Proj 16: Data Encoding (Lab 13-1) (25 pts.)

What you need:

- A Windows machine with the tools we have been using installed. It doesn't need to be Windows XP--I did this project easily on Win 10 TP.

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.

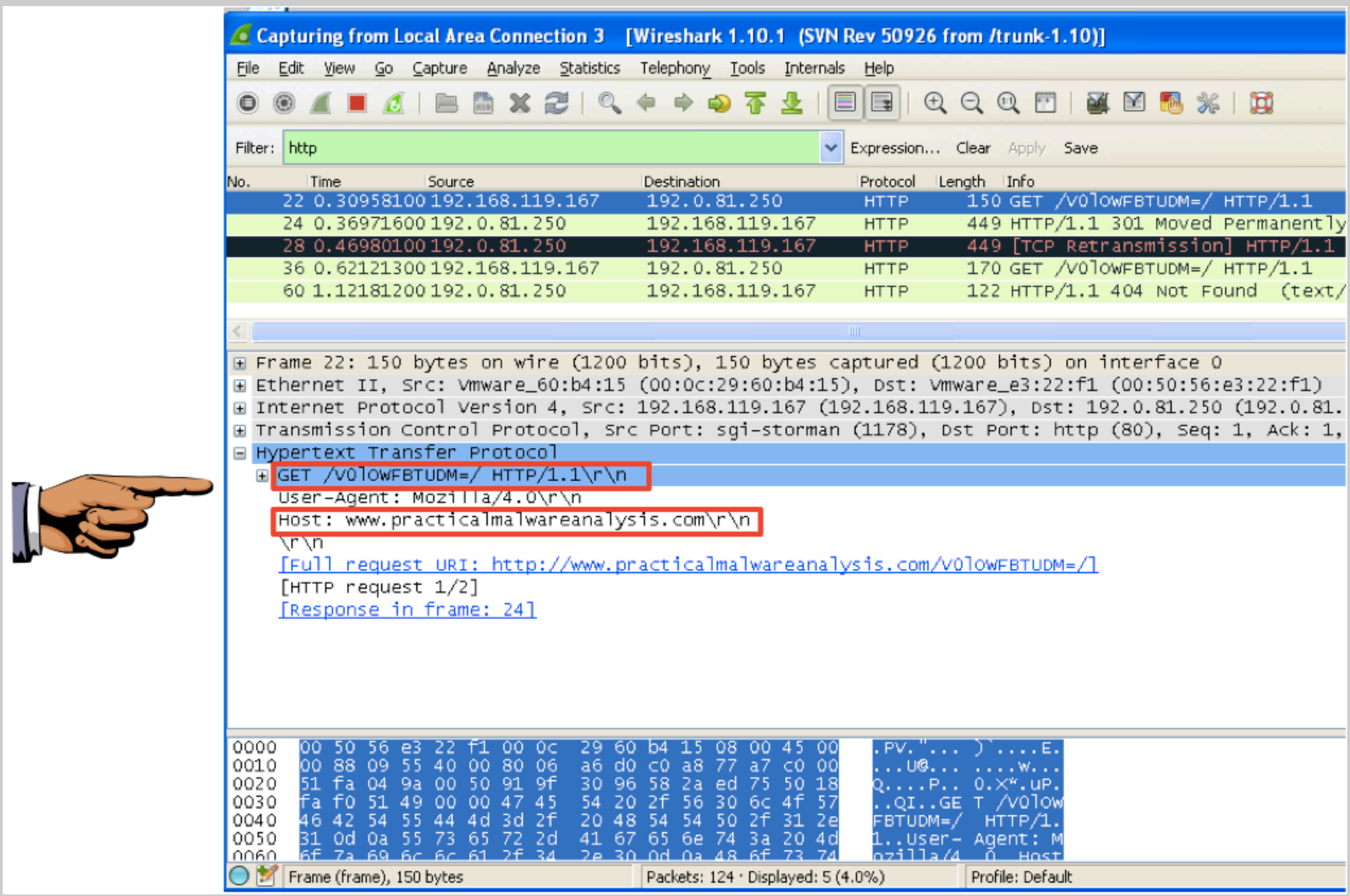
Use either method, and capture a beacon with Wireshark.

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**".

