**Lab 10: Data Encoding (Lab 13-1)**

What you need:

* A Windows machine with the tools we have been using installed. I did this project easily on Win 10 TP. It also works on Windows Server 2008.

**Purpose**

You will practice the techniques in chapter 13.

**Beacons**

The book recommends running the malware with another VM simulating the Internet with inetsim, but I don't see any good reason to bother with that. I just connected a VM to the real Internet and ran the malware.

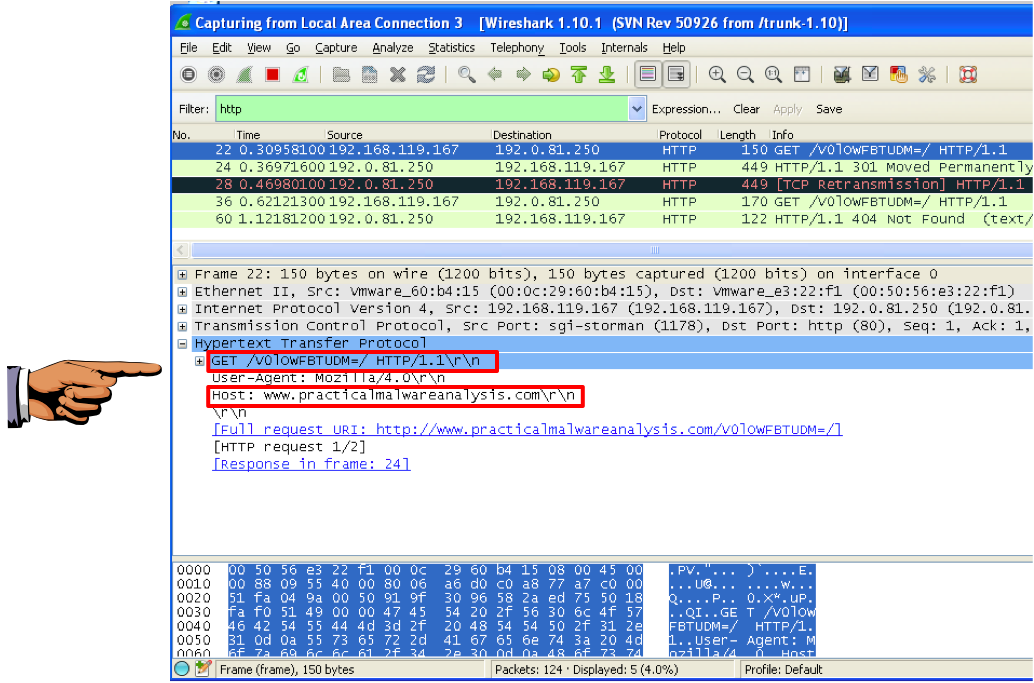
Launch the **Lab13-01.exe** file.

Use either method, and capture a beacon with Wireshark.

Adjust the wireshark window to show these two features, highlighted below:

* **GET /*randomletters*/ HTTP/1.1**
* **Host: www.practicalmalwareanalysis.com**

Save this image with the filename "**Proj 16a from YOUR NAME**".

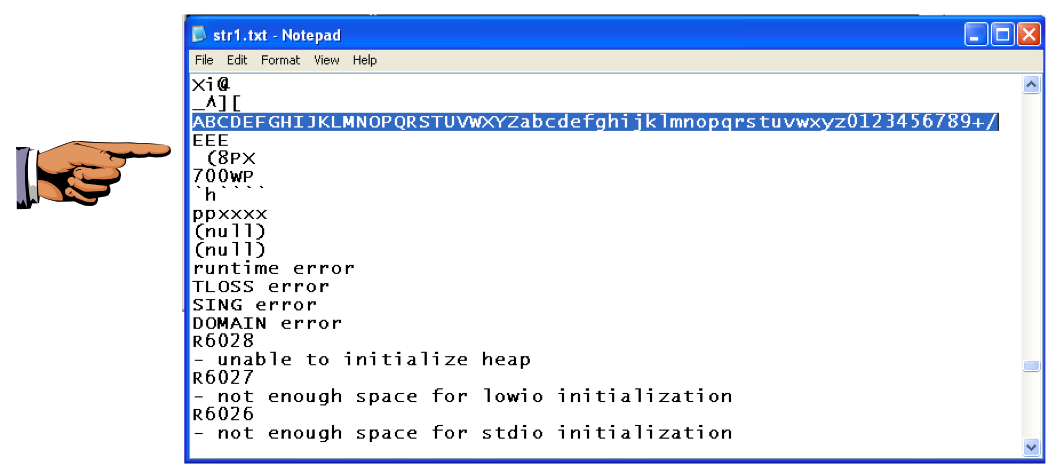


**Strings**

The book uses strings only to point out two strings that are not visible. But there is an interesting string present, showing the use of Base64 encoding.

