**Lab 14: Data Encoding**

**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.

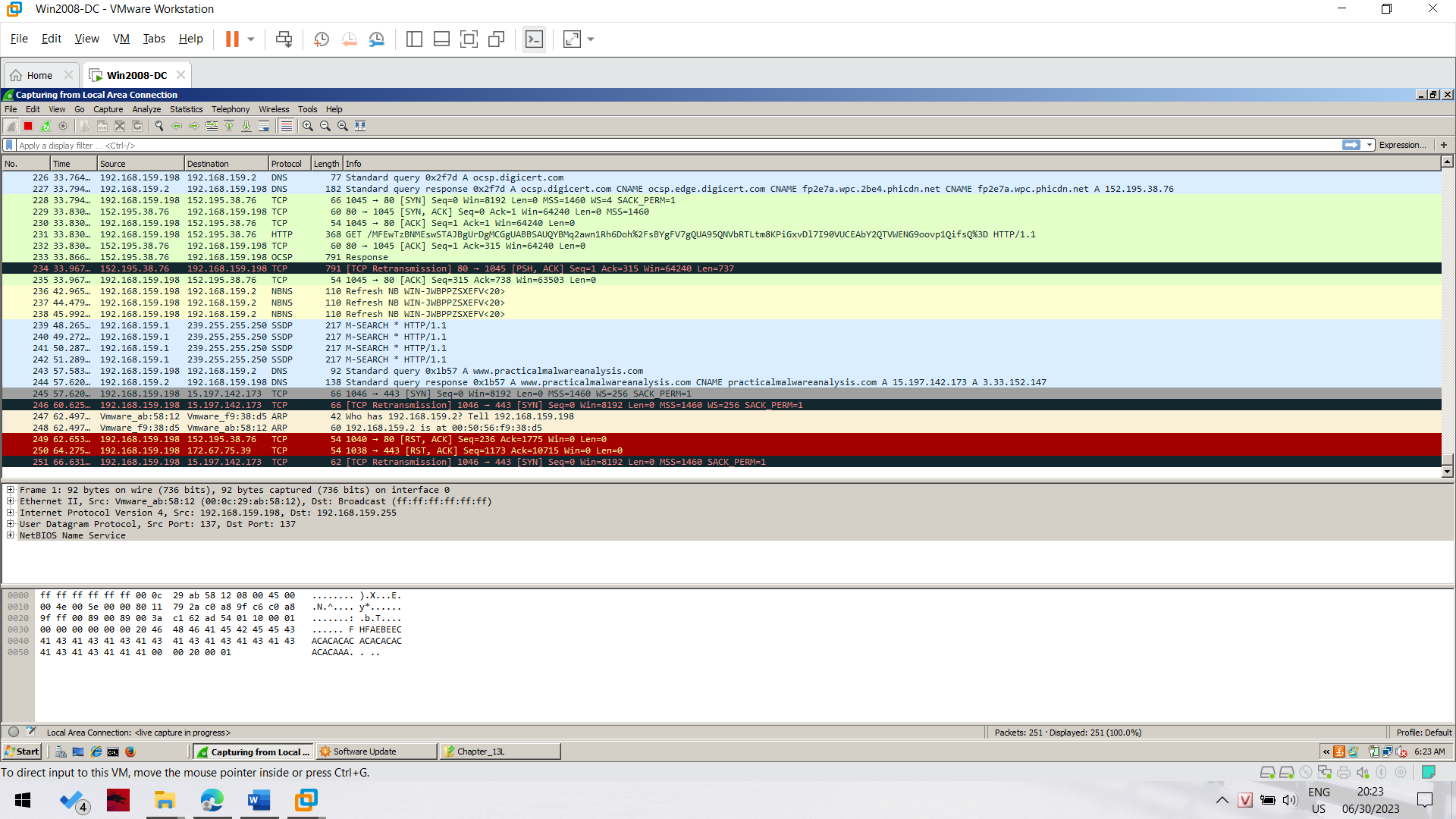
Launch the Lab13-01.exe file.