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

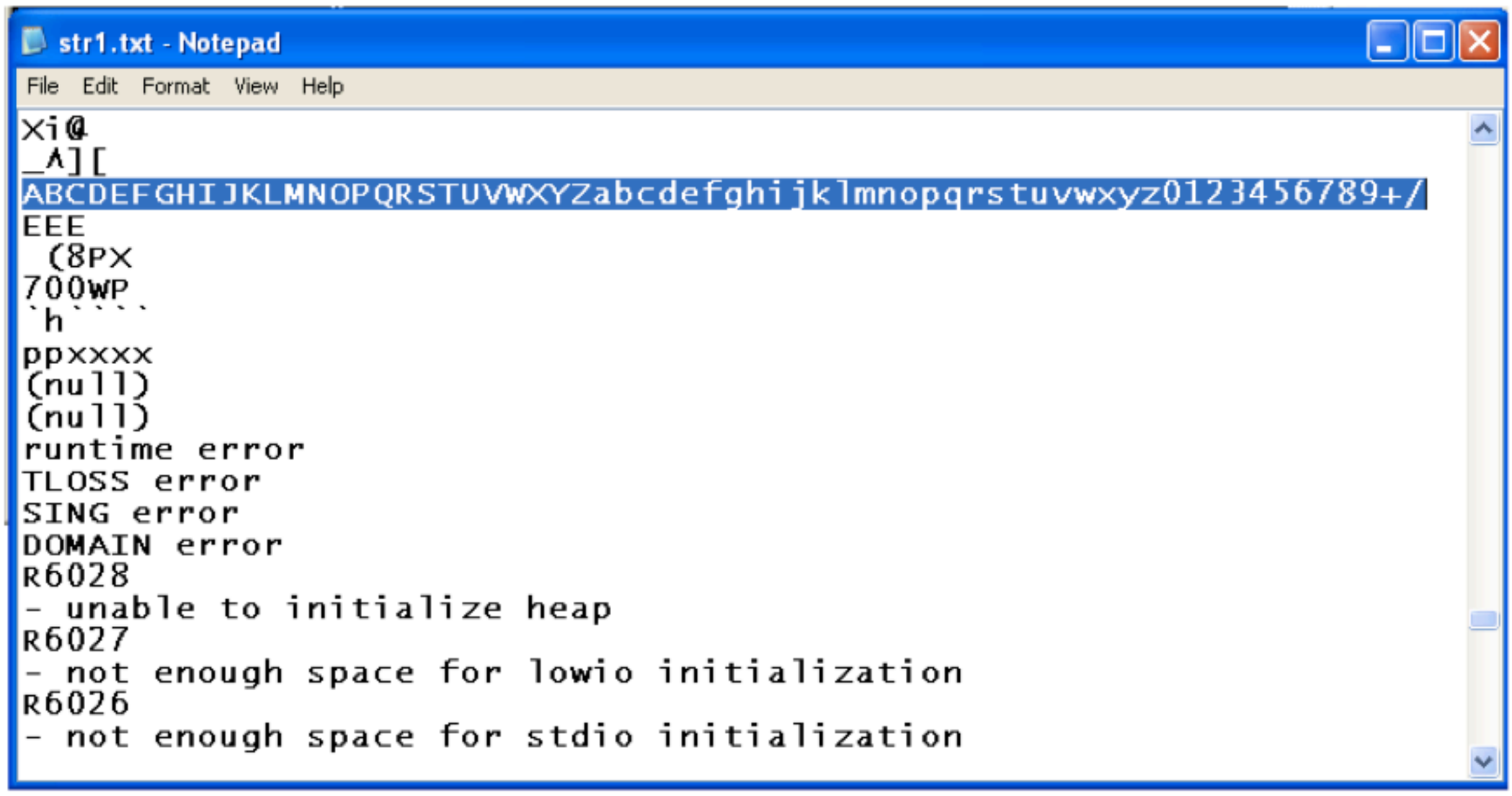


Strings

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

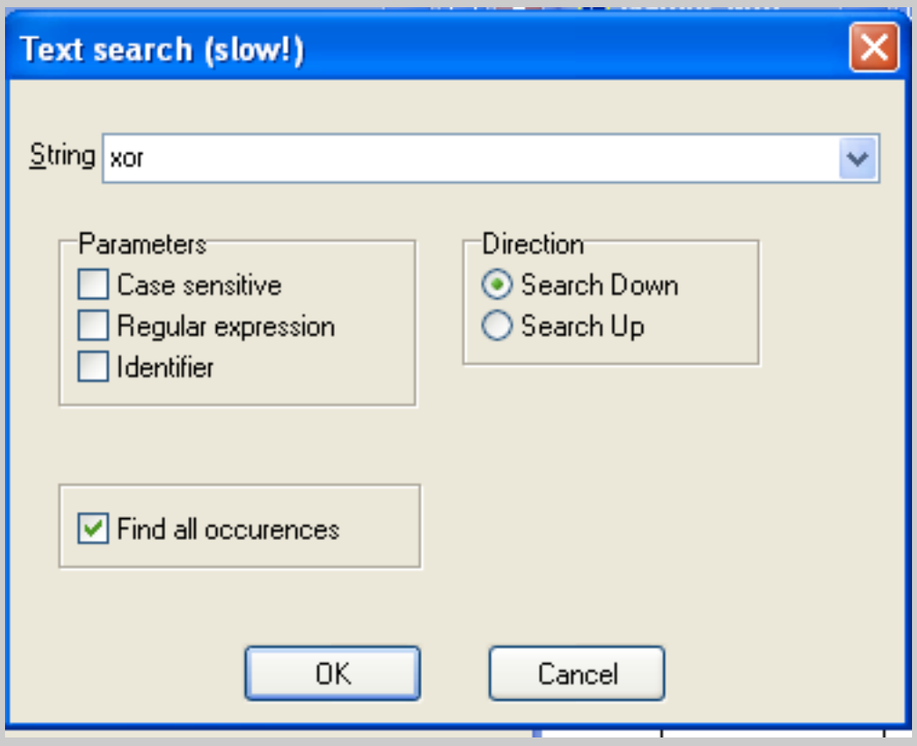
Open **Lab13-01.exe** file in IDA Pro.