Examine the strings in the **Lab13-01.exe** file.

Save an image showing the string highlighted below, with the filename "**Proj 16b from YOUR NAME**".



**IDA Pro**

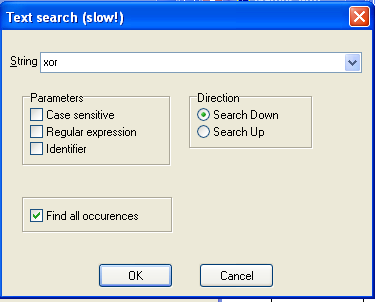
Open **Lab13-01.exe** file in IDA Pro.

Click **Options**, **General**. Check "**Line Prefixes**" and click **OK**.

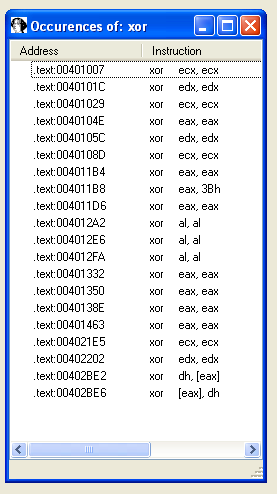
Click in the "IDA View-A" window to make it active.

From the menu bar, click **Search**, **text...**.

In the Text Search dialog, enter **xor** and check "**Find all occurrences**", as shown below:



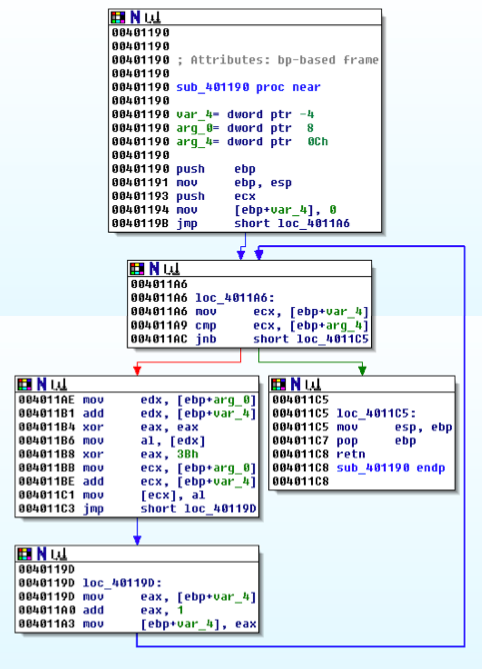
A list of locations using the XOR command appears, as shown below.



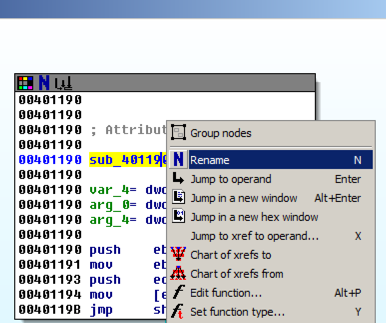
Double-click the **xor eax, 3Bh** instruction.

You should see the function shown below.

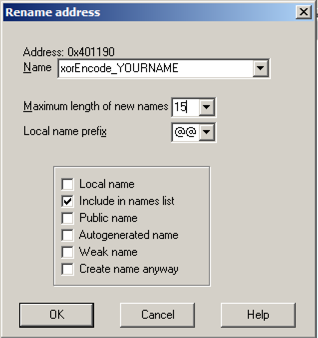
As explained in the book, this function performs xor encoding.



In the top box of the function, right-click **sub\_401190** and click **Rename**, as shown below.



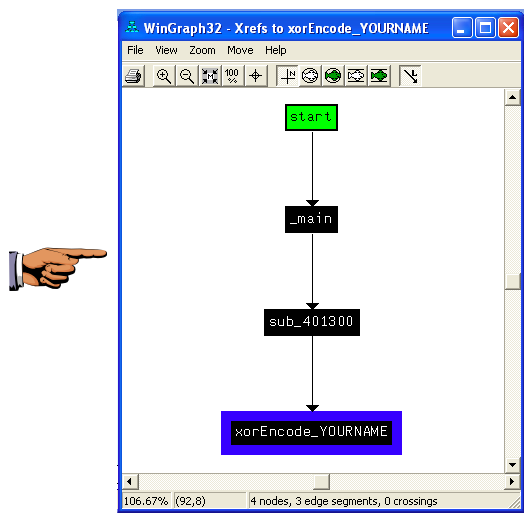
Enter a new name of **xorEncode\_YOURNAME**, as shown below, replacing "YOURNAME" with your own name.



Click **OK**. If you are prompted to, increase the name length limit.

Right-click **xorEncode\_YOURNAME** and click "**Chart of xrefs to**".

A chart showing four boxes appears, ending with one containing your name, as shown below.



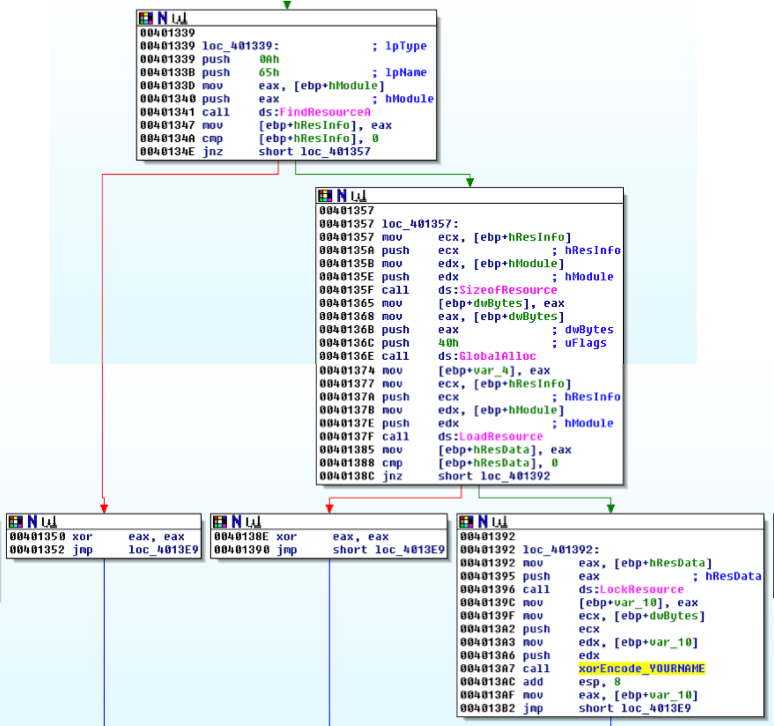
Save an image showing the **four boxes** with **Your name** in the bottom one, "**Proj 16c from YOUR NAME**". Close the "WinGraph32 - Xrefs to xorEncode..." box.

Right-click **xorEncode\_YOURNAME** and click "**Jump to xref to operand...**".

A box pops up showing the address of the xref. Click **OK**.

This function, as shown below, calls these functions (shown in pink letters):

* FindResourceA
* SozeofResource
* GlobalAlloc
* LoadResource
* LockResource



As explained in the book, this code loads a resource and then encodes it.

The resource is identified by its index of 65h, specified in the code at location 401338.

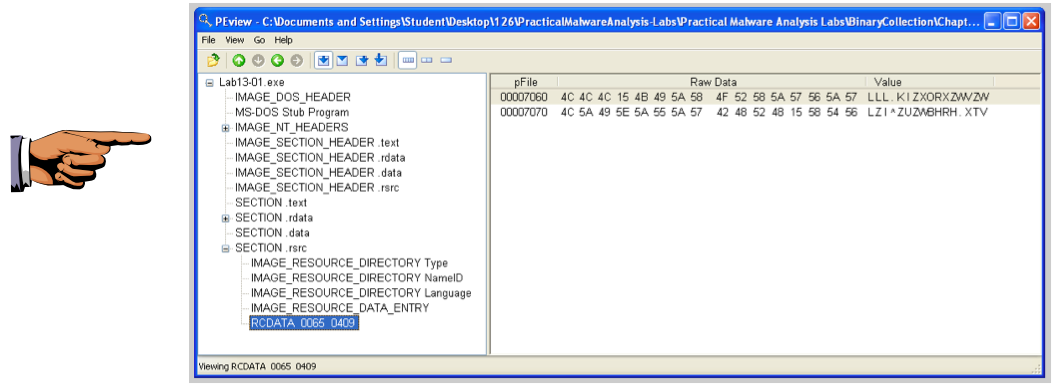
**PEview**

Open the **Lab13-01.exe** file in PEview.

In the left pane, click the **RCDATA 0065 0409** resource.

In the right pane, find the starting address **00007060**, as shown below.

Save an image showing **RCDATA 0065 0409** and **00007060** with the filename "**Proj 16d from YOUR NAME**".



**WinHex**

In a Web browser, go to:

<http://winhex.com/winhex/>

On the left side, click the **Download** button, as shown below.



Right-click the **winhex.zip** file, click "**Extract All**", and click **Extract**.

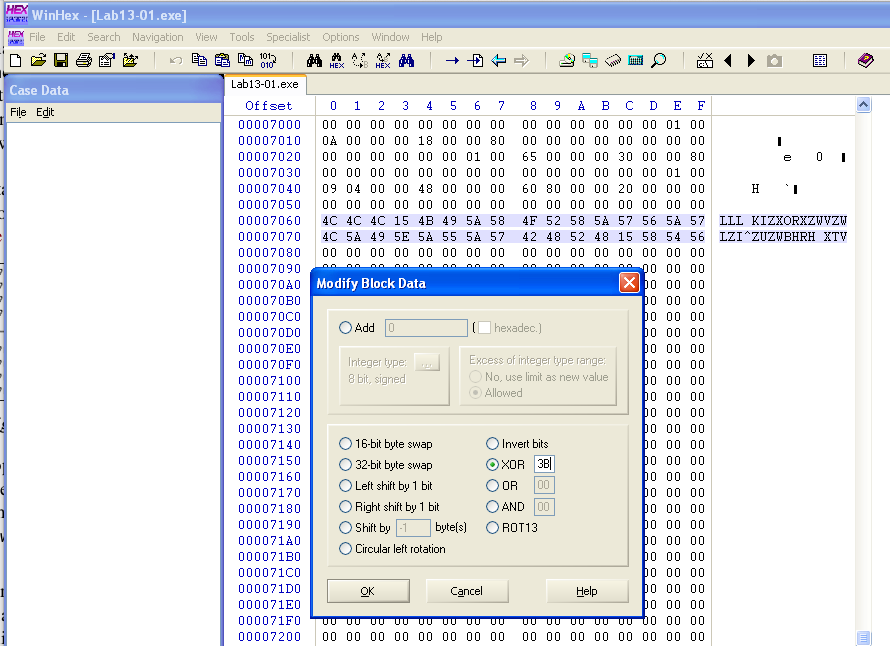
A window appears showing the files contained in the winhex archive. Double-click **setup.exe**. Accept the default options to install WinHex. When the installation is complete, WinHex runs.

|  |
| --- |
| **Troubleshooting**  If double-clicking setup.exe does nothing, open a Command Prompt and launch it from there. |

In WinHex, click **File**, **Open**. Open the **Lab13-01.exe** file in WinHex. Highlight bytes 7060 through 707F, as shown below.

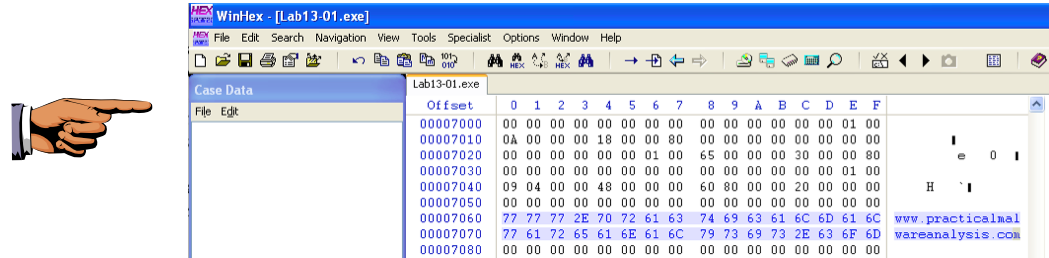
Click **Edit**, "**Modify Data**".

In the "Modify Block Data" box, check the **XOR** radio button and enter a key of **3B**, as shown below:



Click **OK**.

The decoded string appears on the right side: "www.practicalmalwareanalysis.com", as shown below:



Save an image showing **www.practicalmalwareanalysis.com** with the filename "**Proj 16e from YOUR NAME**".