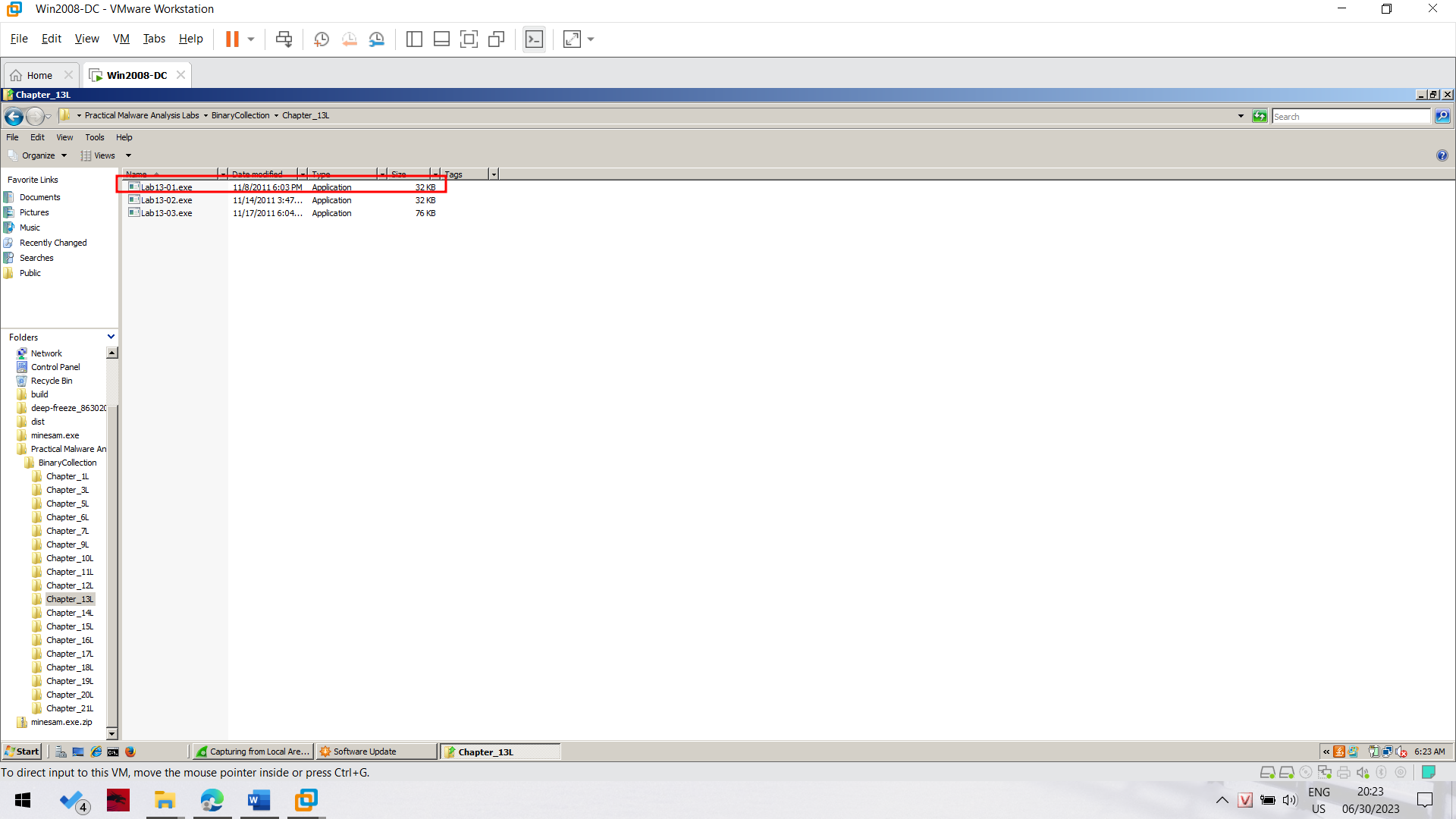
Use either method, and capture a beacon with Wireshark.

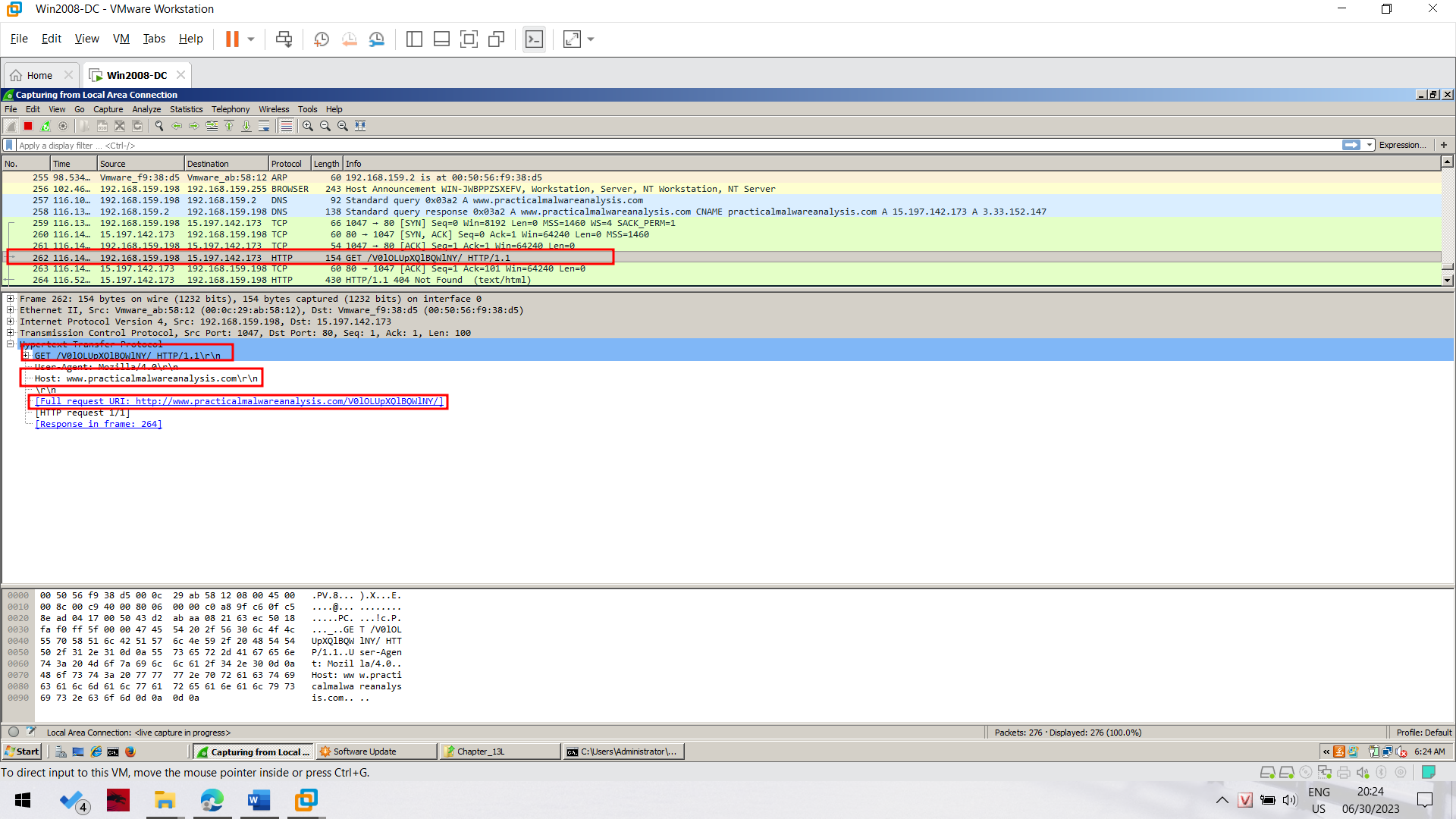
Adjust the wireshark window to show these two features, highlighted below:

GET /randomletters/ HTTP/1.1

Host: www.practicalmalwareanalysis.com



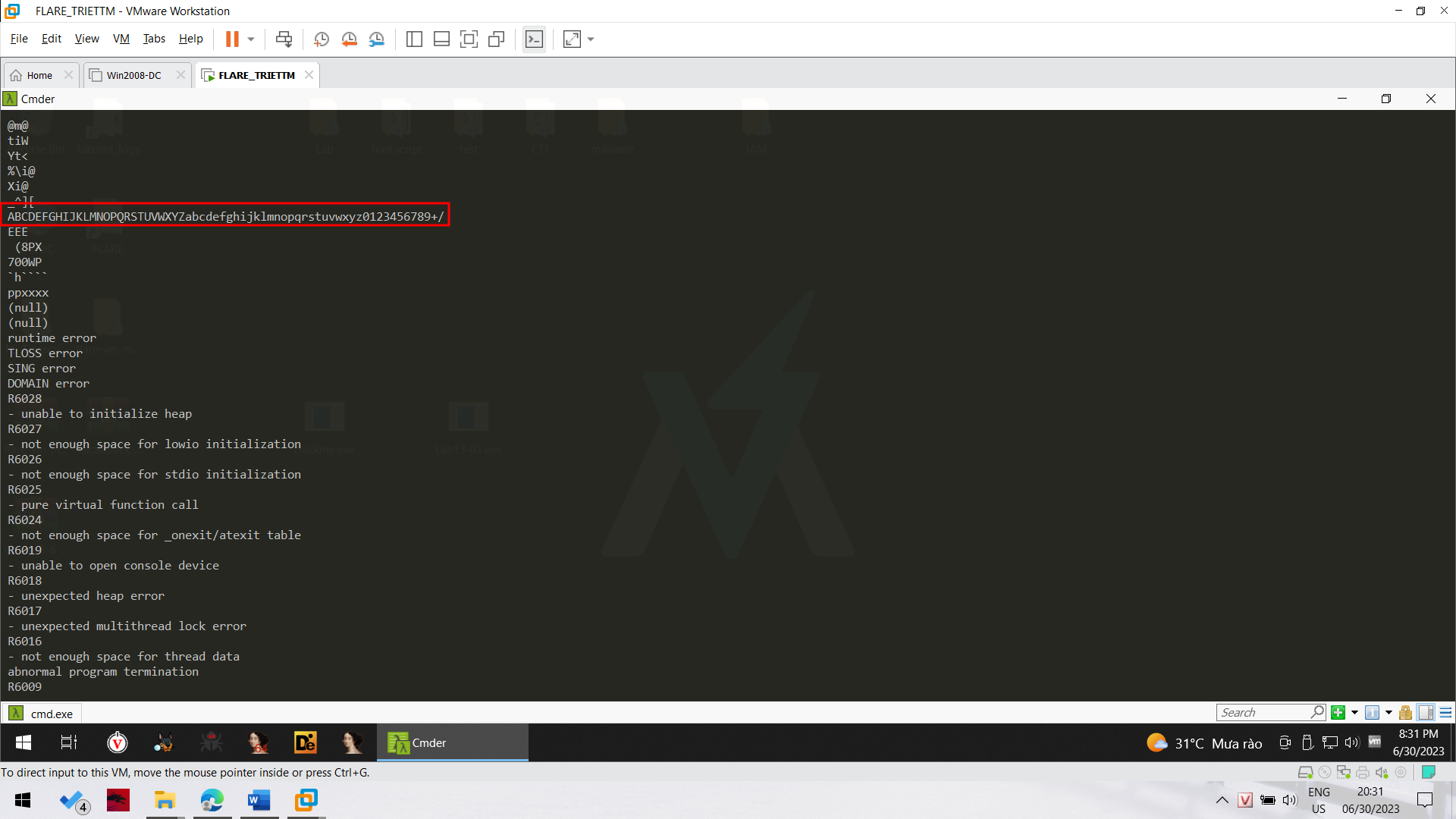




**Strings**

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.