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

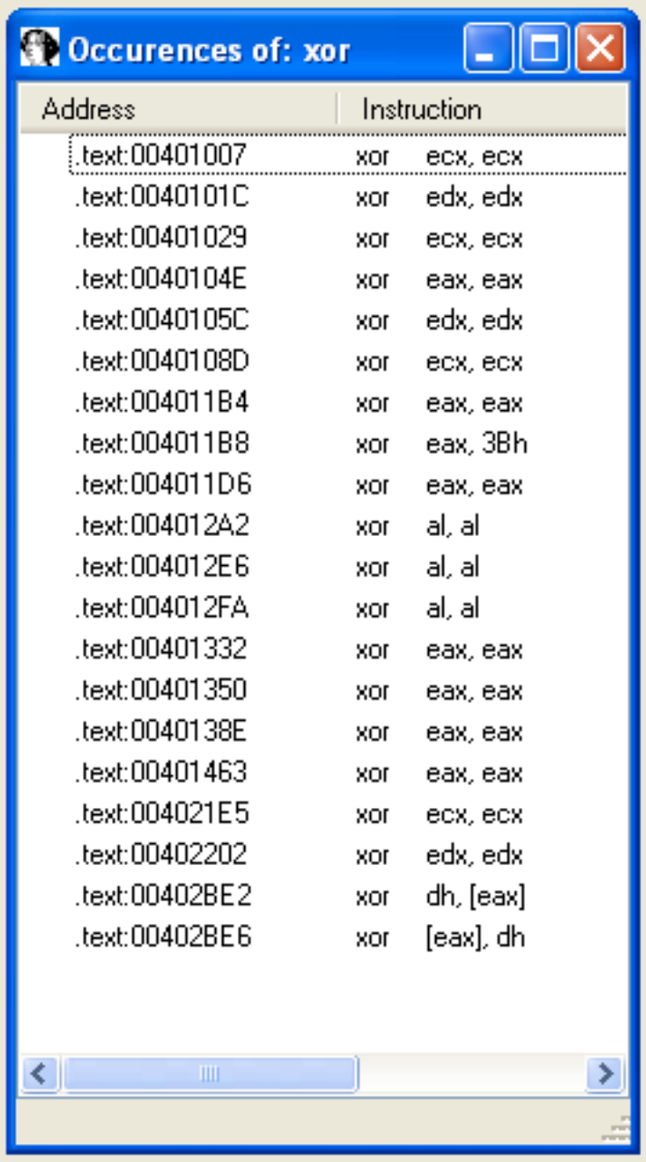
Click in the "IDA View-A" window to make it active.

