Proj 7x: Analyzing Malicious Windows Programs (Lab 7-2) (15 pts.)

What you need:

- A Windows XP or Windows 7 machine with IDA PRO and the other tools we have been using
- The textbook: "Practical Malware Analysis"

Purpose

You will practice the techniques in chapter 7.

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/

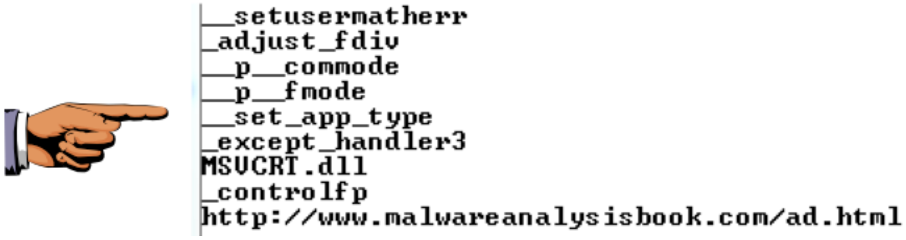
Download and unzip the lab files.

Follow the instructions for **Lab 7-2** in the textbook. There are more detailed solutions in the back of the book. The only purpose of this document is to explain what image to turn in.

Unicode String

Use an appropriate tool to display Unicode strings. You cannot do this with IDA Pro Free.

When you display the URL shown at the bottom of the image below, capture a full-desktop image.



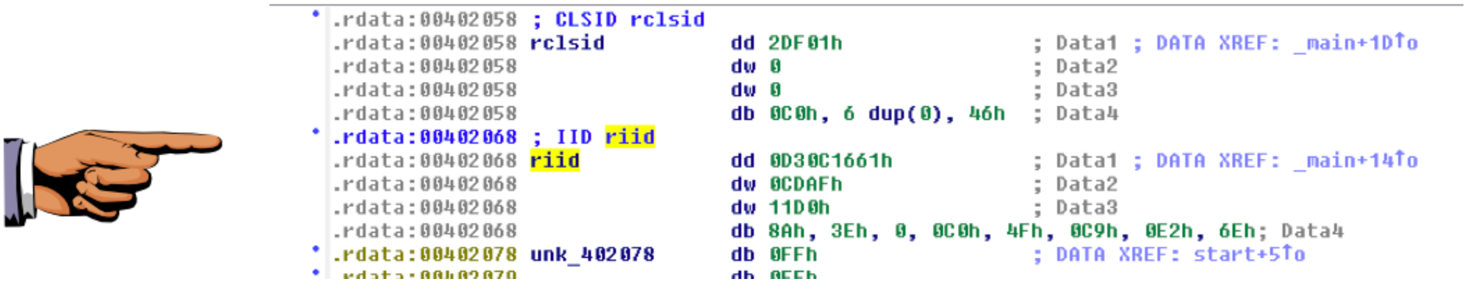
```
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
MSVCRT.dll
_controlfp
http://www.malwareanalysisbook.com/ad.html
```

Save this image with the filename "**Proj 7xa from YOUR NAME**".

rclsid

Use IDA Pro Free to find the value of **rclsid**. It's spread across several lines of assembly code, as shown below, but you can reassemble it to form a single 128-bit value starting with 2DF0 and ending with 0046.

Save a full-desktop image showing the value of **rclsid**, as shown below.



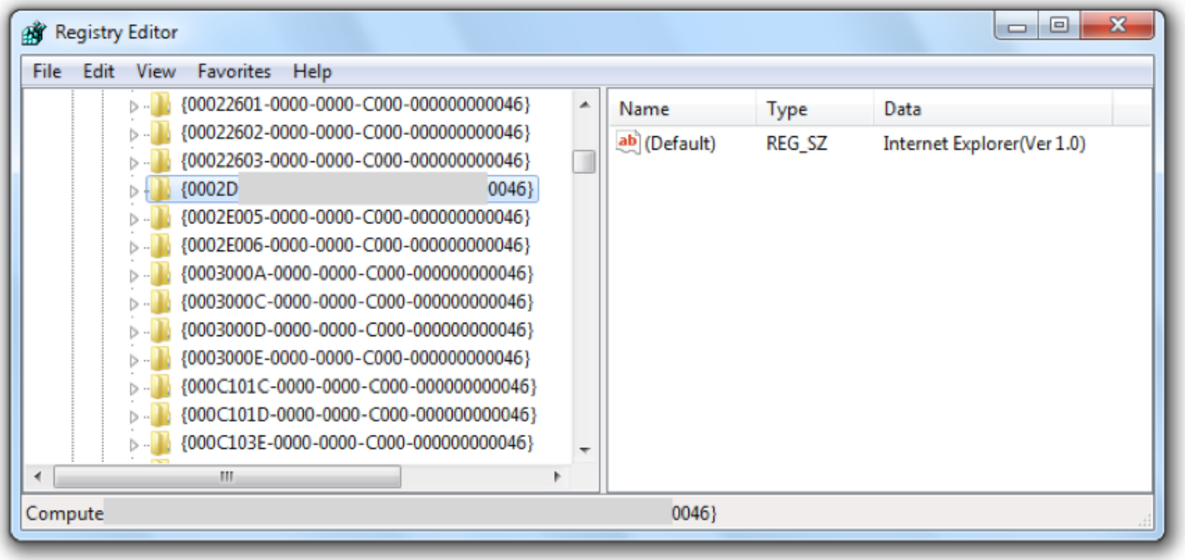
```
.rdata:00402058 ; CLSID rclsid
.rdata:00402058 rclsid          dd 2DF01h               ; Data1 ; DATA XREF: _main+1D↑o
.rdata:00402058                 dw 0                    ; Data2
.rdata:00402058                 dw 0                    ; Data3
.rdata:00402058                 db 0C0h, 6 dup(0), 46h  ; Data4
.rdata:00402068 ; IID riid
.rdata:00402068 riid            dd 0D30C1661h           ; Data1 ; DATA XREF: _main+14↑o
.rdata:00402068                 dw 0CDAFh               ; Data2
.rdata:00402068                 dw 11D0h                ; Data3
.rdata:00402068                 db 8Ah, 3Eh, 0, 0C0h, 4Fh, 0C9h, 0E2h, 6Eh; Data4
.rdata:00402078 unk_402078      db 0FFh                 ; DATA XREF: start+5↑o
.rdata:00402079                 db 0FFh
```

Save this image with the filename "**Proj 7xb from YOUR NAME**".

Registry

Find the **rclsid** in the Registry.

Save a full-desktop image showing its value, including the fields grayed out below.



```
{00022601-0000-0000-C000-000000000046}
{00022602-0000-0000-C000-000000000046}
{00022603-0000-0000-C000-000000000046}
{0002D[redacted]0046}
{0002E005-0000-0000-C000-000000000046}
{0002E006-0000-0000-C000-000000000046}
{0003000A-0000-0000-C000-000000000046}
{0003000C-0000-0000-C000-000000000046}
{0003000D-0000-0000-C000-000000000046}
{0003000E-0000-0000-C000-000000000046}
{000C101C-0000-0000-C000-000000000046}
{000C101D-0000-0000-C000-000000000046}
{000C103E-0000-0000-C000-000000000046}
```

Name	Type	Data
(Default)	REG_SZ	Internet Explorer(Ver 1.0)

Compute[redacted]0046}

Save this image with the filename "**Proj 7xc from YOUR NAME**".

Turning in your Project

Email the images to cnit.126sam@gmail.com with the subject line: **Proj 7x from YOUR NAME**

Last modified 9-30-13 4:43 pm