**IDA Pro**

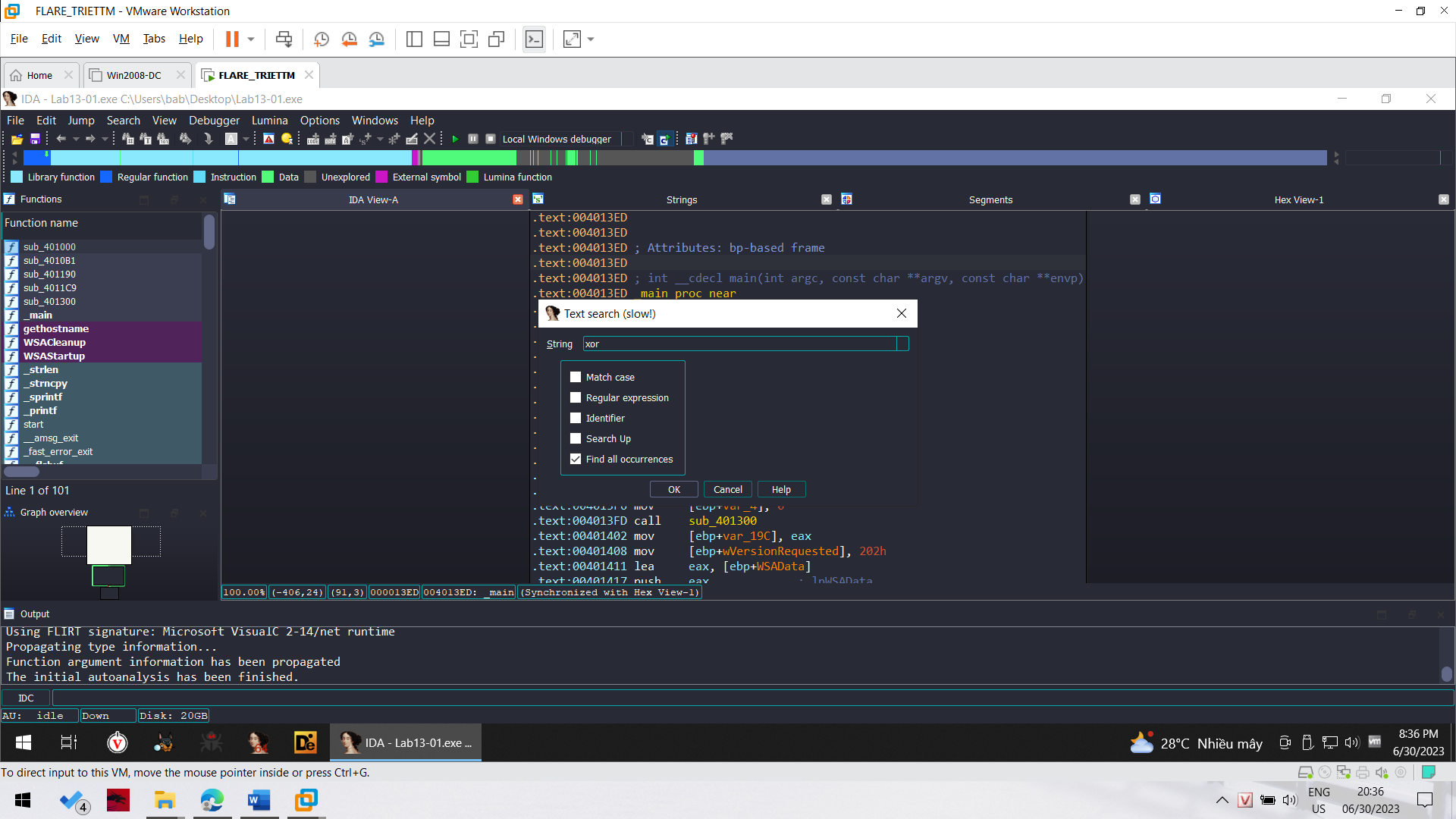
Open Lab13-01.exe file in IDA Pro.

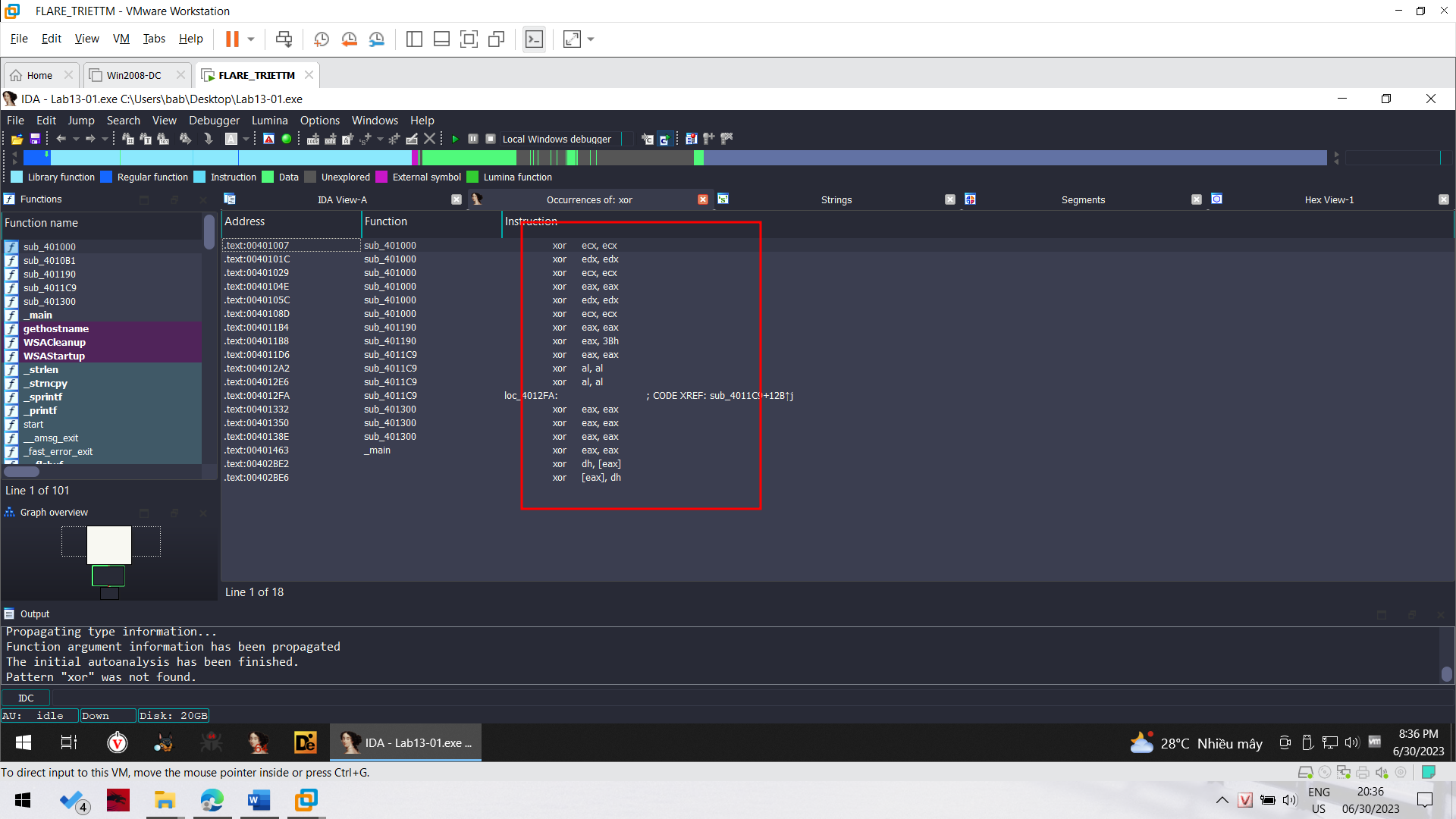
Click Options, General. Check "Line Prefixes" and click OK.