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

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



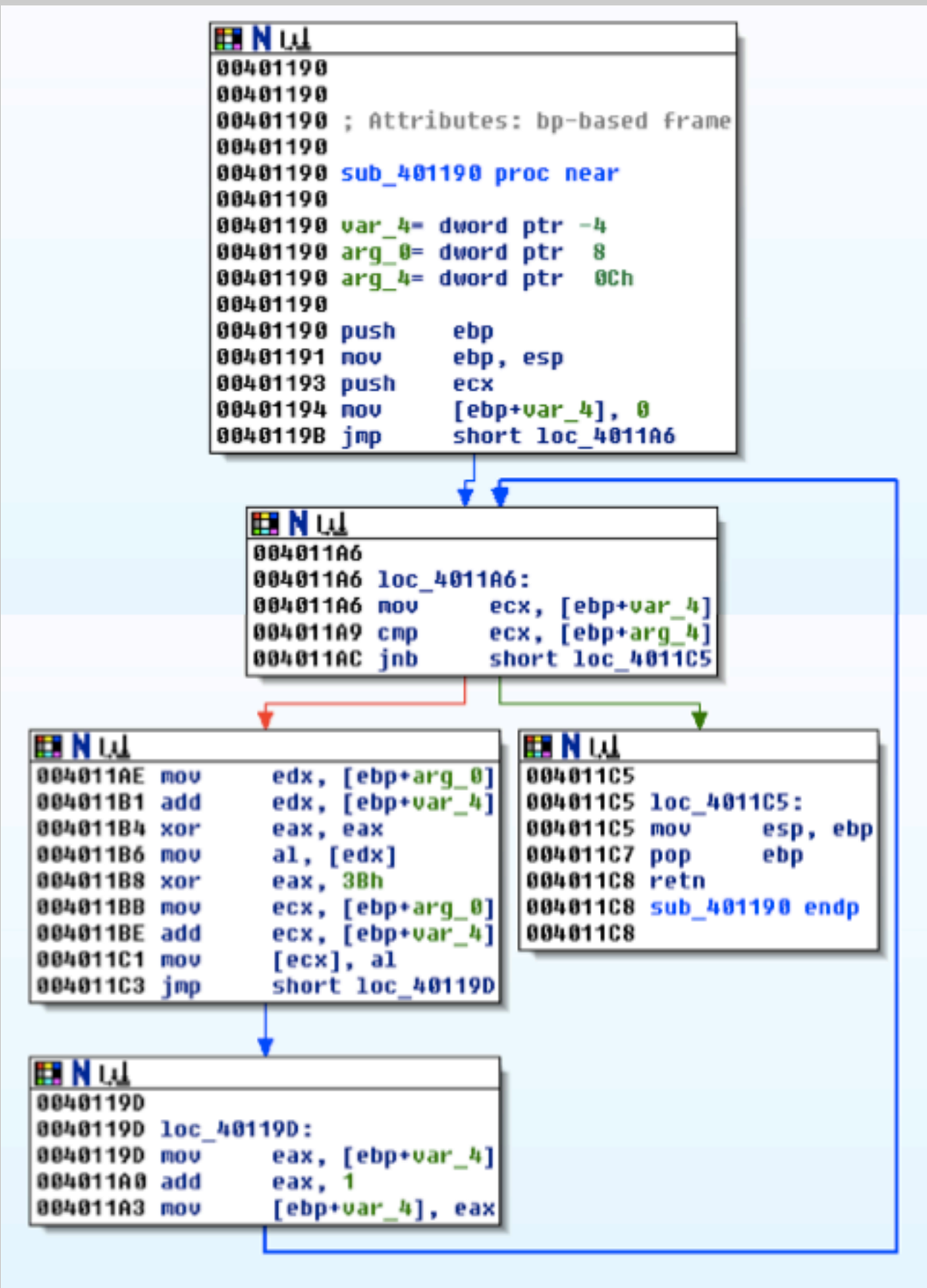
A list of locations using the XOR command appears, as shown below.



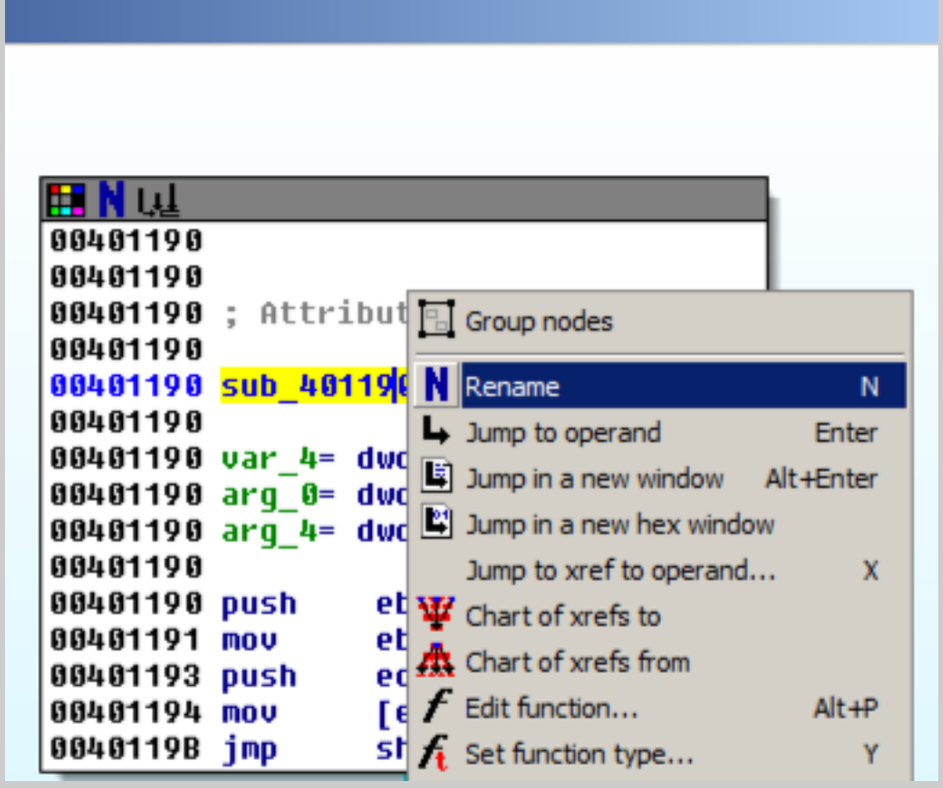
Double-click the **xor eax, 3Bh** instruction.

