

Proj 1x: Using File and Strings (10 pts.)

What you need:

- A Windows computer (real or virtual) with an Internet connection
- The textbook: "Practical Malware Analysis"

Purpose

You will use the 'file' and 'strings' commands to analyze files without filename extensions. These are native Linux commands, but they have been ported to Windows.

Downloading 'file'

In a Web browser, go here:

<http://sourceforge.net/projects/gnuwin32/files/file/5.03/file-5.03-setup.exe/download>

Download the **file-5.03-setup.exe** file and execute it. install the software with the default options.

Open an Administrator Command Prompt window, and execute this command:

```
set PATH=%PATH%;c:\program files\gnuwin32\bin
```

Downloading 'strings'

In a Web browser, go here:

<http://technet.microsoft.com/en-us/sysinternals/bb897439>

Click the "Download Strings" link.

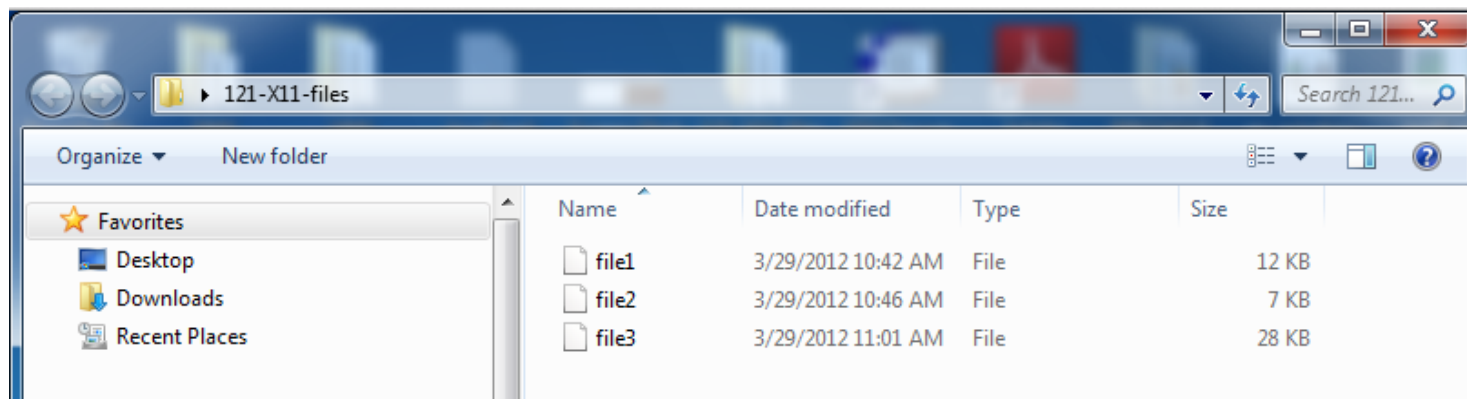
Save the **Strings.zip** file on your desktop. Unzip it, and copy **strings.exe** to the C:\Windows\System32 folder.

Downloading the Files to Examine

In a Web browser, go here:

<http://samsclass.info/121/proj/121-X11-files.zip>

Save the **121-X11-files.zip** file on your desktop. Unzip it. A folder named 121-X11-files opens, containing three files, as shown below:



In a Command Prompt window, execute these commands, replacing 'Student' with your correct user name:

```
cd \Users\Student\Desktop\121-X11-files
file *
```

The file types of the files is revealed, as shown below:

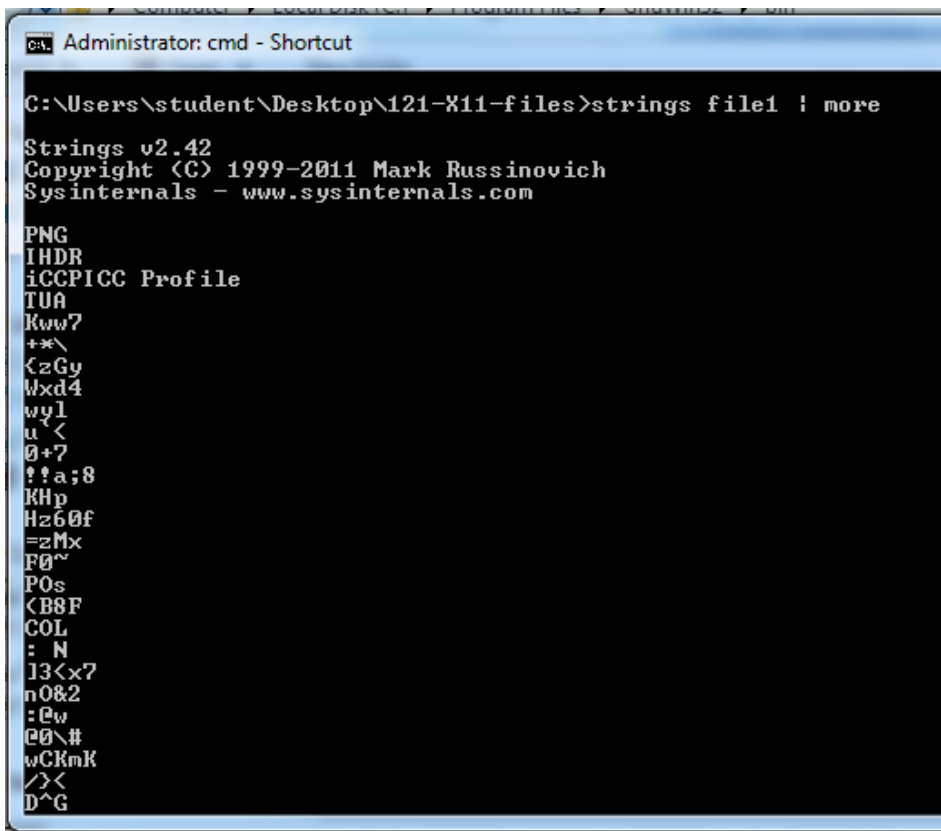
```
C:\Users\student\Desktop\121-X11-files>file *
file1; PNG image, 322 x 68, 8-bit/color RGB, non-interlaced
file2; Non-ISO extended-ASCII English text, with very long lines, with CRLF line
terminators
file3; PE32 executable for MS Windows (console) Intel 80386 32-bit
```

Using Strings

In a Command Prompt window, execute this command:

```
strings file1 | more
```

You see the readable strings in the file, which are just nonsense, because this is an image file, as shown below:



```
Administrator: cmd - Shortcut

C:\Users\student\Desktop\121-X11-files>strings file1 | more

Strings v2.42
Copyright (C) 1999-2011 Mark Russinovich
Sysinternals - www.sysinternals.com

PNG
IHDR
iCCP
Profile
TUA
KwW?
+x\
<zGy
Wxd4
wyl
u<
0+?
!!a;8
KHp
Hz60f
=zMx
F0~
POs
<B8F
COL
: N
13<x?
n0&2
:0w
00\#
wCKmK
/><
D^G
```

Find Secret Messages

Now you have tools powerful enough to find the two secret messages I have hidden in those files.

To find them, I recommend this procedure:

- Change all file extensions to reflect the correct filetype you learned with file
- Open the files in the appropriate program for each type
- View the strings inside each file

You will find messages saying "The secret message is..." in two of the files. One of them contains no secret.

When you find the secrets, save them, as screen captures.

Turning in your Project

Email the images showing the secret messages to cnit.126sam@gmail.com with the subject line: **Proj 1x from YOUR NAME**

Last modified 8-22-13