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

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

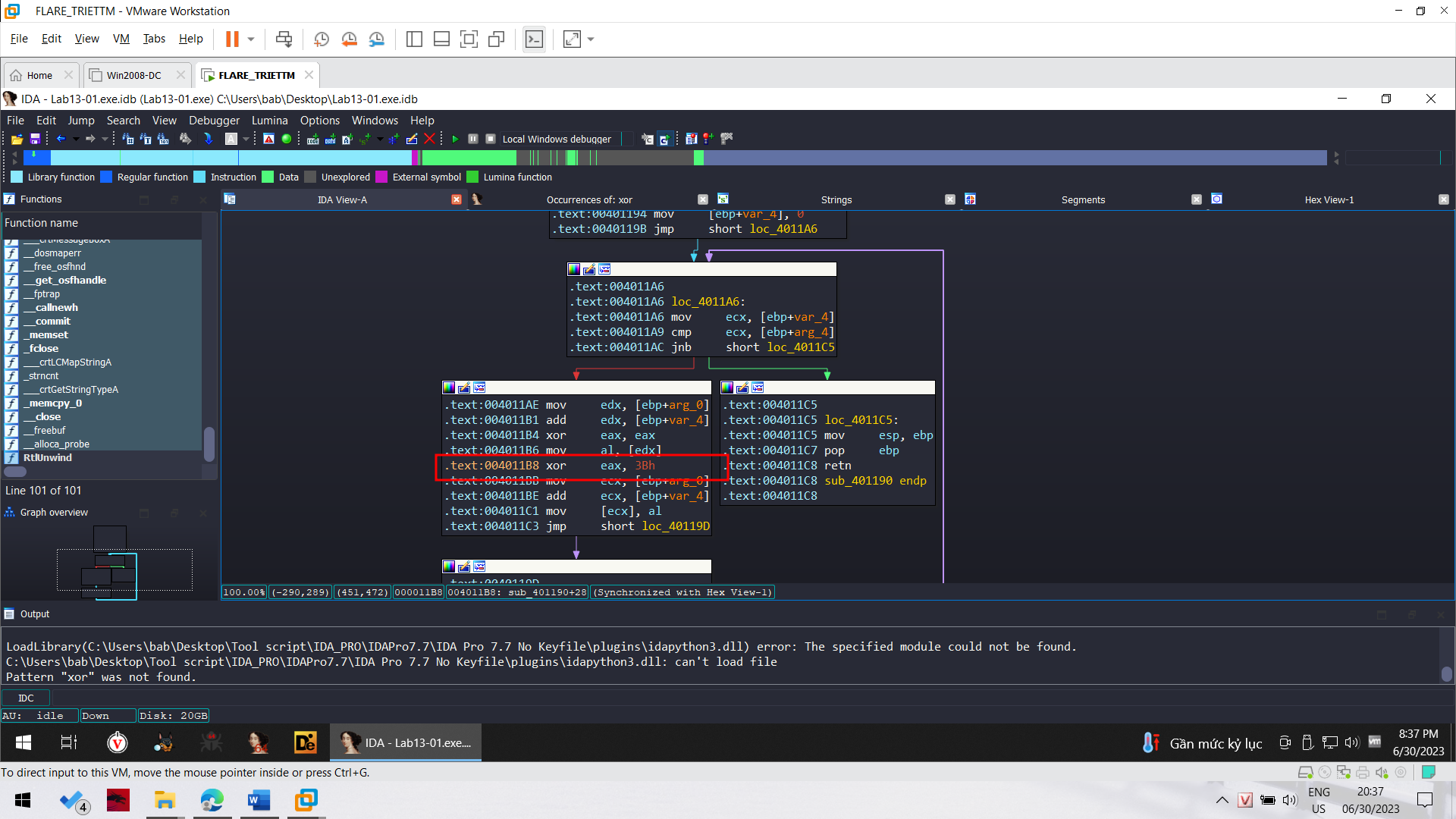
In the Text Search dialog, enter xor and check "Find all occurrences", as shown below:



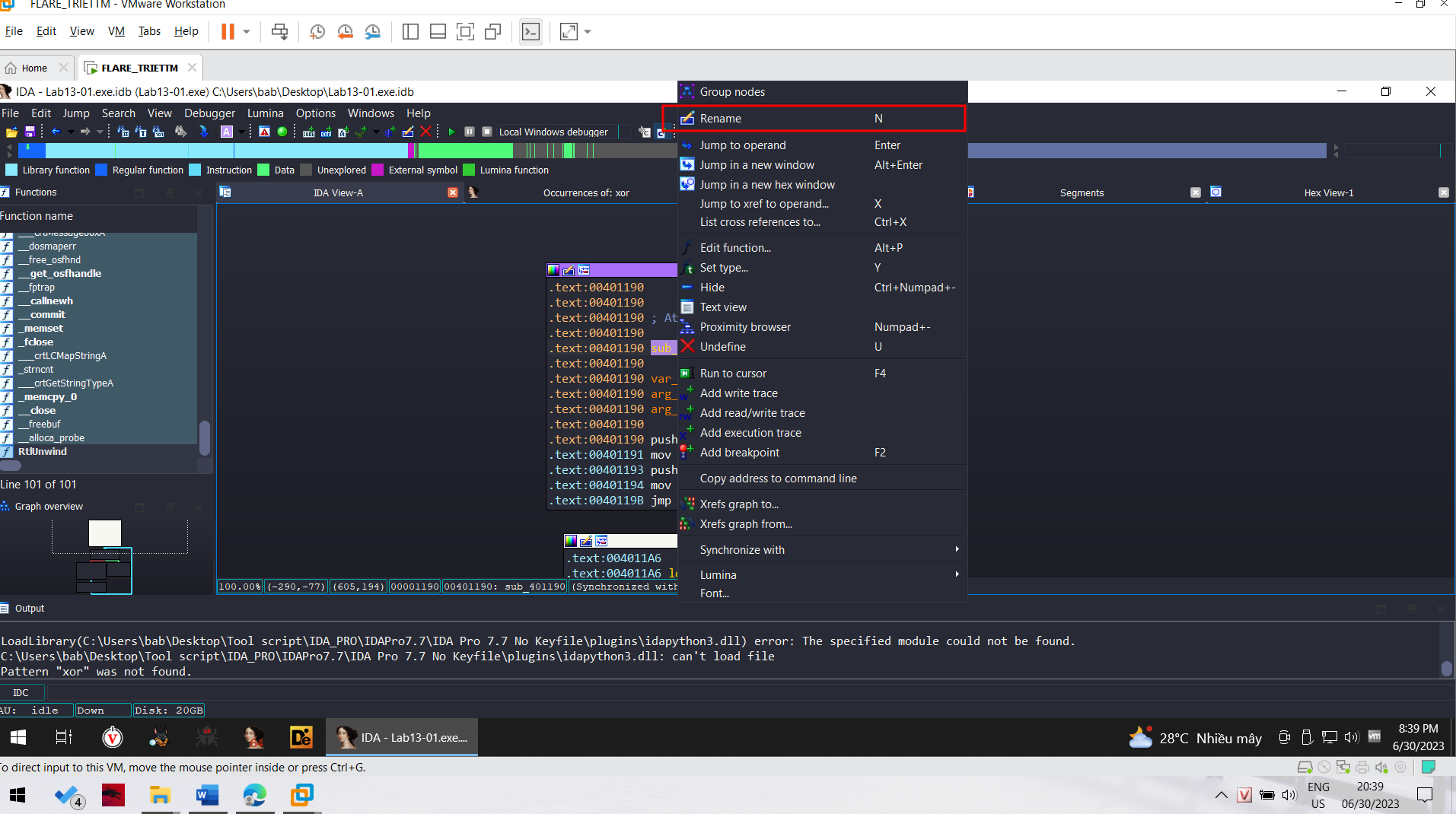


Double-click the xor eax, 3Bh instruction.

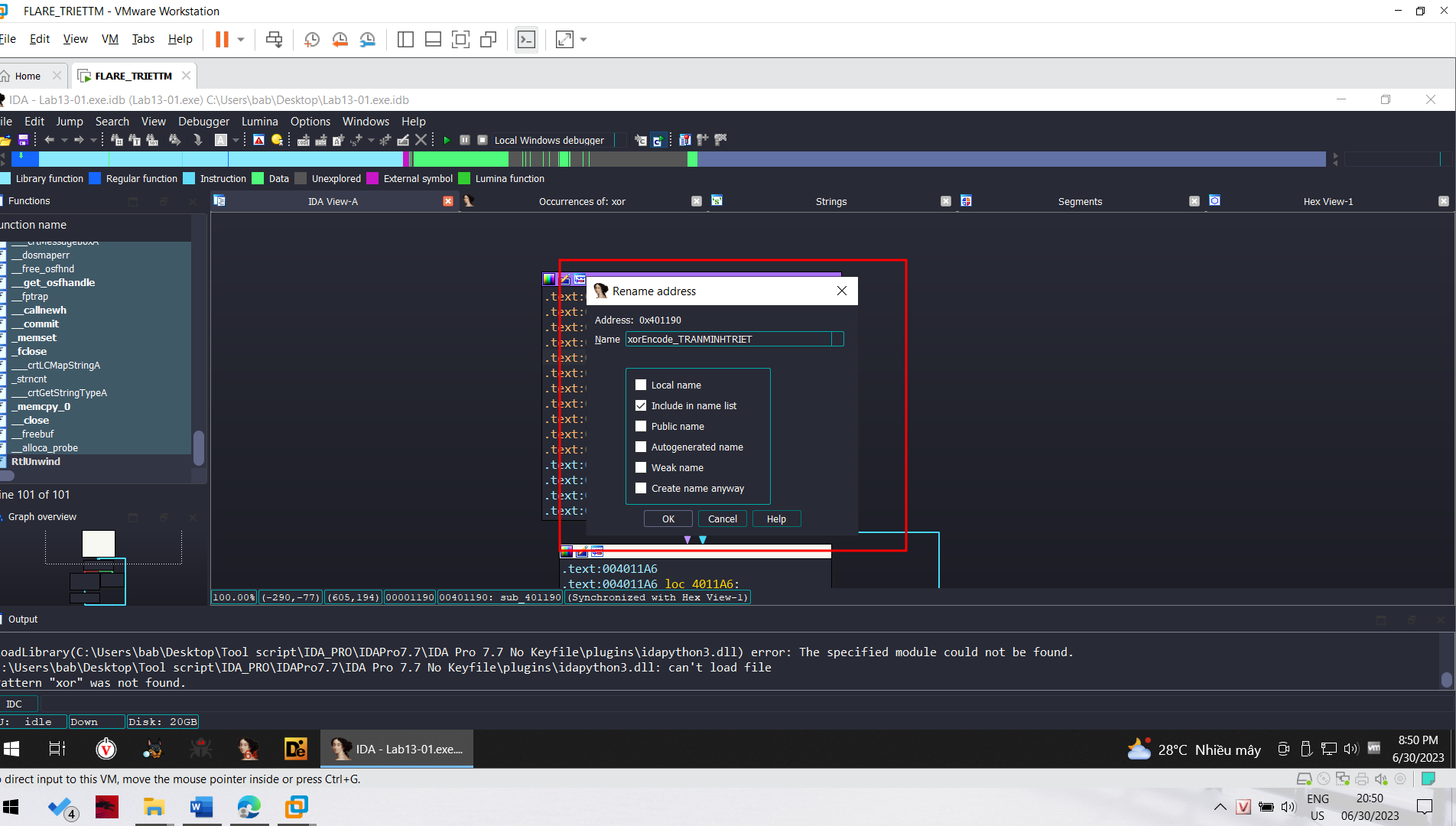
You should see the function shown below.