You should see the function shown below.

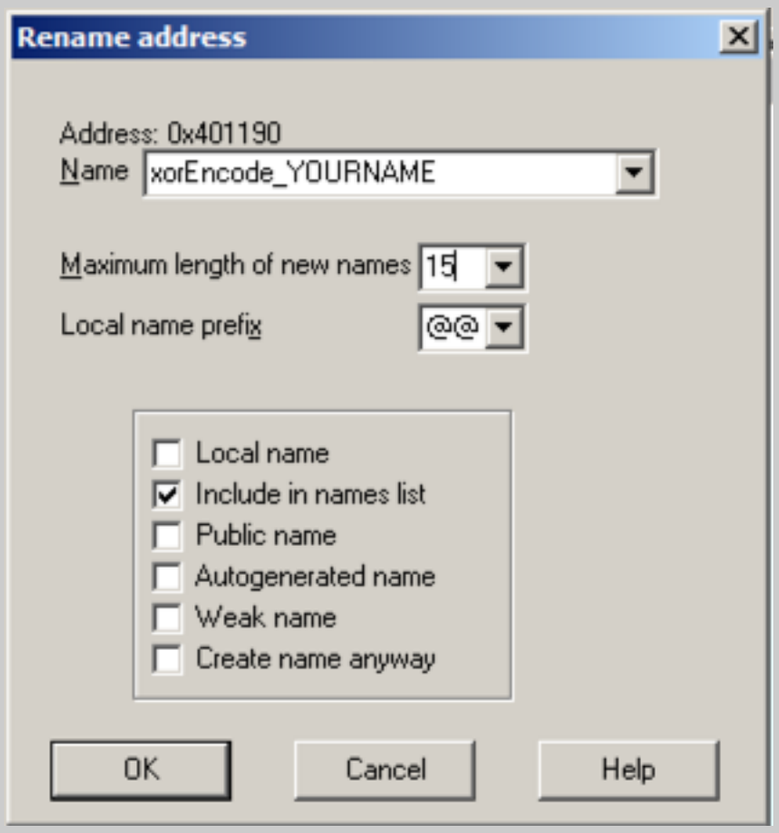
As explained in the book, this function performs xor encoding.



In the top box of the function, right-click **sub_401190** and click **Rename**, as shown below.



