

Proj 6: IDA Pro (Lab 5-1) (20 pts., 4 images)

What you need:

- A Windows machine, real or virtual, such as the Windows 2008 Server VM we've been using
- The textbook: "Practical Malware Analysis"

Purpose

You will practice using IDA Pro.

You should already have the lab files, but if you don't, do this:

Downloading the Lab Files

In a Web browser, go here:

<http://practicalmalwareanalysis.com/labs/>

Download and unzip the lab files.

Downloading and Installing IDA Pro

In your Windows machine, open a Web browser and go to

https://www.hex-rays.com/products/ida/support/download_freeware.shtml

Download "**IDA Freeware**" and install it.

If that link is down, use this alternate download link:

<https://samsclass.info/126/proj/idafree50.exe>

Follow the Textbook

Follow the instructions for **Lab 5-1** in the textbook, questions 1-8, to analyze Lab05-01.dll using only IDA Pro. There are more detailed solutions in the back of the book.

Opening Lab05-01.dll in IDA Pro

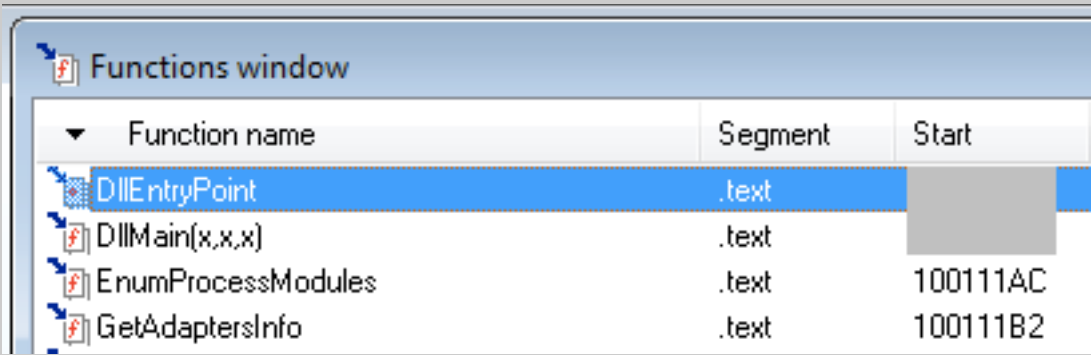
Launch IDA Pro. Click **OK**. Click **New**. Click the "**PE Dynamic Library**" icon and click **OK**. Navigate to Lab05-01.dll and open it.

Q 1: Finding the Address of DLLMain

In IDA Pro, click **Windows**, "**Functions window**".

Click the "**Function name**" header to sort by name and scroll to the top.

Your image should show the location of DLLMain, as shown below:



Press the **PrntScrn** key to capture an image of the whole desktop.

Open Paint and paste the image in with **Ctrl+V**.

Save this image with the filename "**Proj 6a from YOUR NAME**".

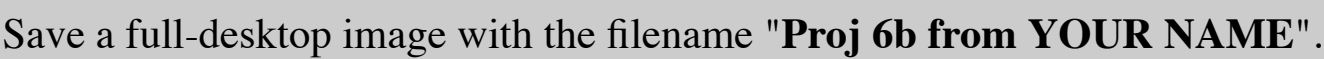
YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT!

Q 2: Find the import for gethostbyname

In IDA Pro, click **Windows**, **Imports**. Click the **Name** header to sort by name. Find "gethostbyname" -- note that capital letters and lowercase letters sort into separate groups.

Widen the **Address** column to make the entire address visible.

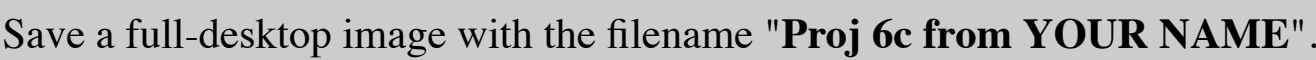
Your image should show the location of gethostbyname, as shown below:



In IDA Pro, click **Windows**, "**IDA View-A**". Press the **SPACEBAR** to get to text view.

Press **g** to Go. Enter the address **0x10001656** and click **OK**.