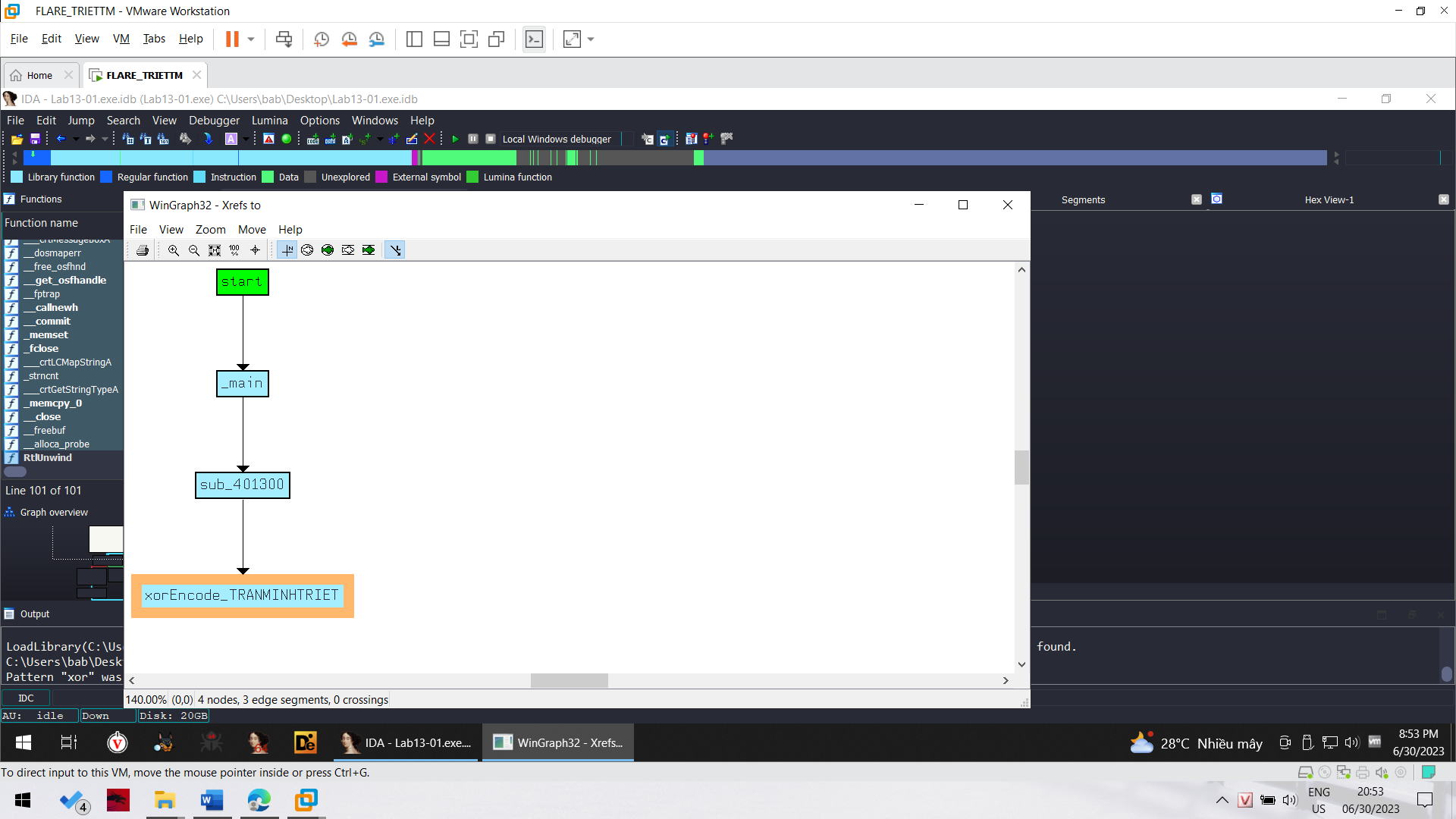
As explained in the book, this function performs xor encoding. 