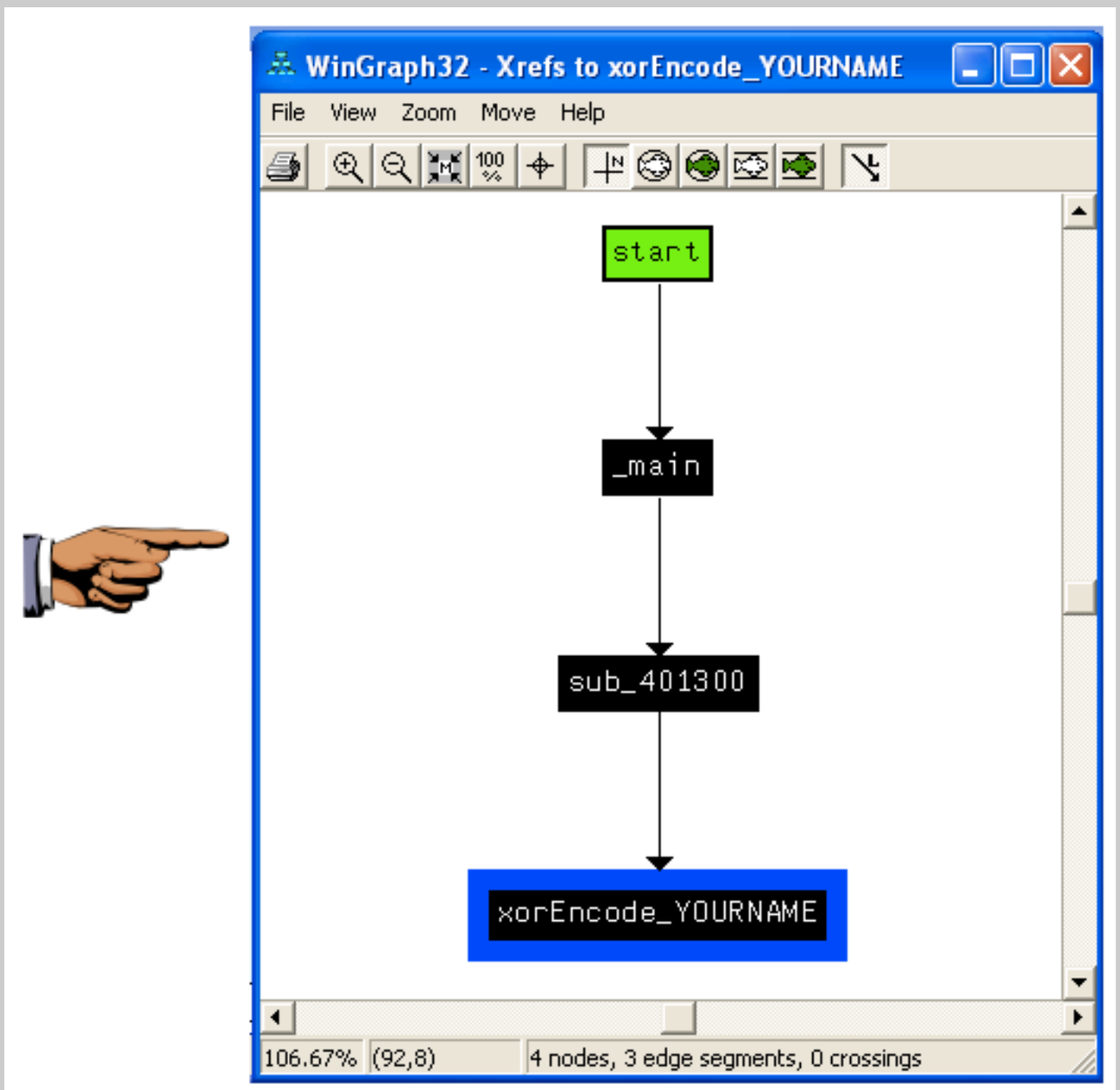
Enter a new name of **xorEncode_YOURNAME**, as shown below, replacing "YOURNAME" with your own name.



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

```
00401339
00401339 loc_401339:                    ; lpType
00401339 push    0Ah
0040133B push    65h                    ; lpName
0040133D mov     eax, [ebp+hModule]
00401340 push    eax                    ; hModule
00401341 call    ds:FindResourceA
00401347 mov     [ebp+hResInfo], eax
0040134A cmp     [ebp+hResInfo], 0
0040134E jnz     short loc_401357
```

```
00401357
00401357 loc_401357:
00401357 mov     ecx, [ebp+hResInfo]
0040135A push    ecx                    ; hResInfo
0040135B mov     edx, [ebp+hModule]
0040135E push    edx                    ; hModule
0040135F call    ds:SizeofResource
00401365 mov     [ebp+dwBytes], eax
00401368 mov     eax, [ebp+dwBytes]
0040136B push    eax                    ; dwBytes
0040136C push    40h                    ; uFlags
0040136E call    ds:GlobalAlloc
00401374 mov     [ebp+var_4], eax
00401377 mov     ecx, [ebp+hResInfo]
0040137A push    ecx                    ; hResInfo
0040137B mov     edx, [ebp+hModule]
0040137E push    edx                    ; hModule
0040137F call    ds:LoadResource
00401385 mov     [ebp+hResData], eax
00401388 cmp     [ebp+hResData], 0
0040138C jnz     short loc_401392
```

```
00401350 xor     eax, eax
00401352 jmp     loc_4013E9
```

```
0040138E xor     eax, eax
00401390 jmp     short loc_4013E9
```

```
00401392
00401392 loc_401392:
00401392 mov     eax, [ebp+hResData]
00401395 push    eax                    ; hResData
00401396 call    ds:LockResource
0040139C mov     [ebp+var_10], eax
0040139F mov     ecx, [ebp+dwBytes]
004013A2 push    ecx
004013A3 mov     edx, [ebp+var_10]
004013A6 push    edx
004013A7 call    xorEncode_YOURNAME
004013AC add     esp, 8
004013AF mov     eax, [ebp+var_10]
004013B2 jmp     short loc_4013E9
```

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.

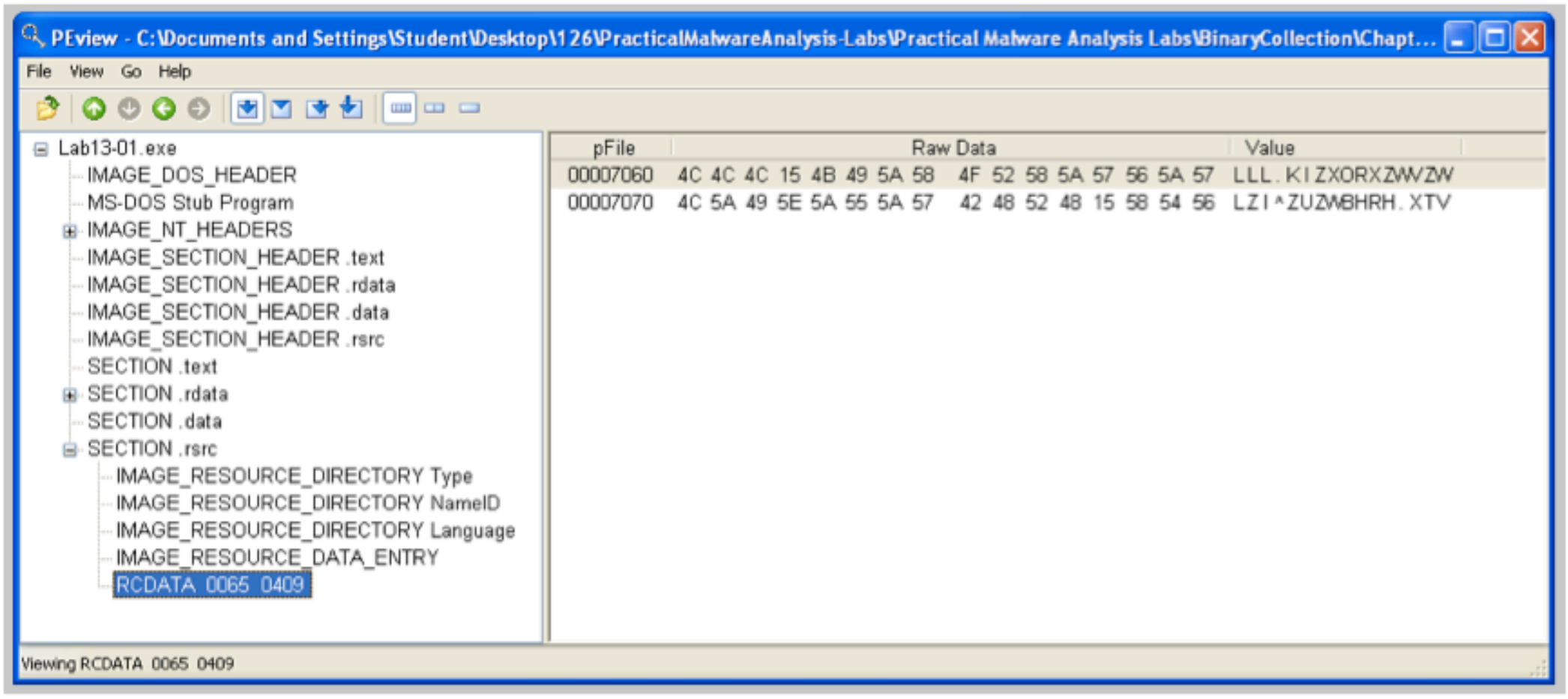
PEview

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.

