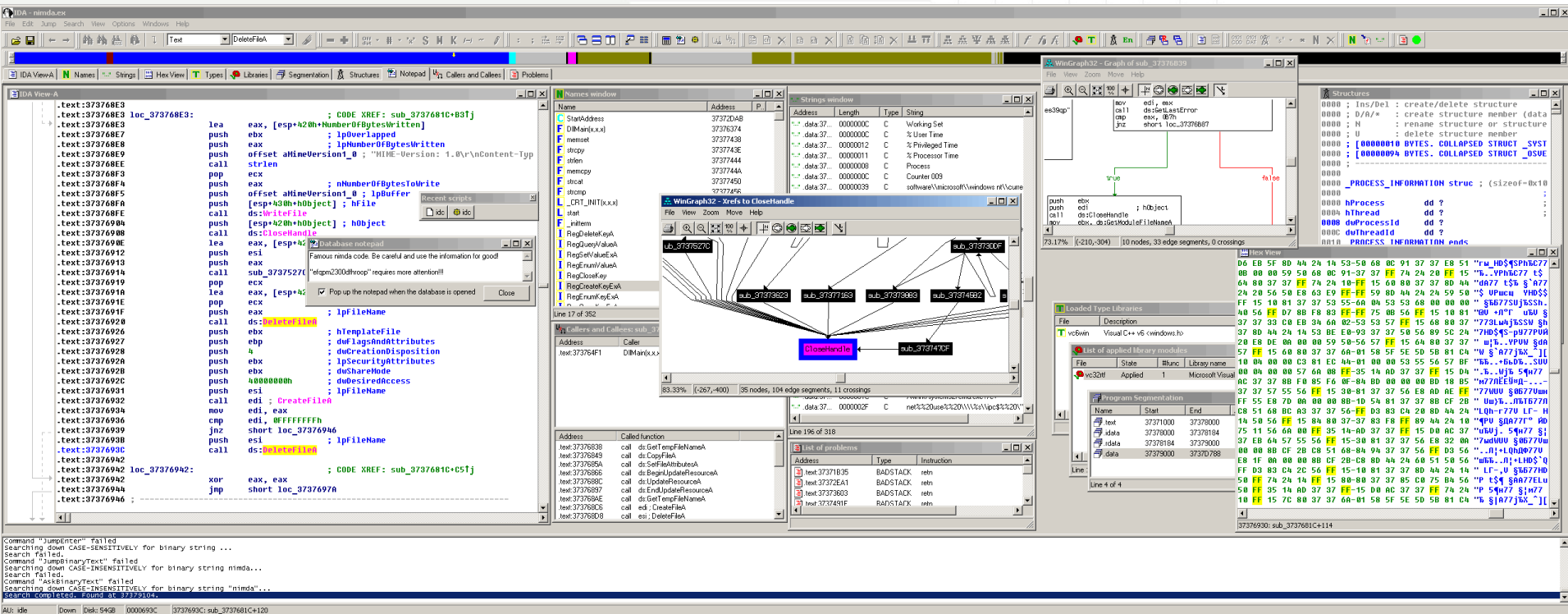


PLEASE CONSIDER THE  
ENVIRONMENT, AVOID  
PRINTING SLIDES!

# WHAT IS IDA PRO?



- IDA Pro combines an interactive, programmable, multi-processor disassembler coupled to a local and remote debugger augmented by a complete plugin environment
- IDA Pro is the industry standard for hostile code analysis, vulnerability research, software validation, interactive debugging, and much more



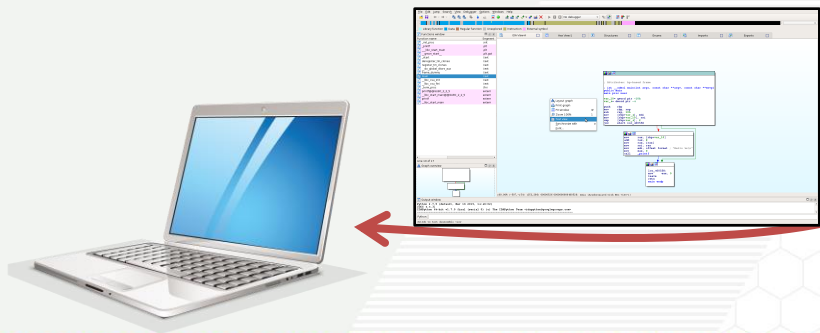
THANK YOU TO THE SCHOOL OF ECE!!



- IDA Pro enables multi-processor disassembly and debugging across more than 50 processor families
- IDA Pro provides a unique advantage to software security research and education
- Simply having IDA Pro experience makes you a top candidate for many careers
  - Malware analyst, low-level software developer, security researcher, ...
- The School of ECE saw the exciting potential of providing students access to IDA Pro
- IDA Pro is not cheap --- A single floating license costs over \$2800 USD!
- The School of ECE has graciously purchased 30 floating licenses for this course!
- We are among a small group of universities which have this educational benefit

# HOW TO ACCESS IDA PRO

- IDA Pro is installed in the School of ECE's cloud servers
- Four very powerful Red Hat Linux 7 machines
  - `ece-linlabsrv01.ece.gatech.edu`
  - 100+ GB memory and 24 cores each!
- IDA Pro runs on those machines, we can connect to the GUI in 2 ways:
  - 1) Standard SSH with X11 forwarding
    - Best on fast internet connections (e.g., on campus)
  - 2) FastX Client
    - Best on slow internet connections



`ece-linlabsrv01.ece.gatech.edu`

- FastX is a custom X server & client implementation
  - It is optimized to be more efficient over slow internet connections
  - Standard SSH with X forwarding is terrible over slow connections
- Georgia Tech OIT provides FastX Client for Windows, Linux, and Mac
  - Available at: <http://software.oit.gatech.edu>
- The IDA Pro Servers are running the custom FastX server
- The FastX Client handles connecting to the IDA Pro Servers and displaying the X11 GUI
- Supported by Georgia Tech OIT 😊

## DO NOT FORGET TO VPN!



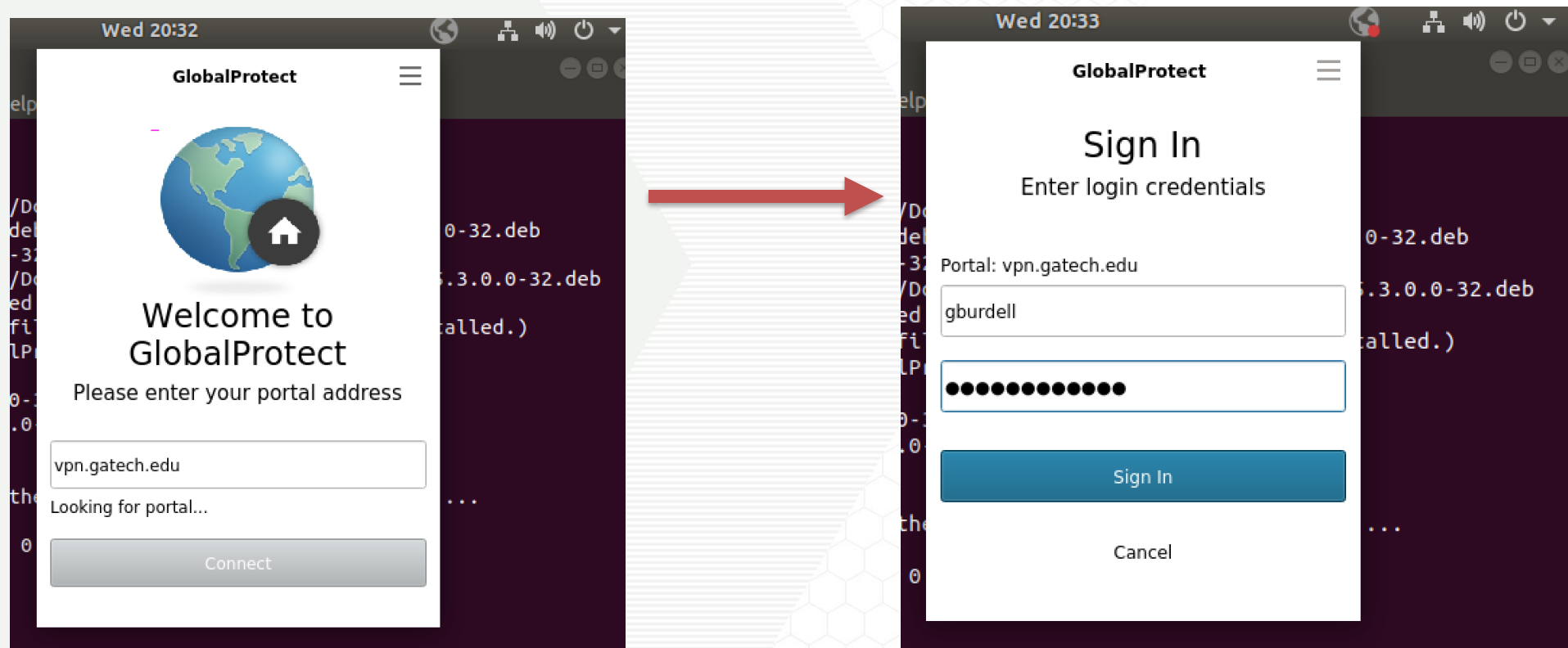
- We can only access these machines through the Georgia Tech VPN!
  - Even on eduroam you need the VPN
  - Only the on-campus ECE computer labs can access them without the VPN
- Georgia Tech OIT provides & supports VPN clients for Linux, Windows, Mac, ...
- [https://gatech.service-now.com/home?id=kb\\_article\\_view&sysparm\\_article=KB0026837](https://gatech.service-now.com/home?id=kb_article_view&sysparm_article=KB0026837)



# HOW TO CONNECT TO IDA PRO SERVERS FROM LINUX

CREATING THE NEXT®

[https://gatech.service-now.com/home?id=kb\\_article\\_view&sysparm\\_article=KB0028027](https://gatech.service-now.com/home?id=kb_article_view&sysparm_article=KB0028027)





## AFTER VPN, STANDARD SSH WITH X11 FORWARDING



- Be sure to set X11 forwarding on, compression on, and cipher preferences for fast ciphers

A screenshot of a terminal window titled "Terminal - brendan@brendan-laptop: ~". The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal content shows a user at the prompt "brendan@brendan-laptop:~\$ " typing the command "ssh -XC bds3@ece-linlabsrv01.ece.gatech.edu". Below the command, there are two bullet points: "• ece-linlabsrv01.ece.gatech.edu" and "• 100+ GB memory and 24 cores each!". Further down, there is a line of text: "IDA Pro runs on those machines, we can connect to the GUI in". Below this, there is a numbered list: "1) Standard SSH with X11 forwarding" followed by a checkbox and the text "Best on fast internet connections (e.g., on campus)", and "2) FastX Client".

```
Terminal - brendan@brendan-laptop: ~
File Edit View Terminal Tabs Help
brendan@brendan-laptop:~$ ssh -XC bds3@ece-linlabsrv01.ece.gatech.edu
• ece-linlabsrv01.ece.gatech.edu
• 100+ GB memory and 24 cores each!

IDA Pro runs on those machines, we can connect to the GUI in
1) Standard SSH with X11 forwarding
   [ ] Best on fast internet connections (e.g., on campus)
2) FastX Client
```

# ENTER PASSWORD AND YOU'RE CONNECTED!



- Now you have a terminal with X11 forwarding from ece-linlabsrv01.ece.gatech.edu

```
Terminal - brendan@brendan-laptop: ~
File Edit View Terminal Tabs Help
brendan@brendan-laptop:~$ ssh -XC bds3@ece-linlabsrv01.ece.gatech.edu
*****
This computer system is the property of the Georgia Institute of Technology.
Any user of this system must comply with all Institute and Board of Regents
policies, including the Acceptable Use Policy, Cyber Security Policy and
Data Privacy Policy (http://b.gatech.edu/it-policies). Users should have no
expectation of privacy, as any and all files on this system may be
intercepted, monitored, recorded, copied, inspected, and/or disclosed to
authorized personnel in order to meet Institute obligations.
By using this system, I acknowledge and consent to these terms.
*****
bds3@ece-linlabsrv01.ece.gatech.edu's password: 
```

```
Terminal - brendan@brendan-laptop: ~
File Edit View Terminal Tabs Help
login session at the discretion of the CSG. bFlagrantaggio
or repeated violations may in extreme cases bds3@ece.gatech...
subject to suspension or revocation of account
privileges. Jobs running for longer than 5 days on
the ecelinsrv systems will be automatically
terminated at the discretion of the CSG. If you need
to run substantially long jobs, email help@ece
requesting a PACE account.

If you are having problems running applications, see
http://www.ece-help.gatech.edu/unix/cshrc.html for
information on configuring your login environment.

bds3@ece-linlabsrv01.ece.gatech.edu>
bds3@ece-linlabsrv01.ece.gatech.edu>
bds3@ece-linlabsrv01.ece.gatech.edu>
bds3@ece-linlabsrv01.ece.gatech.edu>
bds3@ece-linlabsrv01.ece.gatech.edu>
```