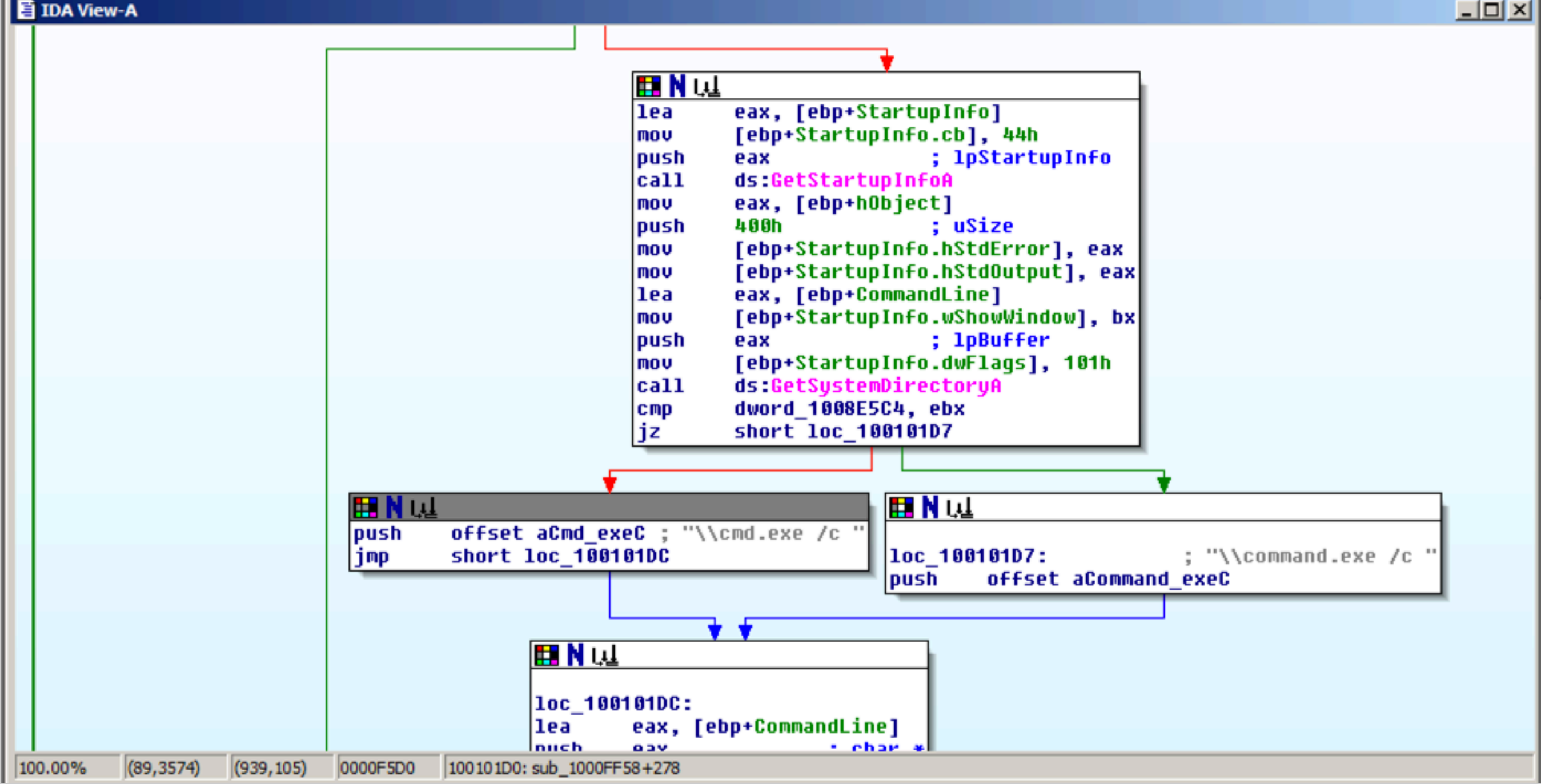
Scroll up to show the comments IDA added to the start of the function, listing its local variables, as shown below:



In IDA Pro, click **Windows**, **Strings**. Make the window larger. Sort by **String**. Find the String "`\cmd.exe /c`" and double-click it. The function opens in text view, as shown below.

In the line containing "`\\cmd.exe /c`", double-click the address to the right of "XREF", as indicated by the red outline in the image below.



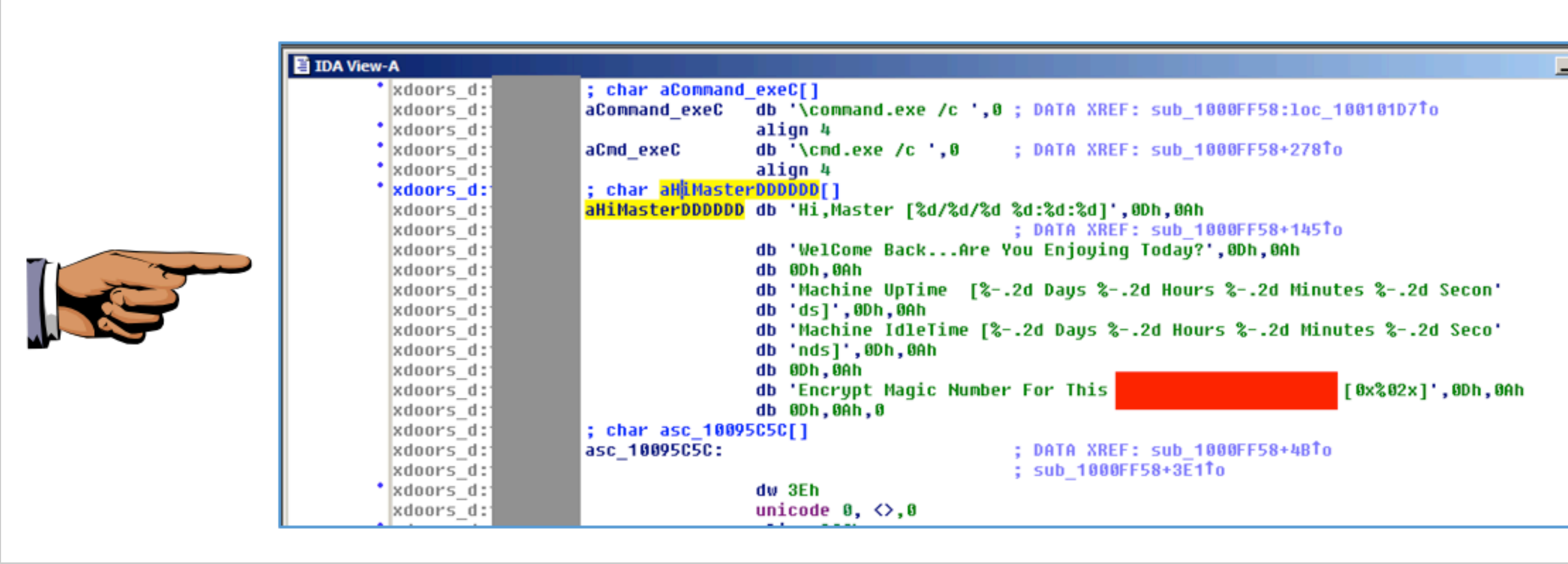


Drag the graph view down to see the subroutines before it. About three boxes up you should find text beginning with "Hi, Master", as shown below.

```
push    eax
movzx   eax, [ebp+SystemTime.wHour]
push    eax
movzx   eax, [ebp+SystemTime.wDay]
push    eax
movzx   eax, [ebp+SystemTime.wMonth]
push    eax
movzx   eax, [ebp+SystemTime.wYear]
push    eax
lea     eax, [ebp+var_EC0]
push    offset aHiMasterDDDDDD ; "Hi,Master [%d/%d/%d %d:%d:%d]\r\nWelCome "...
push    eax                ; char *
call    ds:sprintf
add     esp, 44h
xor     ebx, ebx
lea     eax, [ebp+var_EC0]
push    ebx
push    eax                ; char *
call    strlen
```

Double-click **aHiMasterDDDD** to find the complete message. The purpose of the malware is clearly stated.

Your image should show what the code is doing, as shown below. The purpose is behind the red rectangle in the image below.



Save a full-desktop image with the filename "Proj 6d from YOUR NAME".

Turning in your Project

Email the images showing to cnit.126sam@gmail.com with the subject line: **Proj 6 from YOUR NAME**