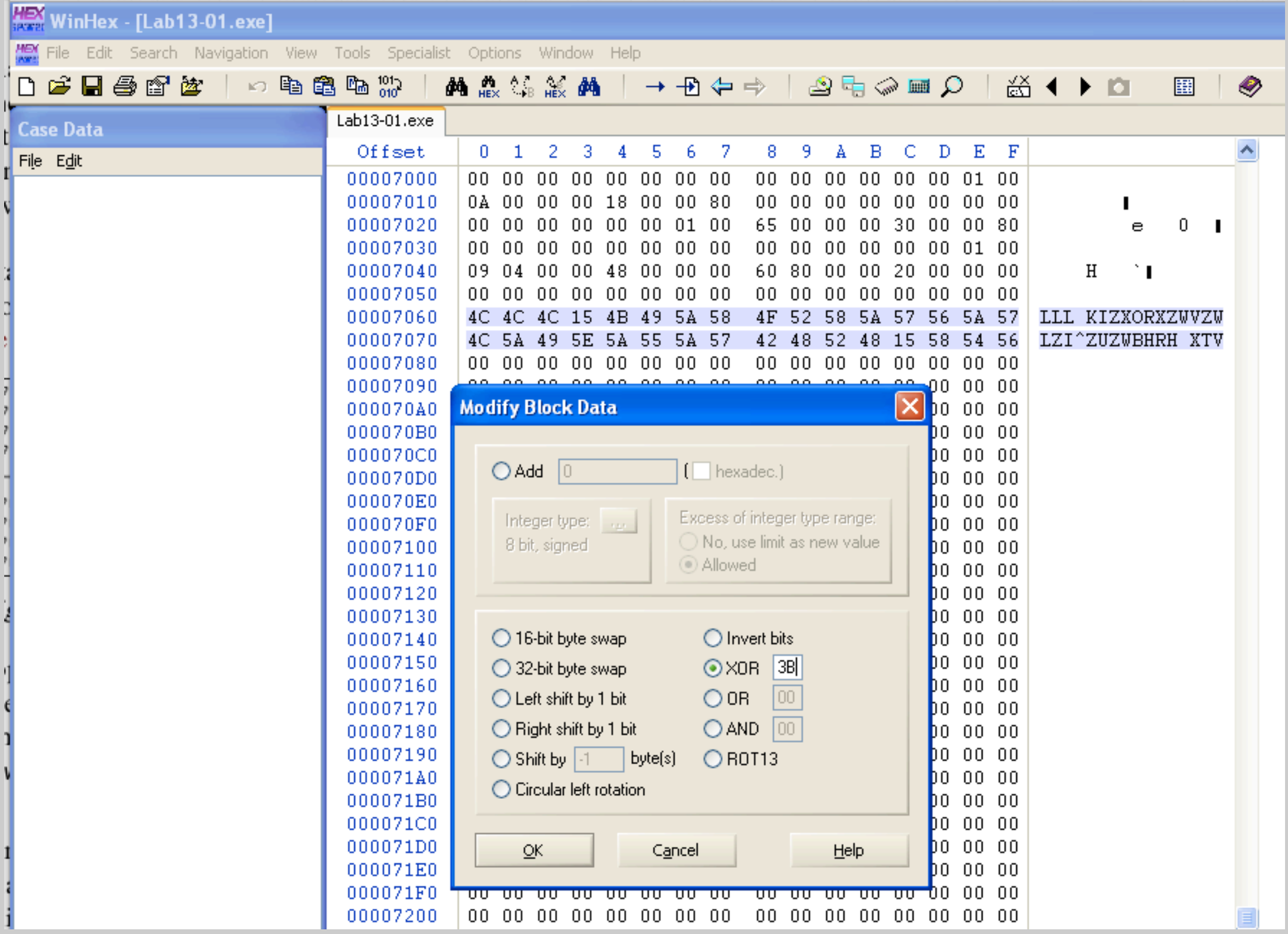
Right-click the **winhex.zip** file, click "**Extract All**", and click **Extract**.

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.

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

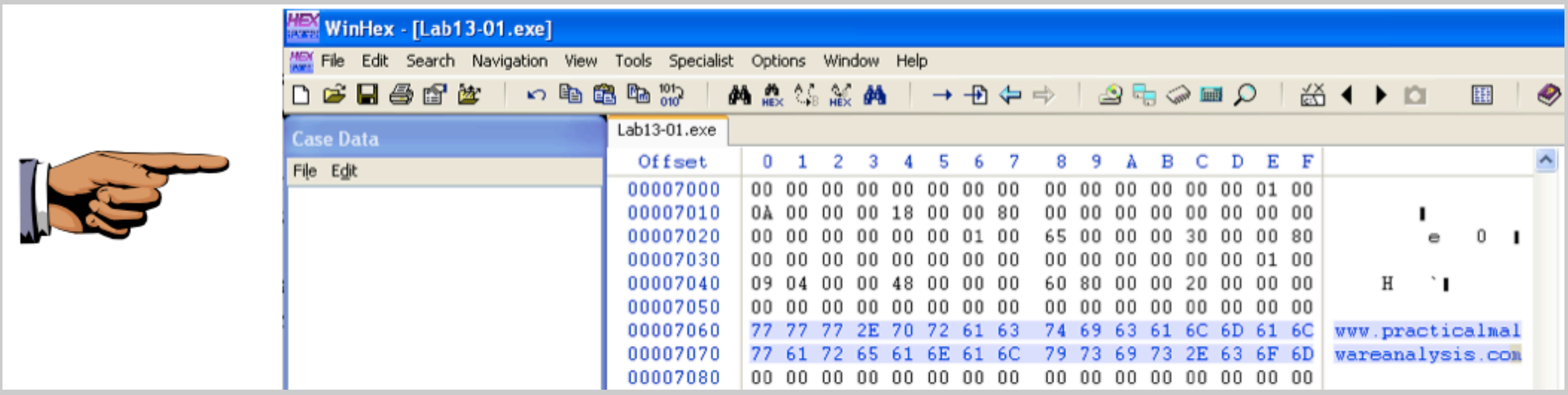
Click **Edit**, "**Modify Data**".

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**".

Turning in your Project

Email the images to cnit.126sam@gmail.com with the subject line: **Proj 16 from YOUR NAME**

Last modified 5-2-16