## ANOTHER LINUX OPTION: LINUX FASTX CLIENT



- SSH with X forwarding is terrible over slow connections
- FastX is optimized for slow connections
  - Also, Georgia Tech OIT will always recommend that you use FastX

### 1. Download FastX from GT OIT

- <http://software.oit.gatech.edu>

### 2. Extract the tar.gz file

### 3. cd to the extracted FastX directory

### 4. Execute: \$ PATH=\$PATH:./ ./FastX

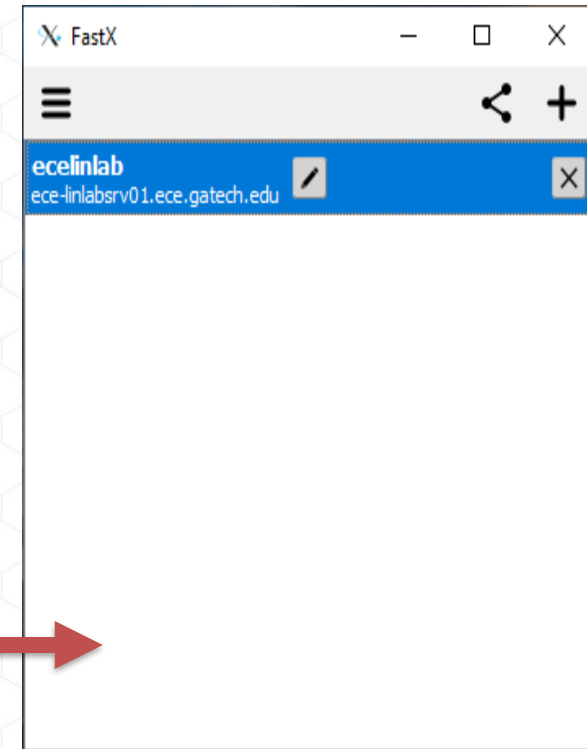
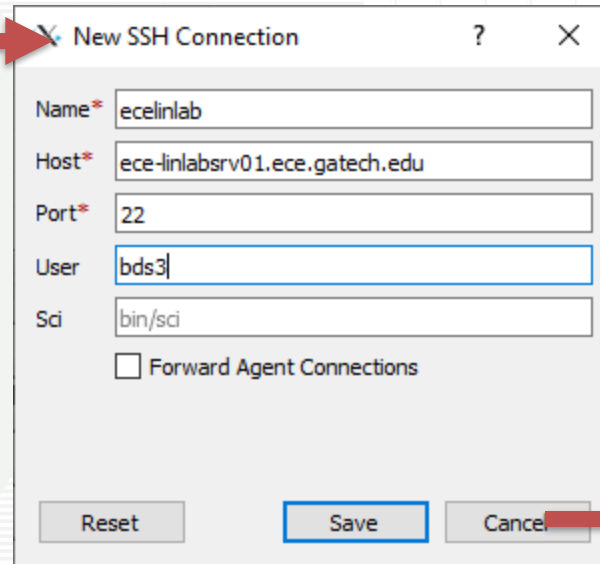
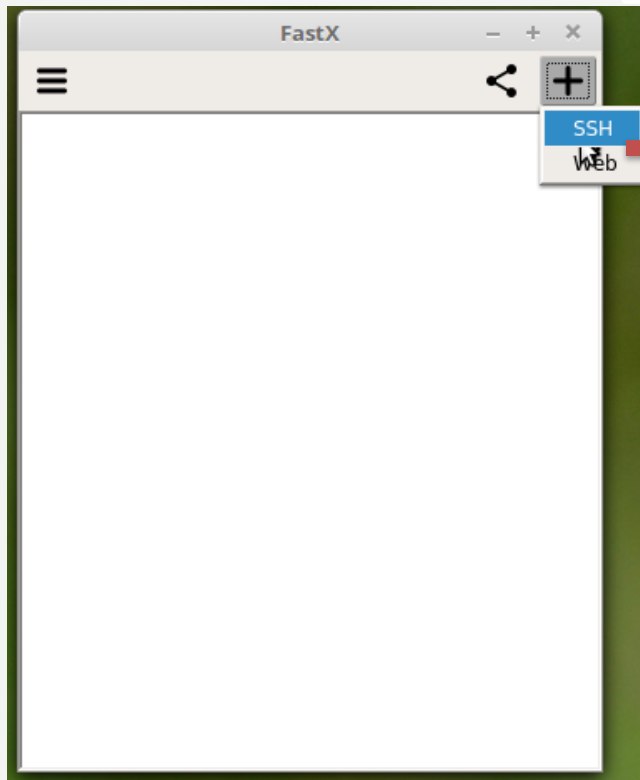
- There is a BUG in the Linux FastX client!
- It needs the FastX directory in the PATH to correctly find its dependencies!

A terminal window titled "brendan@brendan-laptop ~/Downloads/FastX" showing the following commands and output:

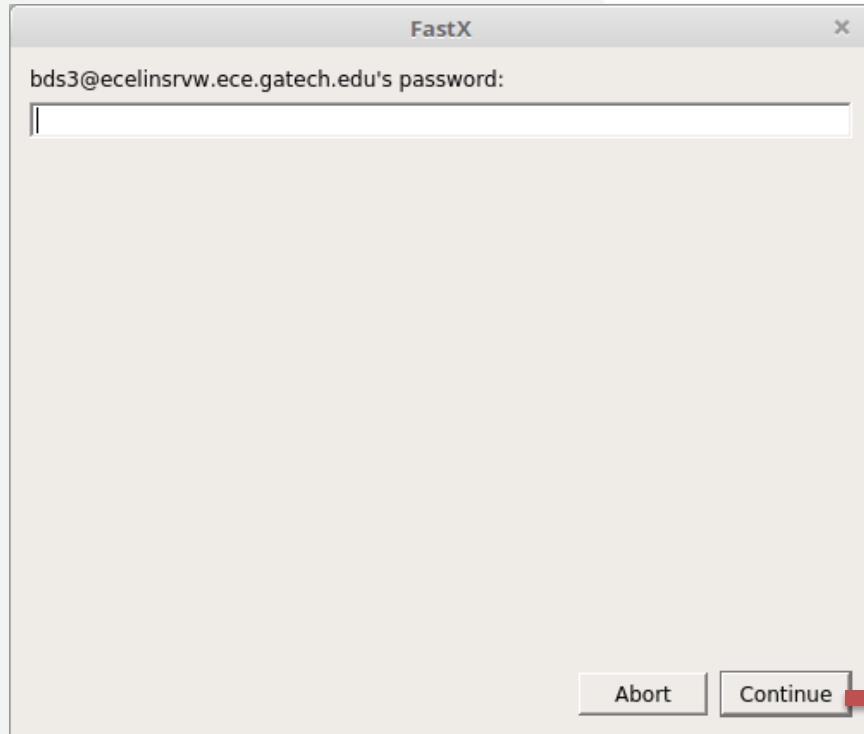
```
brendan@brendan-laptop ~/Downloads $ tar xzf FastX-2.0.82.rhel6.x86_64.tar.gz
brendan@brendan-laptop ~/Downloads $ cd FastX/
brendan@brendan-laptop ~/Downloads/FastX $ PATH=$PATH:./ ./FastX
```

The terminal output shows a message about a branch update and a long email body text starting with "On your first day of class".

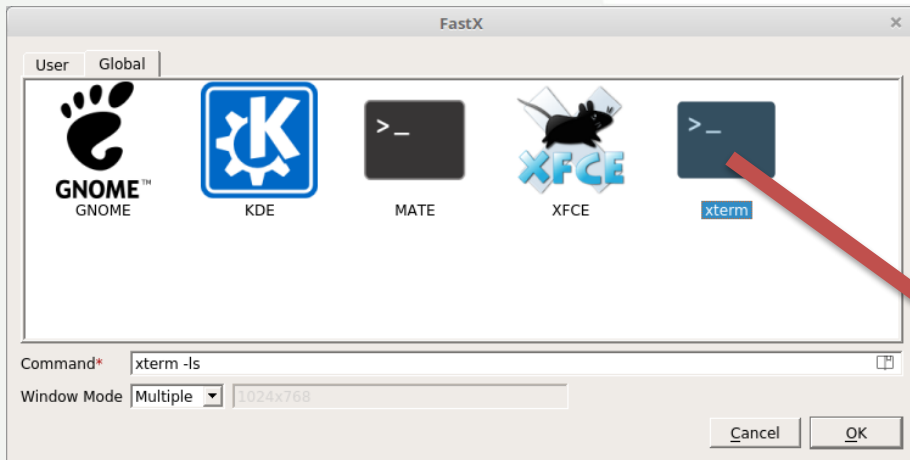
## ANOTHER LINUX OPTION: LINUX FASTX CLIENT



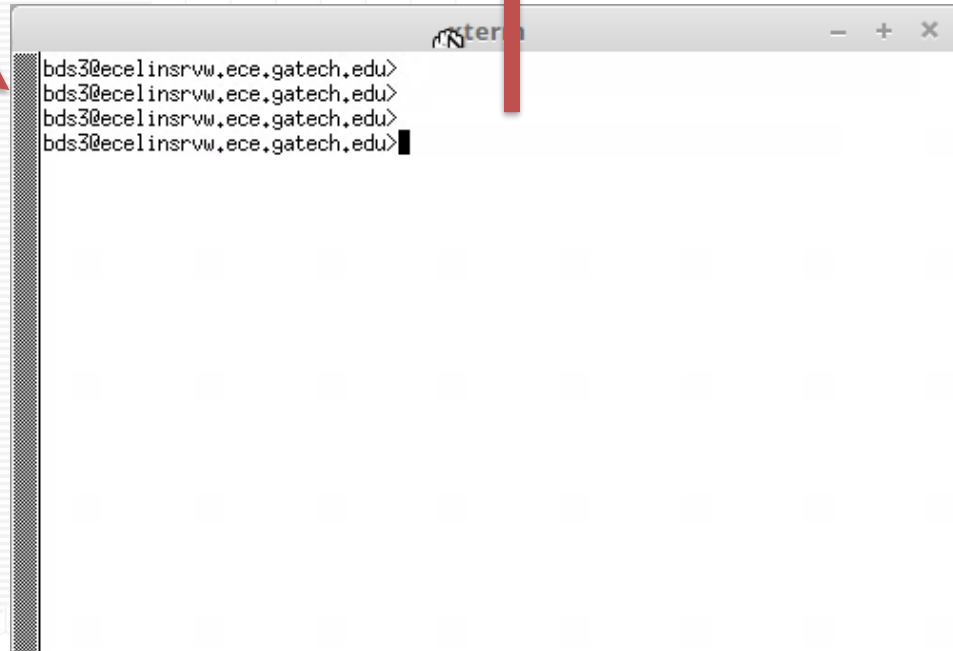
## ANOTHER LINUX OPTION: LINUX FASTX CLIENT



## ANOTHER LINUX OPTION: LINUX FASTX CLIENT



- Now you have a terminal with X11 forwarding from `ece-linlabsrv01.ece.gatech.edu`

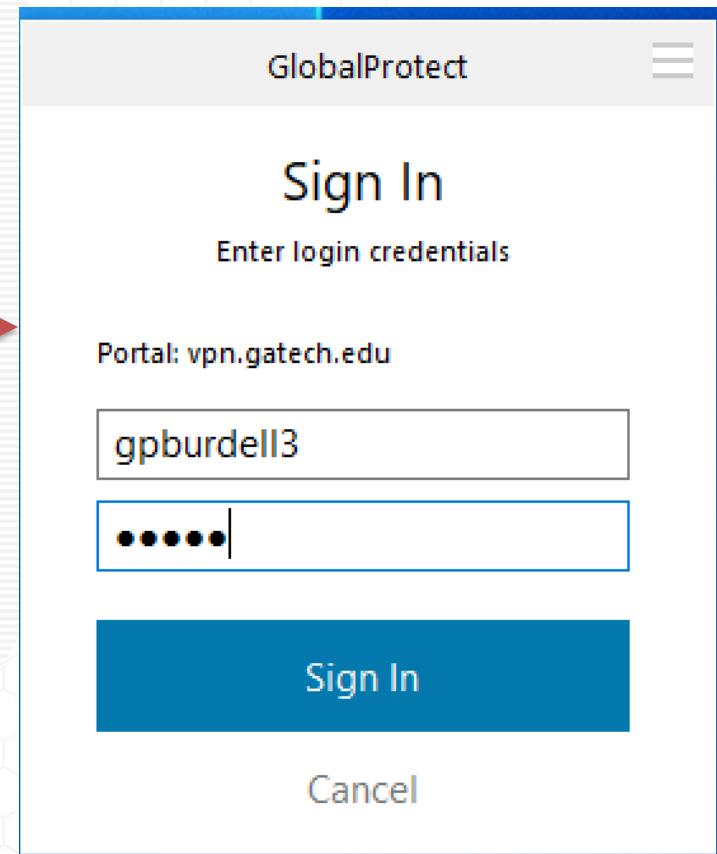
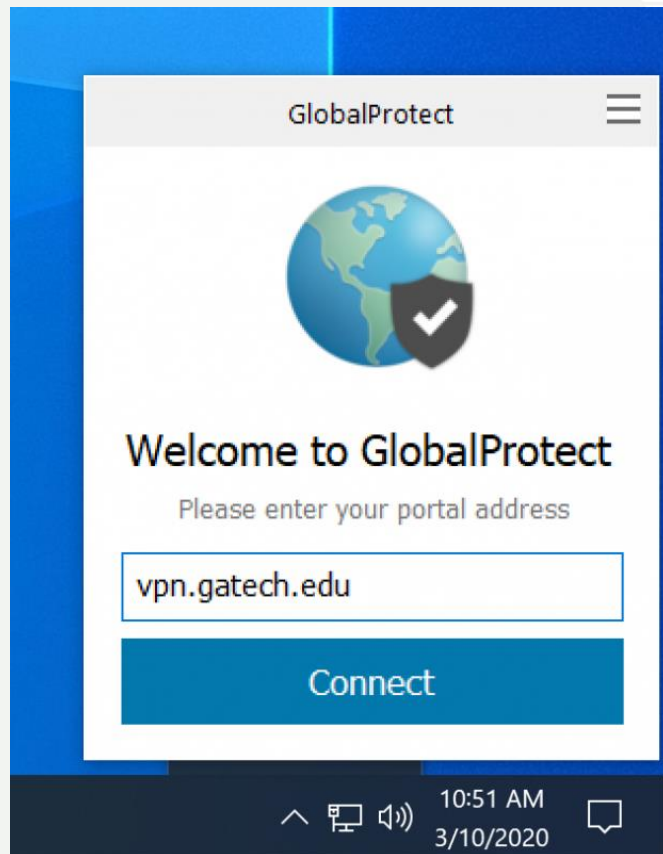




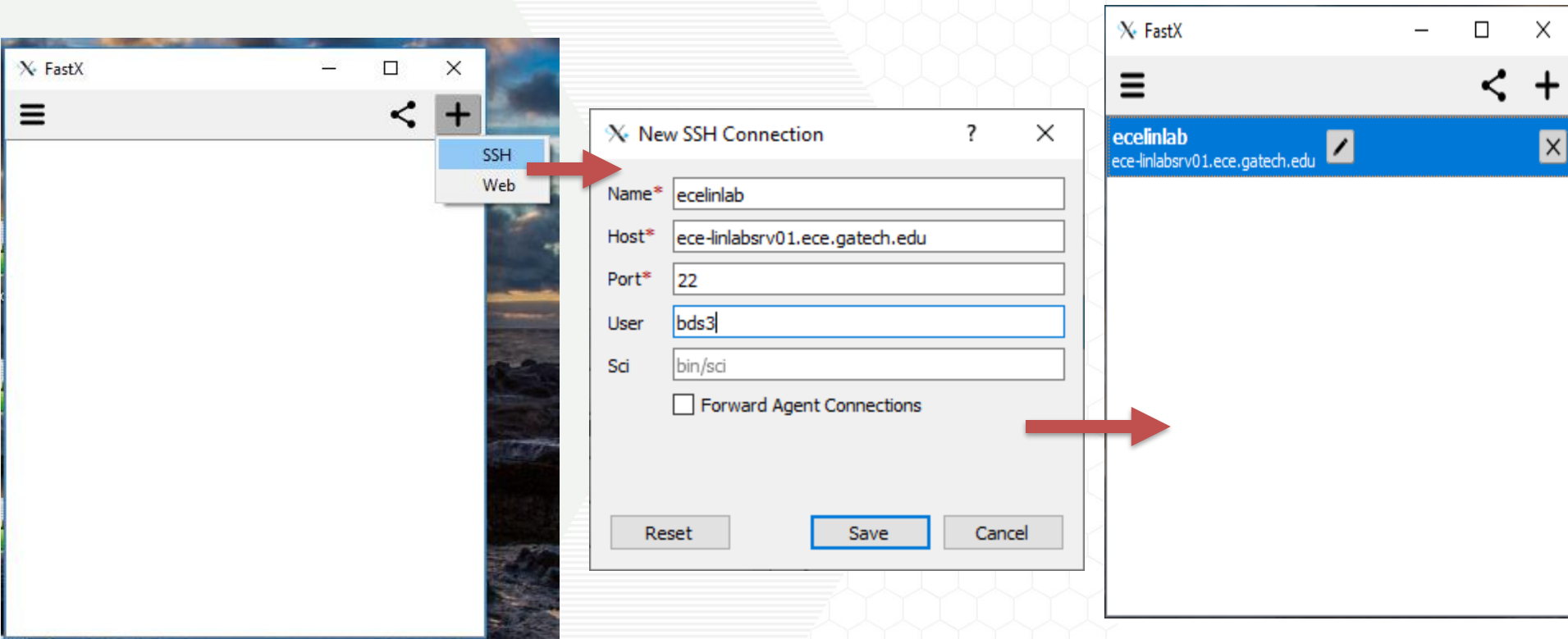
# HOW TO CONNECT TO IDA PRO SERVERS FROM WINDOWS

CREATING THE NEXT®

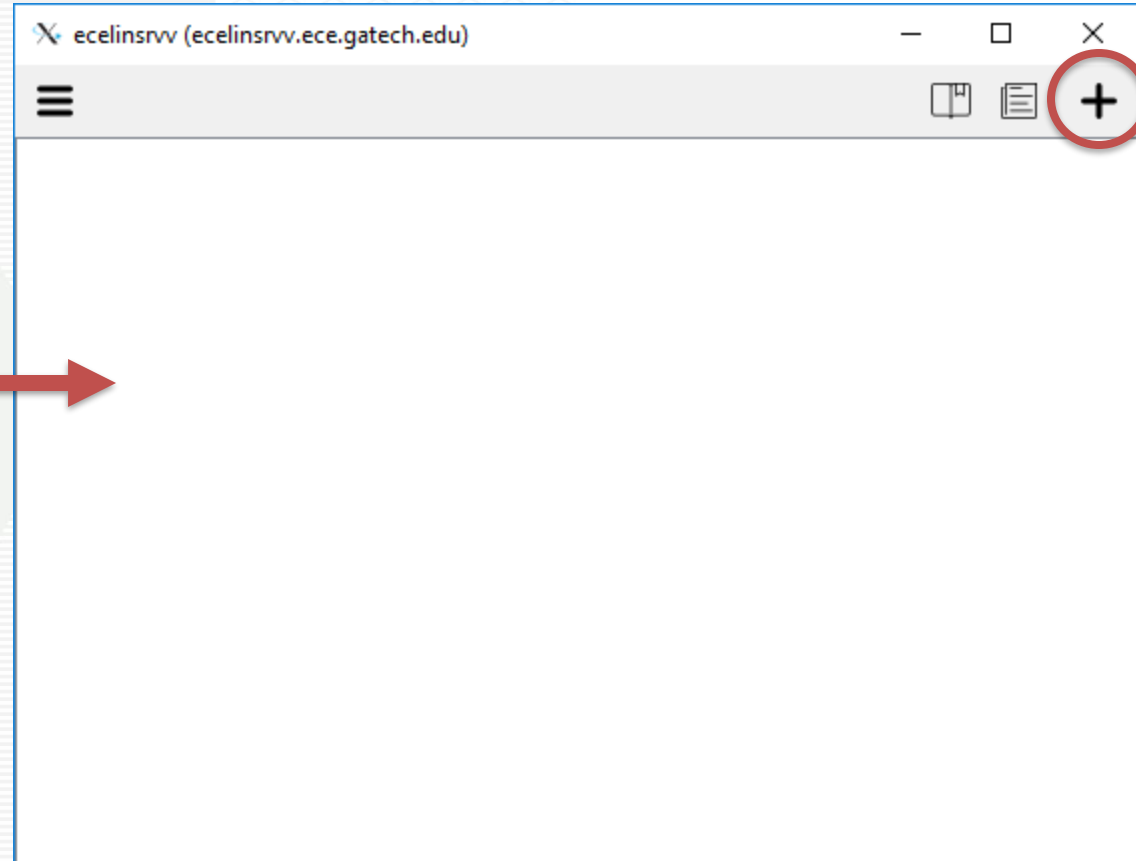
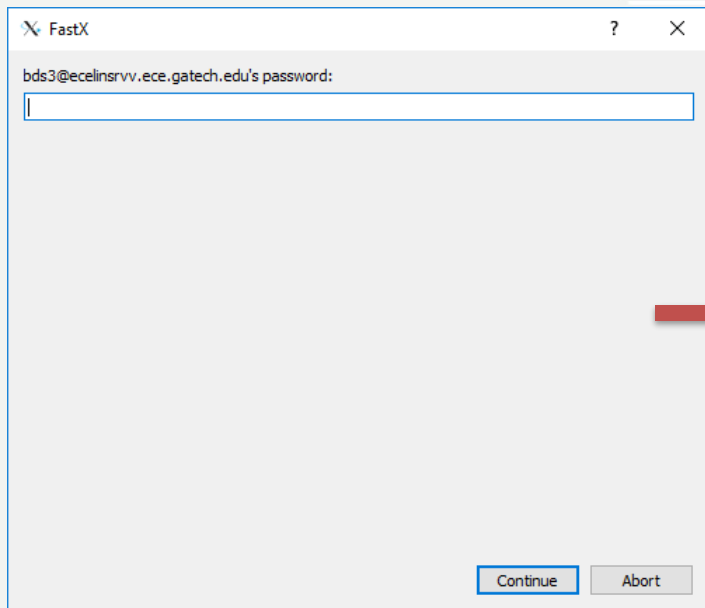
[https://gatech.service-now.com/home?id=kb\\_article\\_view&sysparm\\_article=KB0026742](https://gatech.service-now.com/home?id=kb_article_view&sysparm_article=KB0026742)



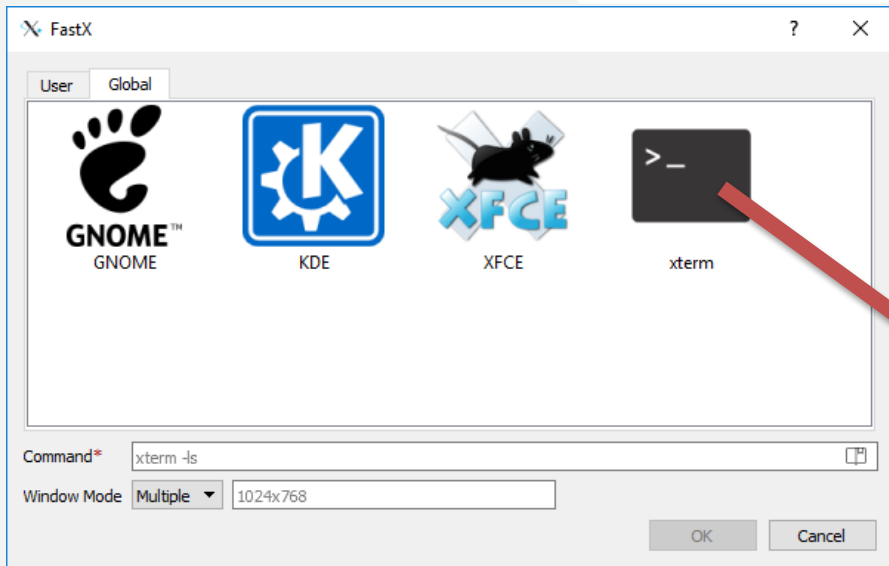
## AFTER VPN, WINDOWS FASTX CLIENT



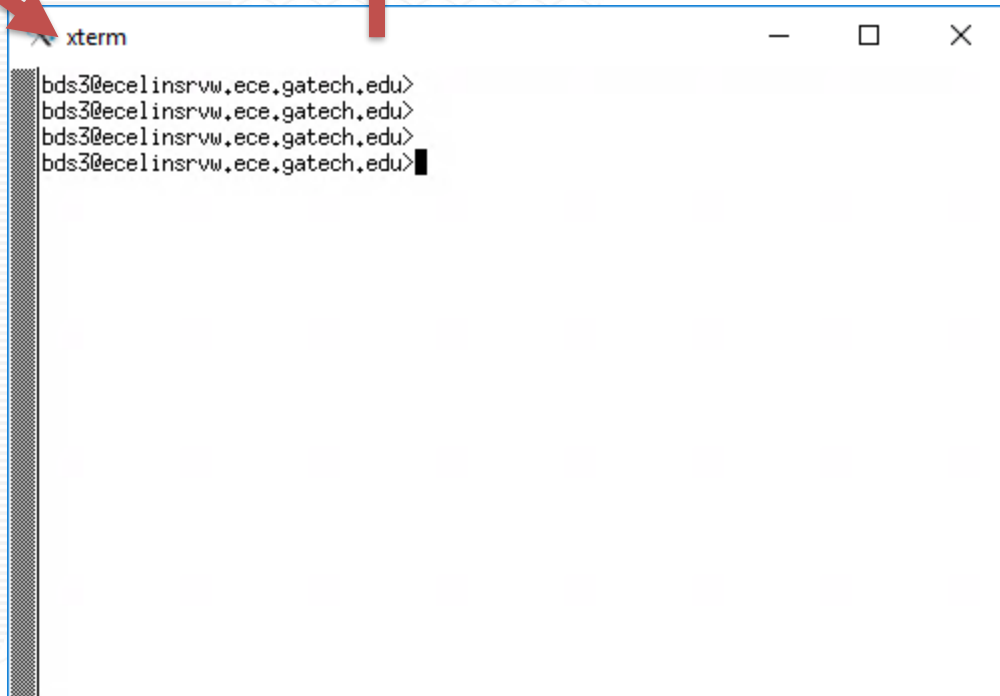
## LAUNCH APPS IN FASTX



## LAUNCH APPS IN FASTX



- Now you have a terminal with X11 forwarding from `ece-linlabrv01.ece.gatech.edu`



The background features a large, stylized 'X' shape. The left arm of the 'X' is filled with a yellow-to-orange gradient and contains a faint image of a modern building with glass windows. The right arm of the 'X' is white with a light gray hexagonal pattern. Horizontal orange diagonal lines separate the main text sections.

**ONCE YOU ARE CONNECTED  
TO THE IDA PRO SERVERS...**

**YOU ARE IN ECE TERRITORY!  
ALL PROBLEMS MUST BE SENT TO:  
[HELP@ECE.GATECH.EDU](mailto:HELP@ECE.GATECH.EDU)**

**CREATING THE NEXT®**

A series of parallel orange diagonal lines at the bottom right of the slide.



- Before you can do anything with IDA Pro, you **must** first set up the running environment
- Use the following command: `$ source /tools/software/hex-rays/idapro.csh`
- Note: You may not see the `/tools/software/hex-rays/` directory until you execute that command
  - It is our “secret” key!
- Only needs to be done once (per terminal) to set up the environment
- Everything related to IDA Pro is available in `/tools/software/hex-rays/`
  - We have read & execute permissions in that folder (after executing “`$ source ...`”)
- Feel free to look through the directories, read the docs, and check out the SDK!

## A TALE OF TWO IDAS



- IDA Pro has two different executables
  - Which executable you use depends on what binary you are analyzing
- **ida** for working with 32-bit binaries
- **ida64** for working with 64-bit binaries
- You will get an error if you use the wrong one
- I recommend executing them with “&” after to put the process in the background

## NOTICE THE TCSH!



- The default shell on the ECE machines should be `/bin/tcsh`
- THIS IS NOT BASH! But it is similar
  - <https://help.ece.gatech.edu/linux/shells>
- The “`$ source /tools/software/hex-rays/idapro.csh`” command will ONLY work in tcsh!
- You can check your current shell with “`echo $0`”
- After you run “`$ source ...`” you can switch to `/bin/bash` if you want

```
bds3@ecelinsrvw.ece.gatech.edu>
bds3@ecelinsrvw.ece.gatech.edu>
bds3@ecelinsrvw.ece.gatech.edu>echo $0
/bin/tcsh
bds3@ecelinsrvw.ece.gatech.edu>source /tools/idapro/ida-
bds3@ecelinsrvw.ece.gatech.edu>/bin/bash
[bds3@ecelinsrvw ~]$ ida &
[1] 44579
[bds3@ecelinsrvw ~]$
[1]+  Exit 1                  ida
[bds3@ecelinsrvw ~]$ ida64 &
[1] 44602
[bds3@ecelinsrvw ~]$
[1]+  Exit 1                  ida64
[bds3@ecelinsrvw ~]$
```

- Notice that IDA Pro will be executing on the remote server
- So you have to move any files/test cases/etc. to your home directory before you begin
- You also need to pull your answers/submission files back down when you're finished
- Many remote file copy utilities exist for every platform
- On Linux, use the scp command:
  - Please see this helpful cheat-sheet for a range of scp uses:  
[http://www.hypexr.org/linux\\_scp\\_help.php](http://www.hypexr.org/linux_scp_help.php)

```
brendan@brendan-laptop ~/homeworks/hello $ scp ./hello bds3@ecelinsrvw.ece.gatech.edu:~/homeworks/
*****
This computer system is the property of the Georgia Institute of Technology.
Any user of this system must comply with all Institute and Board of Regents
policies, including the Acceptable Use Policy, Cyber Security Policy and
Data Privacy Policy (http://b.gatech.edu/it-policies). Users should have no
expectation of privacy, as any and all files on this system may be
intercepted, monitored, recorded, copied, inspected, and/or disclosed to
authorized personnel in order to meet Institute obligations.

By using this system, I acknowledge and consent to these terms.
*****
bds3@ecelinsrvw.ece.gatech.edu's password:
hello
brendan@brendan-laptop ~/homeworks/hello $
```

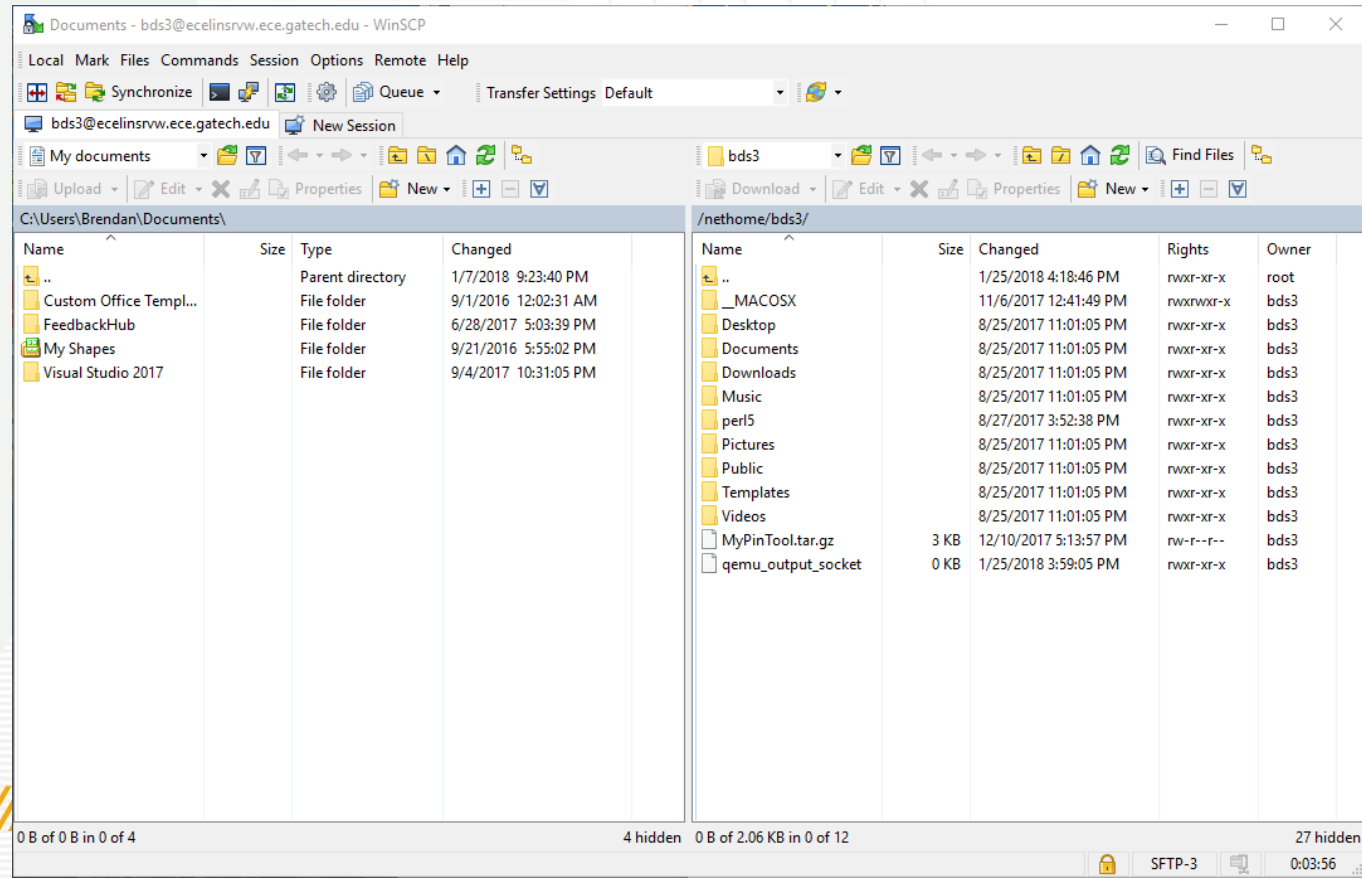
100% 8608 8.4KB/s 00:00



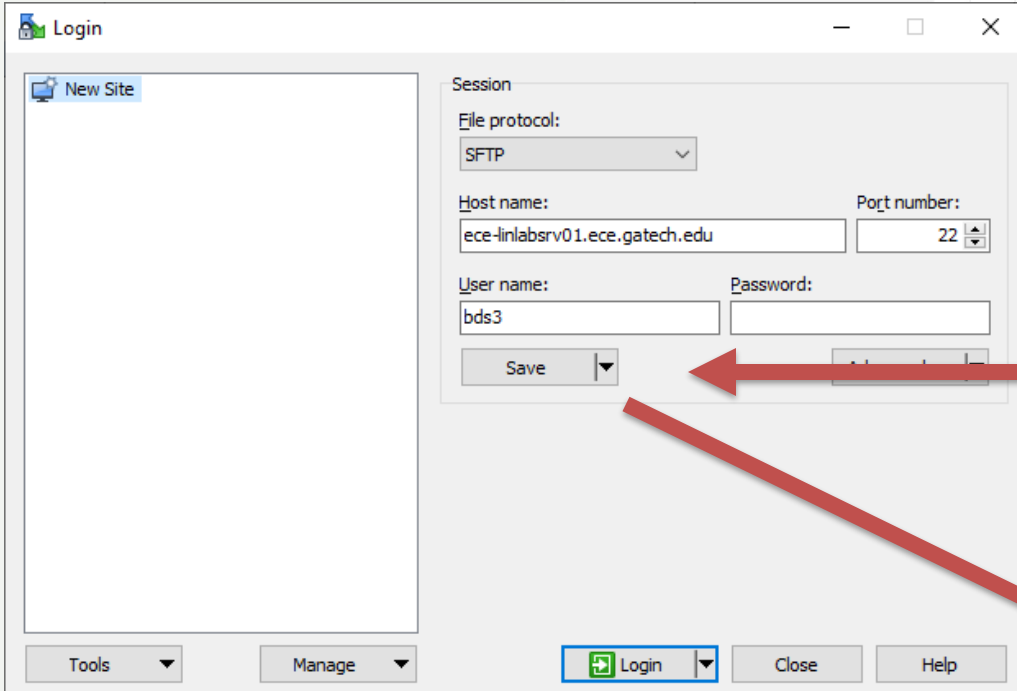
# WINSCP FOR THOSE WHO LIKE GUIs

- Another great option on Windows is WinSCP
- Download from: <https://winscp.net/eng/download.php>
- The exact same source code as SCP, just wrapped in a Windows GUI

- Simply drag and drop files between the two machines 😊

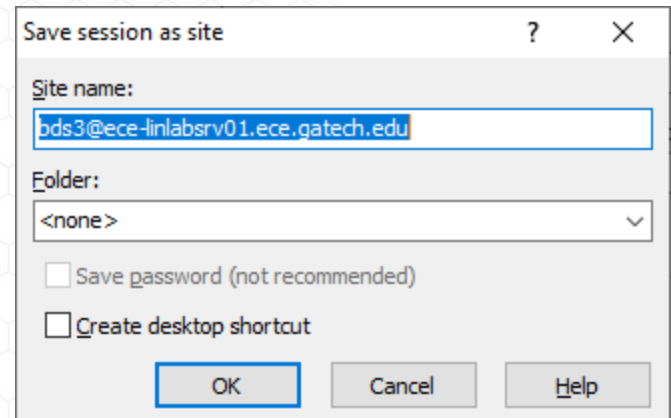


# SIGNING INTO WINSCP



The WinSCP Login dialog box is shown. It has a 'New Site' button on the left. The 'Session' section contains the following fields: 'File protocol' (SFTP), 'Host name' (ece-linlabsrv01.ece.gatech.edu), 'Port number' (22), 'User name' (bds3), and 'Password' (empty). There is a 'Save' button with a dropdown arrow. At the bottom, there are 'Tools', 'Manage', 'Login' (with a green icon), 'Close', and 'Help' buttons. Two red arrows point from the 'Save' button to the 'Save session as site' dialog box.

- Protocol = SFTP
- Fill in the host name and username fields
- Port = 22
- Remember to save!
- Give the session a nice name



The 'Save session as site' dialog box is shown. It has a 'Site name' field containing 'bds3@ece-linlabsrv01.ece.gatech.edu'. Below it is a 'Folder' dropdown menu set to '<none>'. There are two checkboxes: 'Save password (not recommended)' and 'Create desktop shortcut', both of which are unchecked. At the bottom are 'OK', 'Cancel', and 'Help' buttons.



# ENTER PASSWORD & YOU'RE ALL SET!



Password - bds3@ecelinsrvw.ece.gatech.edu



Searching for host...

Connecting to host...

Authenticating...

Using username "bds3"

Password:

OK

- Now simply drag and drop files between the hosts

Documents - bds3@ecelinsrvw.ece.gatech.edu - WinSCP

Local Mark Files Commands Session Options Remote Help

Synchronize Queue Transfer Settings Default

bds3@ecelinsrvw.ece.gatech.edu New Session

My documents Upload Edit Properties New

C:\Users\Brendan\Documents

Name	Size	Type	Changed
..		Parent directory	1/7/2018 9:23:40 PM
Custom Office Templ...		File folder	9/1/2016 12:02:31 AM
FeedbackHub		File folder	6/28/2017 5:03:39 PM
My Shapes		File folder	9/21/2016 5:55:02 PM
Visual Studio 2017		File folder	9/4/2017 10:31:05 PM

0 B of 0 B in 0 of 4

4 hidden

/nethome/bds3/

Name	Size	Changed	Rights	Owner
..		1/25/2018 4:18:46 PM	rw-r--r--	root
__MACOSX		11/6/2017 12:41:49 PM	rw-rw-r--	bds3
Desktop		8/25/2017 11:01:05 PM	rw-r--r--	bds3
Documents		8/25/2017 11:01:05 PM	rw-r--r--	bds3
Downloads		8/25/2017 11:01:05 PM	rw-r--r--	bds3
Music		8/25/2017 11:01:05 PM	rw-r--r--	bds3
perl5		8/27/2017 3:52:38 PM	rw-r--r--	bds3
Pictures		8/25/2017 11:01:05 PM	rw-r--r--	bds3
Public		8/25/2017 11:01:05 PM	rw-r--r--	bds3
Templates		8/25/2017 11:01:05 PM	rw-r--r--	bds3
Videos		8/25/2017 11:01:05 PM	rw-r--r--	bds3
MyPinTool.tar.gz	3 KB	12/10/2017 5:13:57 PM	rw-r--r--	bds3
qemu_output_socket	0 KB	1/25/2018 3:59:05 PM	rw-r--r--	bds3

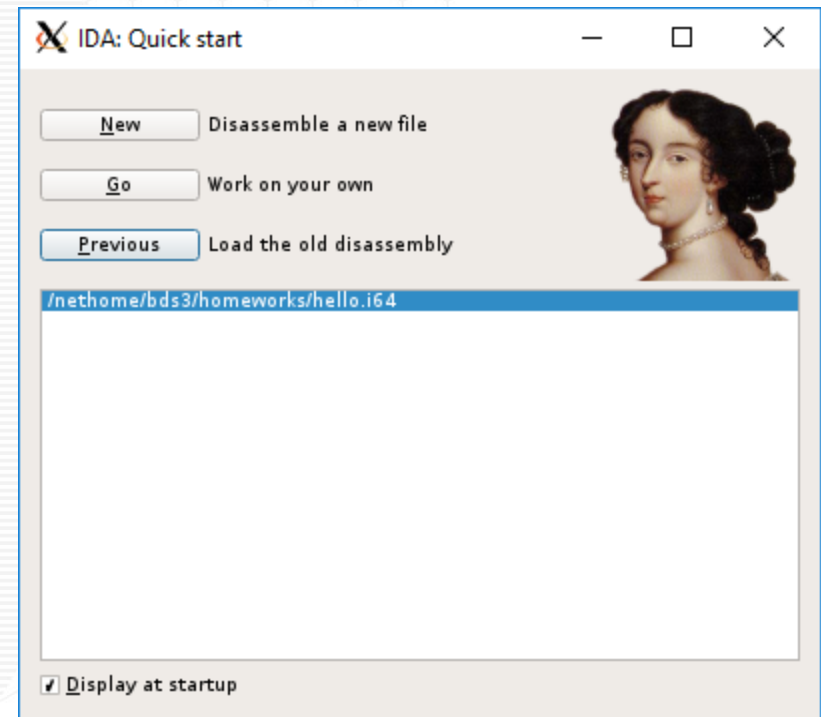
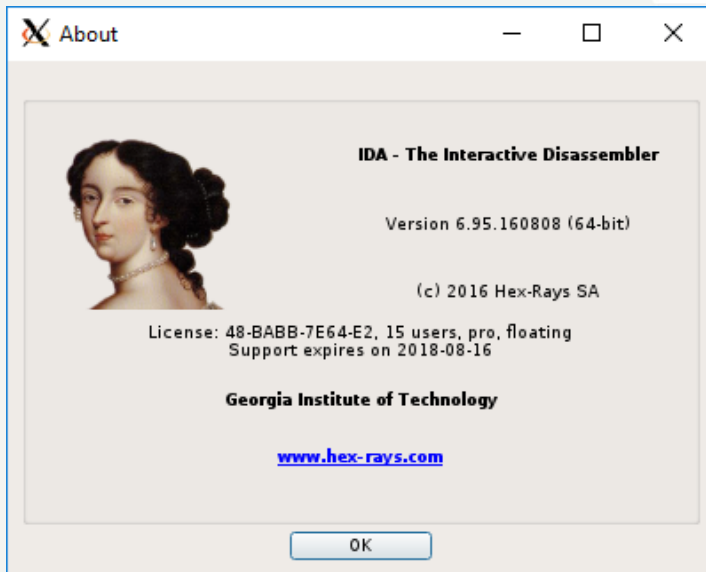
0 B of 2.06 KB in 0 of 12

27 hidden

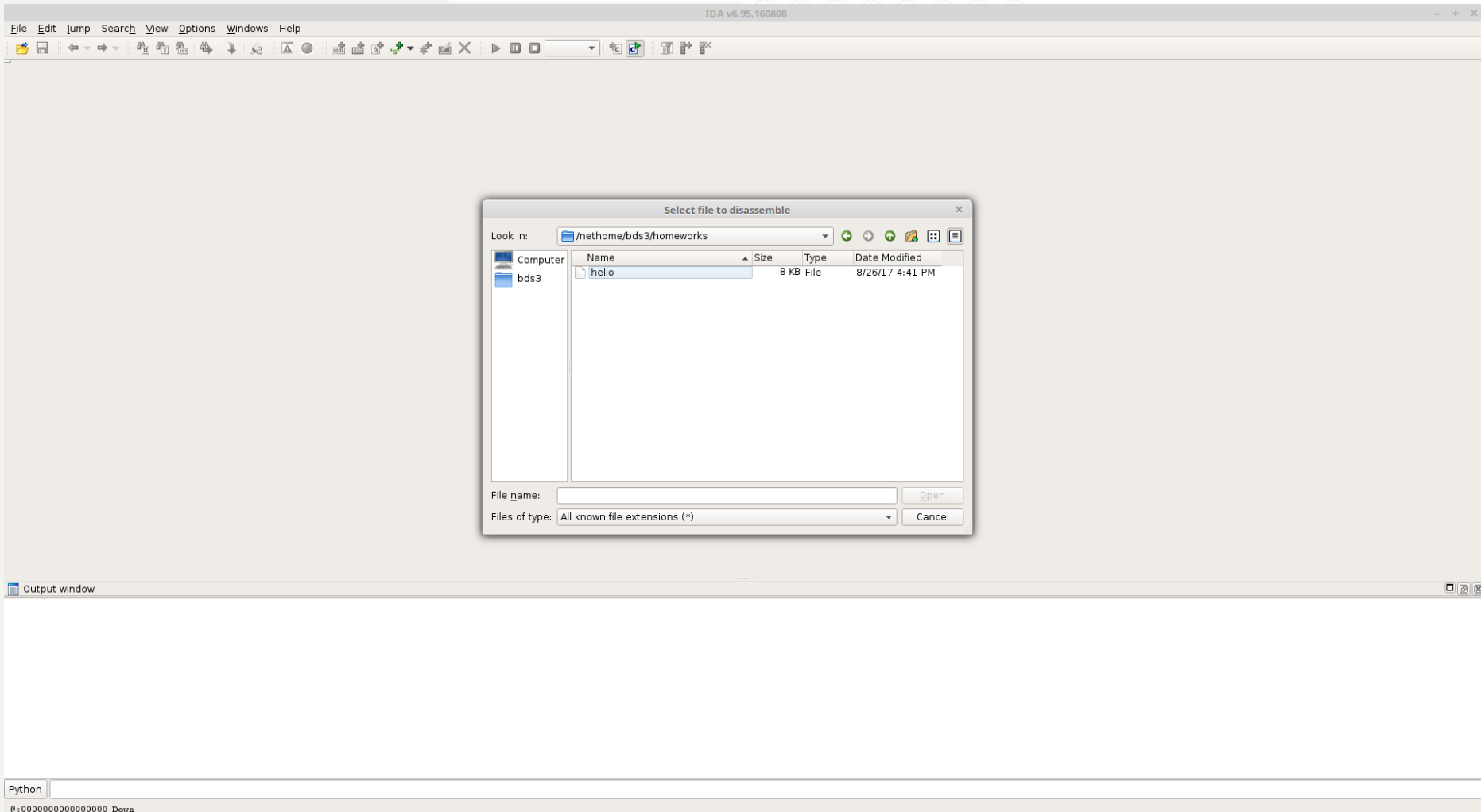
SFTP-3 0:03:56

## SELECT YOUR ANALYSIS TARGET!

- When IDA Pro starts it will ask you to start a new disassembly or open a previous one



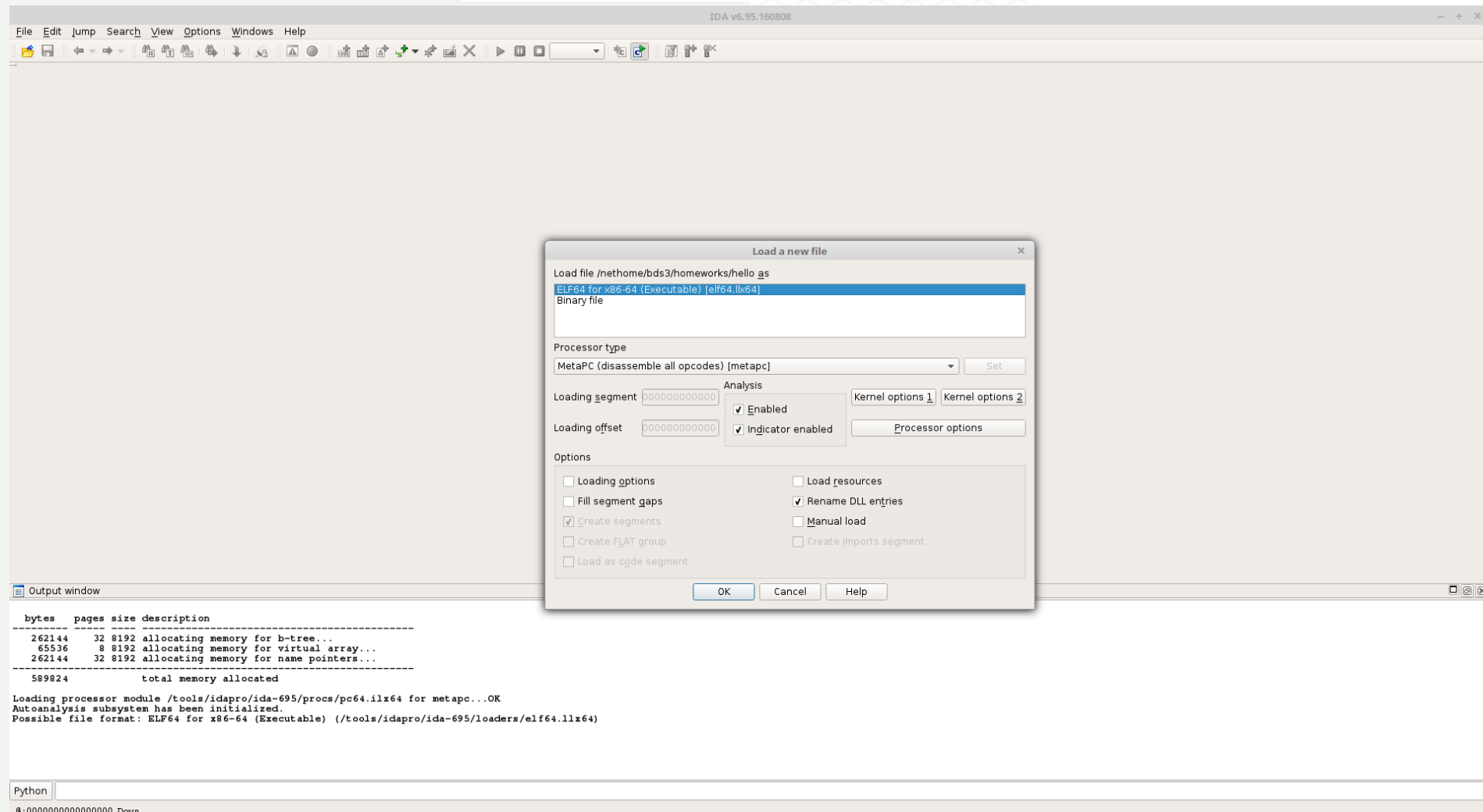
# LOADING A NEW FILE



# IDA WILL THEN ASK FOR LOADING INSTRUCTIONS



- The defaults are almost always correct ... unless you are dealing with nasty malware!



# IDA WILL OPEN IN CONTROL FLOW GRAPH VIEW

- Right-click and select Text View to view the flat disassembled code

File Edit Jump Search View Debugger Options Windows Help

Library function Data Regular function Unexplored Instruction External symbol

Functions window

Function name	Segment
_init_proc	.init
_printf	.plt
__libc_start_main	.plt
__gmon_start__	.plt.got
_start	.text
deregister_tm_clones	.text
register_tm_clones	.text
_do_global_dtors_aux	.text
frame_dummy	.text
main	.text
__libc_csu_init	.text
__libc_csu_fini	.text
__term_proc	.fini
printf@GLIBC_2.2.5	extern
__libc_start_main@@GLIBC_2.2.5	extern
__printf	extern
__libc_start_main	extern

Layout graph  
Print graph  
Fit window  
Zoom 100%  
Text view  
Synchronize with  
Font...

```
; Attributes: bp-based frame
; int __cdecl main(int argc, const char **argv, const char **envp)
public main
main proc near
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
mov     rax, [rax]
mov     rsi, rax
mov     edi, offset format ; "Hello %s\n"
mov     eax, 0
call    _printf

loc_400558:
mov     eax, 0
leave
retn
main endp
```

Line 10 of 17

Graph overview

Output window

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>

Python

Switch to text disassembly view

# COMMENTS: RIGHT-CLICK -> ENTER COMMENTS (OR PRESS ":")



File Edit Jump Search View Debugger Options Windows Help

Library function Data Regular function Unexplored Instruction External symbol

Functions window

Function name Segment

- \_\_init\_proc .init
- \_printf .plt
- \_\_libc\_start\_main .plt
- \_gmon\_start\_ .plt.got
- \_start .text
- deregister\_tm\_clones .text
- register\_tm\_clones .text
- \_do\_global\_ctors\_aux .text
- frame\_dummy .text
- main .text
- \_\_libc\_csu\_init .text
- \_\_libc\_csu\_fini .text
- \_term\_proc .fini
- printf@@GLIBC\_2.2.5 extern
- \_\_libc\_start\_main@@GLIBC\_2.2.5 extern
- printf extern
- \_\_libc\_start\_main extern

IDA View-A

```
.text:0000000000400510 mov     eax, 0
.text:0000000000400515 test    rax, rax
.text:0000000000400519 jz      short loc_40050B
.text:000000000040051A push    rbp
.text:000000000040051B mov     rbp, rsp
.text:000000000040051E call    rax
.text:0000000000400520 pop     rbp
.text:0000000000400521 jmp     register_tm_clones
.text:0000000000400521 endp
.frame_dummy
.text:0000000000400521
.text:0000000000400526 ; ===== SUBROUTINE =====
.text:0000000000400526 ;
.text:0000000000400526 ; Attributes: bp-based frame
.text:0000000000400526 ;
.text:0000000000400526 ; int __cdecl main(int argc, const char **argv, const char **envp)
.text:0000000000400526 public main
.text:0000000000400526 main proc near ; DATA XREF: __start+1D10
.text:0000000000400526
.text:0000000000400526     = qword ptr -10h
.text:0000000000400526     = dword ptr -4
.text:0000000000400526
.text:0000000000400526 push    rbp
.text:0000000000400527 mov     rbp, rsp
.text:0000000000400527 sub     rsp, 10h
.text:000000000040052A mov     [rbp+var_4], edi
.text:0000000000400531 mov     [rbp+var_10], rsi
.text:0000000000400532 cmp     [rbp+var_4], 2
.text:0000000000400535 jnz     short loc_400558
.text:0000000000400539 mov     rax, [rbp+var_10]
.text:000000000040053B add     rax, 8
.text:0000000000400543 mov     rax, [rax]
.text:0000000000400546 mov     rsi, rax
.text:0000000000400549 mov     edi, offset format
.text:000000000040054B mov     eax, 0
.text:0000000000400553 call    _printf
.text:0000000000400558
.text:0000000000400558 loc_400558:
.text:0000000000400558 mov     eax, 0
.text:0000000000400558 leave
.text:000000000040055D retn
.text:000000000040055E main
.text:000000000040055E endp
.text:000000000040055E
.text:000000000040055E ; -----
.text:000000000040055E align 20h
.text:0000000000400560
.text:0000000000400560 ; ===== SUBROUTINE =====
.text:0000000000400560 ;
.text:0000000000400560 ; void __libc_csu_init(void)
.text:0000000000400560 public __libc_csu_init
.text:0000000000400560 __libc_csu_init proc near ; DATA XREF: __start+1610
.text:0000000000400560
.text:0000000000400560 push    r15
.text:0000000000400562 push    r14
.text:0000000000400564 mov     r15d, edi
.text:0000000000400567 push    r13
```

Line 10 of 17

00000527 0000000000400527: main+1 (Synchronized with Hex View-1)

Output window

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>

Python

Enter a regular comment

Enter comment...

Enter repeatable comment...

Edit function...

Hide

Graph view

Proximity browser

Undefine

Synchronize with

Add breakpoint

Xrefs graph to...

Xrefs graph from...

Font...

List gross references to... Ctrl+X

Enter a regular comment



## PRO TIP: RENAME LABELS AS YOU GO!

```
text:0000000000400526      push    rbp
text:0000000000400527      mov     rbp, rsp
text:000000000040052A      sub     rsp, 10h
text:000000000040052E      mov     [rbp+var_4], edi
text:0000000000400531      mov     [rbp+var_10], rsi
text:0000000000400535      cmp     [rbp+var_4], 2
text:0000000000400539      jnz     short loc_400558
text:000000000040053B      mov     rax, [rbp+var_10]
text:000000000040053F      add     rax, 8
text:0000000000400543      mov     rax, [rax]
text:0000000000400546      mov     rsi, rax
text:0000000000400549      mov     edi, offset format ; "Hello %s\n"
text:000000000040054E      mov     eax, 0
text:0000000000400553      call    _printf
text:0000000000400558      loc_400558:
text:0000000000400558      mov     eax, 0 ; CODE XREF: main+13!j
text:000000000040055D      leave
text:000000000040055E      retn
text:000000000040055E      main
text:000000000040055E      endp
```

Rename address

Address: 0x400558

Name: QUIT

Maximum length of new names: 15

Local name prefix: @@

☒ Local name  
☐ Include in names list  
☐ Public name  
☐ Autogenerated name  
☐ Weak name  
☐ Create name anyway

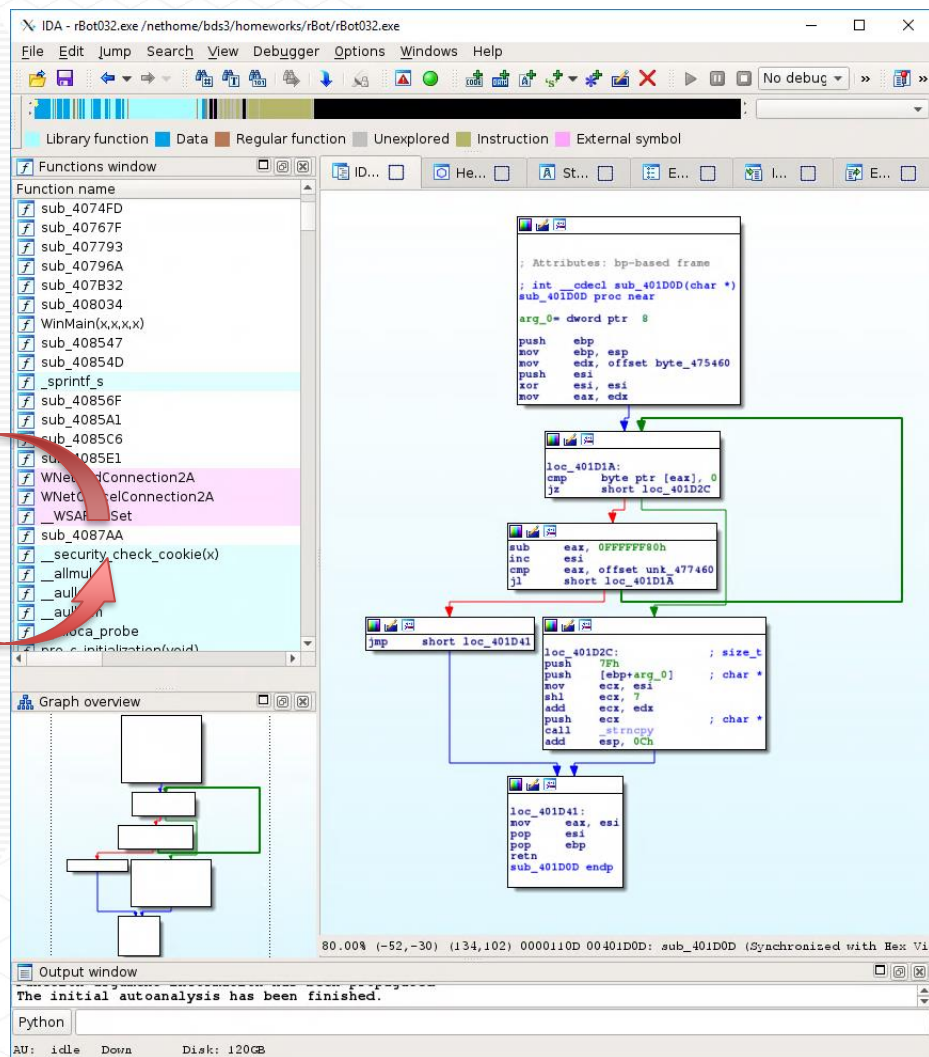
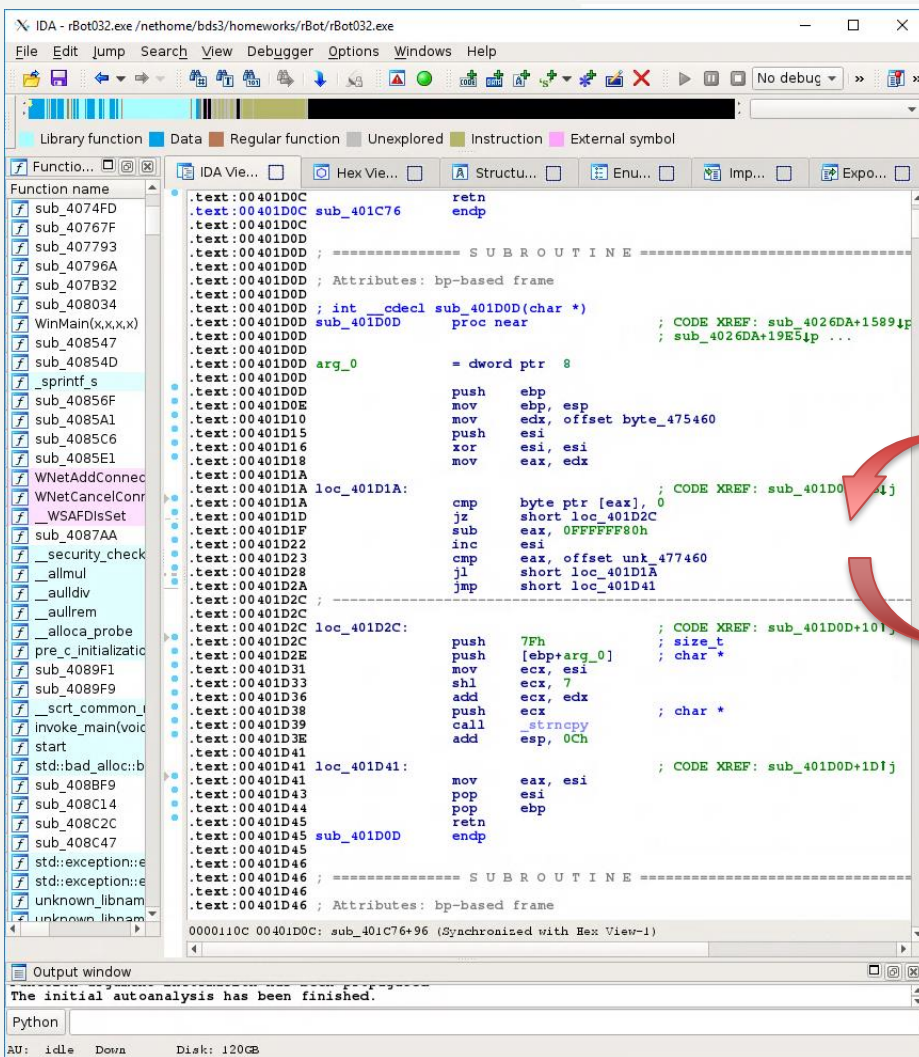
OK Cancel Help

1. Click on the element to rename
2. Press the “n” key
3. Enter name and settings (if any)
4. Enjoy easier to read assembly!

```
text:0000000000400526      push    rbp
text:000000000040052A      sub     rsp, 10h
text:000000000040052E      mov     [rbp+var_4], edi
text:0000000000400531      mov     [rbp+var_10], rsi
text:0000000000400535      cmp     [rbp+var_4], 2
text:0000000000400539      jnz     short QUIT
text:000000000040053B      mov     rax, [rbp+var_10]
text:000000000040053F      add     rax, 8
text:0000000000400543      mov     rax, [rax]
text:0000000000400546      mov     rsi, rax
text:0000000000400549      mov     edi, offset format ; "Hello %s\n"
text:000000000040054E      mov     eax, 0
text:0000000000400553      call    _printf
text:0000000000400558      QUIT:
text:0000000000400558      mov     eax, 0 ; CODE XREF: main+13!j
text:000000000040055D      leave
text:000000000040055E      retn
text:000000000040055E      main
text:000000000040055E      endp
```

## PRO TIP #2: SWITCH BETWEEN VIEWS!

- Text View may be easier to read, but Graph View gives better context
- Comments still show in both views 😊





## PRO TIP #3: NAVIGATION BUTTONS!

- Double-click on a label to jump to it. Want to go back? IDA remembers!



IDA - rBot032.exe / nethome/bds3/homeworks/rBot/rBot032.exe

File Edit Jump Search View Debugger Options Windows Help

Library function Data Regular function Unexplored Instruction External symbol

Function name

- sub\_4074FD
- sub\_40767F
- sub\_407793
- sub\_40796A
- sub\_407B32
- sub\_408034
- WinMain(x,x,x)
- sub\_408547
- sub\_40854D
- sub\_40856F
- sub\_4085A1
- sub\_4085C6
- sub\_4085E1
- WNetAddConne...
- WNetCancelConr...
- \_WSAFDIsSet
- sub\_4087AA
- sub\_4087AA
- \_security\_check...
- \_allmul
- \_aulldiv
- \_aullrem
- \_alloca\_probe
- pro\_4087AA

push 400h ; size\_t  
push ebx ; int  
push offset byte\_45FF0 ; void \*  
call \_memset  
push 0B80h ; size\_t  
push ebx ; int  
push offset byte\_46... ; void \*  
call \_memset  
push offset aMainThread ; "main thread"  
call sub\_401D0D  
push 00h ; size\_t  
push 00h ; int  
off: Attributes: bp-based frame  
call off: int cdecl sub\_401D0D(char \*)  
sub\_401D0D proc near ; CODE XREF: sub\_4026DA+15891p  
7Fh ; sub\_4026DA+19E51p ...  
push edi arg\_0 = dword ptr 8  
push ebp  
call \_st... push ebp, esp  
add esp  
mov dword\_45FE08, 1A0Bh  
push 3Fh ; size\_t  
push offset asc\_45F010 ; "W"  
push offset byte\_45FE0C ; char \*  
call \_strcpy  
push 3Fh ; size\_t  
push offset byte\_47505D ; char \*  
push offset byte\_45FE4C ; char \*  
call \_strcpy  
add esp, 18h  
mov dword\_45FE08, ebx

loc\_4084E7:  
mov esi, ebx

loc\_4084E9: ; lpThreadParameter  
push edi  
call sub\_4024DC  
mov dword\_45FE08, ebx  
cmp eax, 2  
jz short loc\_40850D

100.00% (90,5097) (91,128) 0000787E 0040847E: WinMain(x,x,x,x)+3B2 (Synchronized with Hex View-1)

Output window

The initial autoanalysis has been finished.

Python

AU: idle Down Disk: 120GB

IDA - rBot032.exe / nethome/bds3/homeworks/rBot/rBot032.exe

File Edit Jump Search View Debugger Options Windows Help

Library function Data Regular function Unexplored Instruction External symbol

Functions window

- sub\_4074FD
- sub\_40767F
- sub\_407793
- sub\_40796A
- sub\_407B32
- sub\_408034
- WinMain(x,x,x)
- sub\_408547
- sub\_40854D
- sub\_40856F
- sub\_4085A1
- sub\_4085C6
- sub\_4085E1
- WNetAddConnection2A
- WNetCancelConnection2A
- \_WSAFDIsSet
- sub\_4087AA
- \_security\_check\_cookie(x)
- \_allmul
- \_aulldiv
- \_aullrem
- \_alloca\_probe
- pro\_4087AA

Attributes: bp-based frame  
; int cdecl sub\_401D0D(char \*)  
sub\_401D0D proc near  
arg\_0= dword ptr 8  
push ebp, esp  
mov ebx, esp  
mov edx, offset byte\_475460  
push esi  
xor esi, esi  
mov eax, edx

loc\_401D1A:  
cmp byte ptr [eax], 0  
jz short loc\_401D2C

sub eax, 0FFFFFFF0h  
inc esi  
cmp eax, offset unk\_477460  
jl short loc\_401D1A

jmp short loc\_401D41

loc\_401D2C: ; size\_t  
push 7Fh  
push [ebp+arg\_0] ; char \*  
mov ecx, esi  
shl ecx, 7  
add ecx, edx  
push ecx  
call \_strcpy  
add esp, 0Ch

loc\_401D41:  
mov eax, esi  
pop ebp  
retn  
sub\_401D0D endp

80.00% (-52,-30) (134,102) 0000110D 00401D0D: sub\_401D0D (Synchronized with Hex Vi...

Graph overview

Output window

The initial autoanalysis has been finished.

Python

AU: idle Down Disk: 120GB

## PRO TIP #4: RENAME SYMBOLIC CONSTANTS



- IDA's FLIRT signatures know the arguments for common APIs
- But IDA also knows the symbolic names for most defined constants!
- You just have to tell IDA what value you are looking for

```
LONG WINAPI RegCreateKeyEx (  
    _In_      HKEY          hKey,  
    _In_      LPCTSTR       lpSubKey,  
    _Reserved_ DWORD       Reserved,  
    _In_opt_  LPTSTR        lpClass,  
    _In_      DWORD         dwOptions,  
    _In_      REGSAM        samDesired,  
    _In_opt_  LPSECURITY_ATTRIBUTES lpSecurityAttributes,  
    _Out_     PHKEY         phkResult,  
    _Out_opt_ LPDWORD       lpdwDisposition  
)
```

```
lea    eax, [ebp+phkResult]  
push   ecx          ; lpdwDisposition  
push   eax          ; phkResult  
push   ecx          ; lpSecurityAttributes  
push   0F003Fh      ; samDesired  
push   ecx          ; dwOptions  
push   ecx          ; lpClass  
push   ecx          ; Reserved  
push   offset aSoftwareMicr_1 ; "Software\\Microsoft\\Windows\\CurrentVe"...  
push   80000002h     ; hKey  
call   ebx ; RegCreateKeyEx
```



## PRO TIP #4: RENAME SYMBOLIC CONSTANTS (2)

- Right Click -> Use standard symbolic constant
- Then simply find the constant name you are looking for



Assembly code snippet:

```
push 80000002h ; hKey
call ebx ; Reg
push 0Ch
lea eax, [ebp+phkR]
push eax
push 1
push 0
offset aC
push [ebp+phkR]
call edi ; Reg
push [ebp+phkR]
call esi ; Reg
xor ecx, ecx
lea eax, [ebp+phkR]
push ecx
push eax
push ecx
push 0F003Fh
push ecx
push ecx
push ecx
offset aS
push 80000001h
call ebx ; Reg
push 0Ch
lea eax, [ebp+Data1]
xor ebx, ebx
push eax
```

Assembly code snippet:

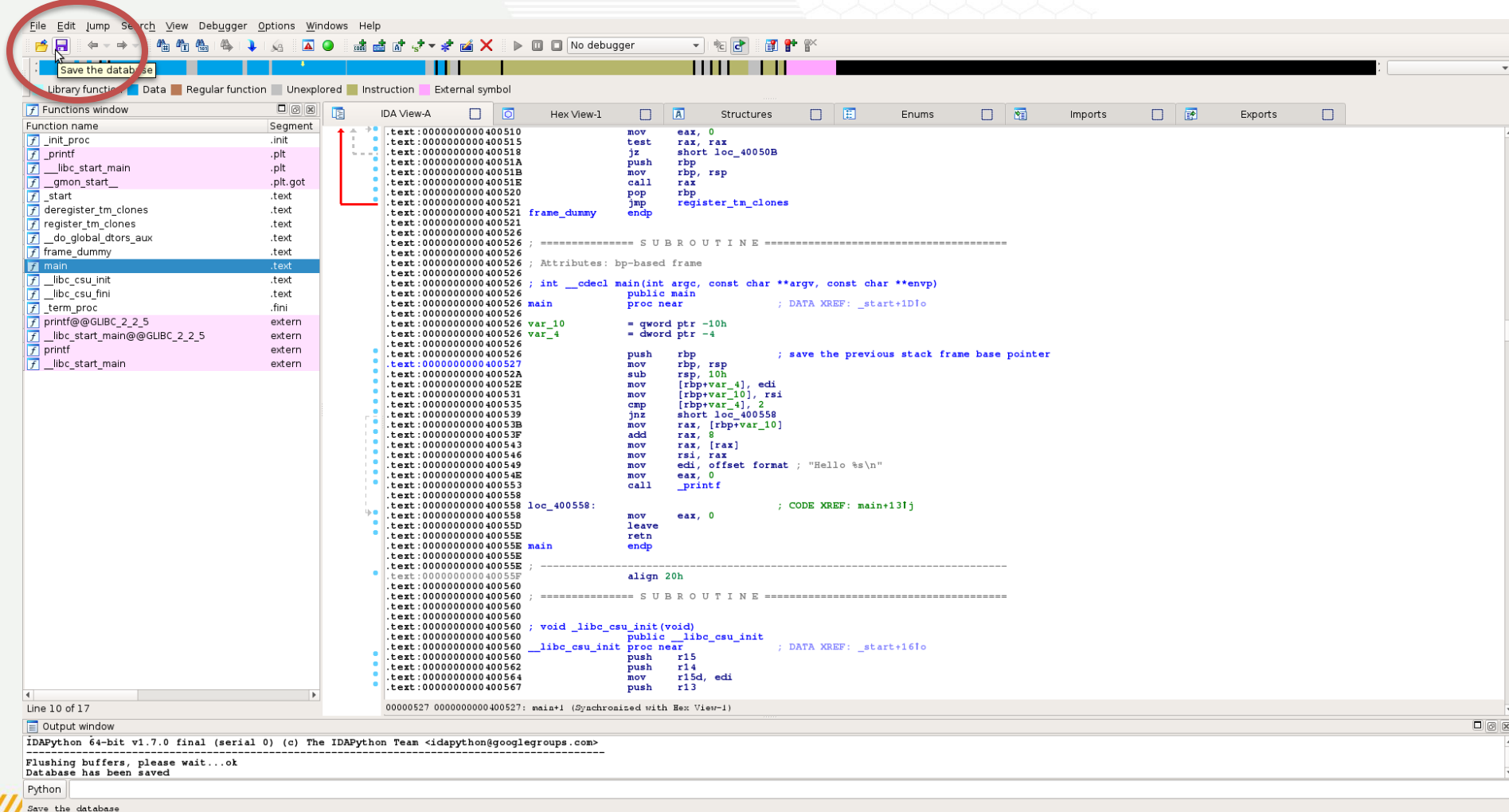
```
push offset aSoftwareMicr_1 ; "
push HKEY_LOCAL_MACHINE ; hKey
call ebx ; RegCreateKeyExA
push 0Ch
lea eax, [ebp+Data1]
```

Type name	Declaration	Type library
CHANGER_PREDISMOUNT_ALIGN_TO_DRIVE	80000002	MS SDK (Windows XP)
DSOP_DOWNLEVEL_FILTER_LOCAL_GROUPS	80000002	MS SDK (Windows XP)
DeviceDsmAction_Notification	FFFFFFFF80000002	MS SDK (Windows XP)
EXCEPTION_DATATYPE_MISALIGNMENT	80000002	MS SDK (Windows XP)
<b>HKEY_LOCAL_MACHINE</b>	<b>80000002</b>	<b>MS SDK (Windows XP)</b>
MQCONN_CREATE_SOCKET_FAILURE	80000002	MS SDK (Windows XP)
PERF_QUERY_COSTLY	FFFFFFFF80000002	MS SDK (Windows XP)
PID_SECURITY	00000013	MS SDK (Windows XP)
STATUS_DATATYPE_MISALIGNMENT	80000002	MS SDK (Windows XP)
TAPE_DRIVE_TENSION	FFFFFFFF80000002	MS SDK (Windows XP)
tomitalic	80000002	MS SDK (Windows XP)
EXCEPTION_DATATYPE_MISALIGNMENT	80000002	Visual C++ v6
HKEY_LOCAL_MACHINE	80000002	Visual C++ v6
HKEY_PERF_ROOT	FFFFFFFF80000002	Visual C++ v6
LINEERR_BADDEVICEID	80000002	Visual C++ v6
PERF_QUERY_COSTLY	FFFFFFFF80000002	Visual C++ v6
PID_SECURITY	FFFFFFFF80000002	Visual C++ v6
STATUS_DATATYPE_MISALIGNMENT	80000002	Visual C++ v6
TAPE_DRIVE_TENSION	FFFFFFFF80000002	Visual C++ v6

- If you can't find the symbol, you may need to add it
- First, look up the symbol's header file definition
- Second, read about adding new Enums and symbolic constants here: <https://www.hex-rays.com/products/ida/support/idadoc/499.shtml>

SAVE OFTEN!

- Losing hours of reverse engineering can be hazardous to your health!
- CTRL-W !!





**Georgia  
Tech**

- The screenshot shows the Immunity Debugger interface. The 'File' menu is open, and the path 'Create MAP file...' > 'Create LST file...' is highlighted. A tooltip for 'Create a listing file' is visible. The main window displays the assembly code for the 'main' function, which is a C program snippet. The bottom status bar indicates that the listing file has been created successfully.

**File Menu Path:**

  - File
  - Open...
  - Load file
  - Produce file
    - Create MAP file... (Alt+F10)
    - Create ASM file...
    - Create INC file...
    - Create LST file... (Create a listing file)
    - Create EXE file...
    - Create DJF file...
    - Create HTML file...
    - Create flow chart GDL...
    - Create call graph GDL...
    - Create C header file...
  - Dump database to IDC file...
  - Dump typeinfo to IDC file...
  - Exit (Alt+X)

**Assembly Code Snippet:**

```

main(int argc, const char **argv, const char **envp)
public main
proc near
; DATA XREF: _start+1D10
= dword ptr -10h
= 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 QUIT
mov rax, [rbp+var_10]
add rax, 8
mov rax, [rax]
mov rax, rax
mov rax, rax
mov edi, offset format
mov eax, 0
call _printf
; CODE XREF: main+131j
mov eax, 0
leave
retn
endp

```

**Status Bar:**

Line 10 of 17

Output window

Database has been saved

Writing listing file /nethome/bds3/homeworks/hello.lst,

address range 00000000004003C8-0000000000601080

Listing file has been created, total 840 lines.

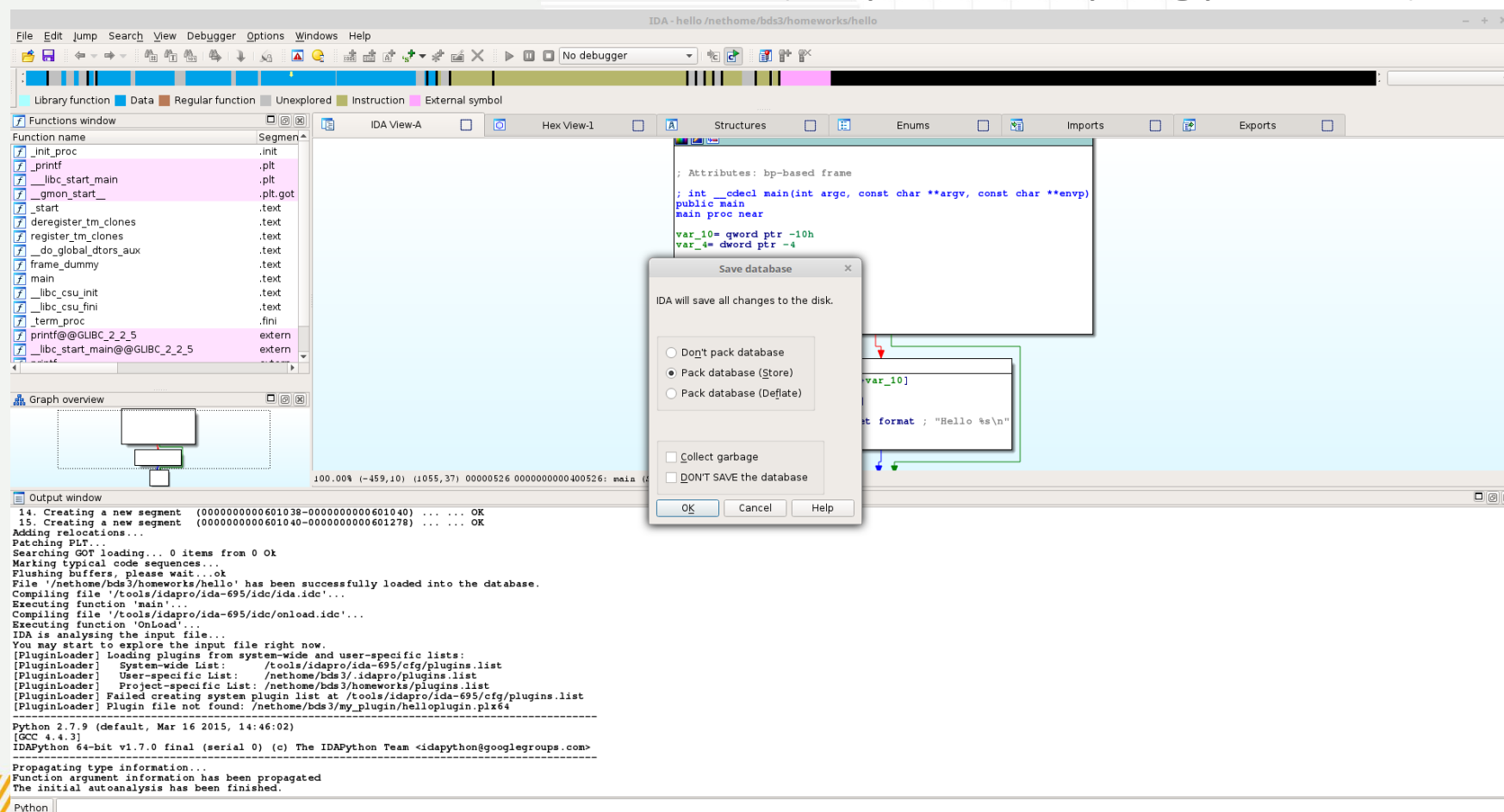
Python

Create a listing file

# READY TO CLOSE IDA? SAVE YOUR DATABASE (OR NOT)



- IDA will compress all of its data into a single database to save your progress
  - The save file is called an idb file for 32-bit and i64 for 64-bit
- You can also tell IDA to not save a database (i.e., you lose everything you've done)



## AS YOU WORK, SO DOES IDA



- IDA performs very substantial analysis for you and saves the results in a number of files while you work
- If you kill IDA (or lose connection to the IDA servers), these files will be corrupted!
- So save often!! Saving will create/update the database file

```
File Edit View Search Terminal Help
bds3@ecelinsrvw.ece.gatech.edu>cd homeworks/
bds3@ecelinsrvw.ece.gatech.edu>ls
hello hello.id0 hello.id1 hello.id2 hello.nam hello.til
bds3@ecelinsrvw.ece.gatech.edu>
[1] Done idaq64
bds3@ecelinsrvw.ece.gatech.edu>ls
hello hello.i64
bds3@ecelinsrvw.ece.gatech.edu>
```

bsaltafo  
bsaltafo  
lrdbsalt

If you are having problems running applications, see  
<http://www.ece-help.gatech.edu/unix/cshrc.html> for  
information on configuring your login environment.

```
bds3@ecelinsrvw.ece.gatech.edu>ls
bin Documents hello_world_plugin.tar.gz perl5 public Videos
```

## ADDITIONAL READINGS (OPTIONAL)



- Chris Eagle. The IDA Pro Book. No Starch Press (2<sup>nd</sup> Edition), 2011.  
ISBN: 978-1593272890
  - You can probably find the PDF version online!
- Guided Hacking's "How To Reverse Engineer" Videos
  - <https://www.youtube.com/playlist?list=PLt9cUwGw6CYFXtAEIzDLob2aOaSfZqHJc>

**QUESTIONS?**

**CREATING THE NEXT®**