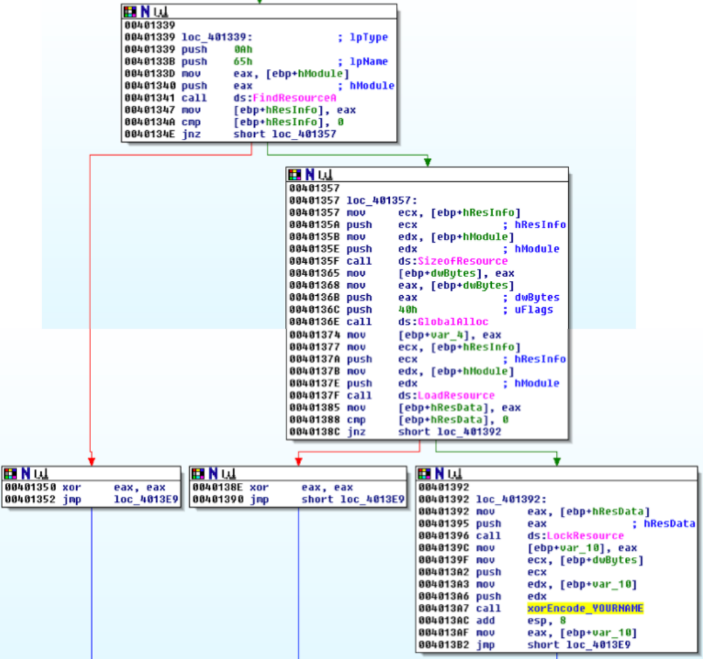
In the top box of the function, right-click sub\_401190 and click Rename, as shown below



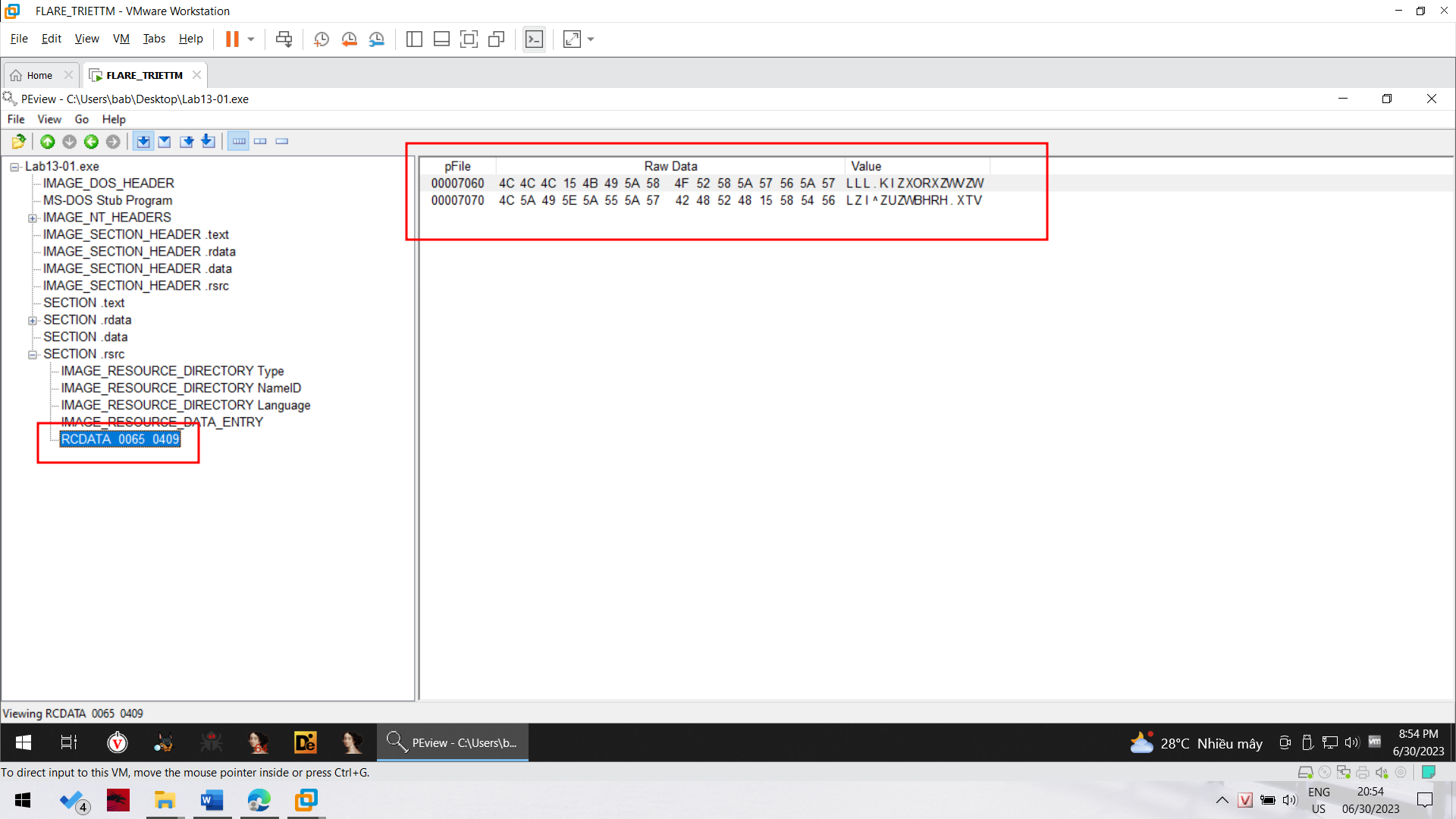
Enter a new name of xorEncode\_YOURNAME, as shown below, replacing "YOURNAME" with your own name.







PEview



WinHex

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:

