PROJ 16: Data Encoding

Prof. Alberto LaCava

CY -640

MALWARE ANALYSIS & DEFENSE

Nikhil Patel

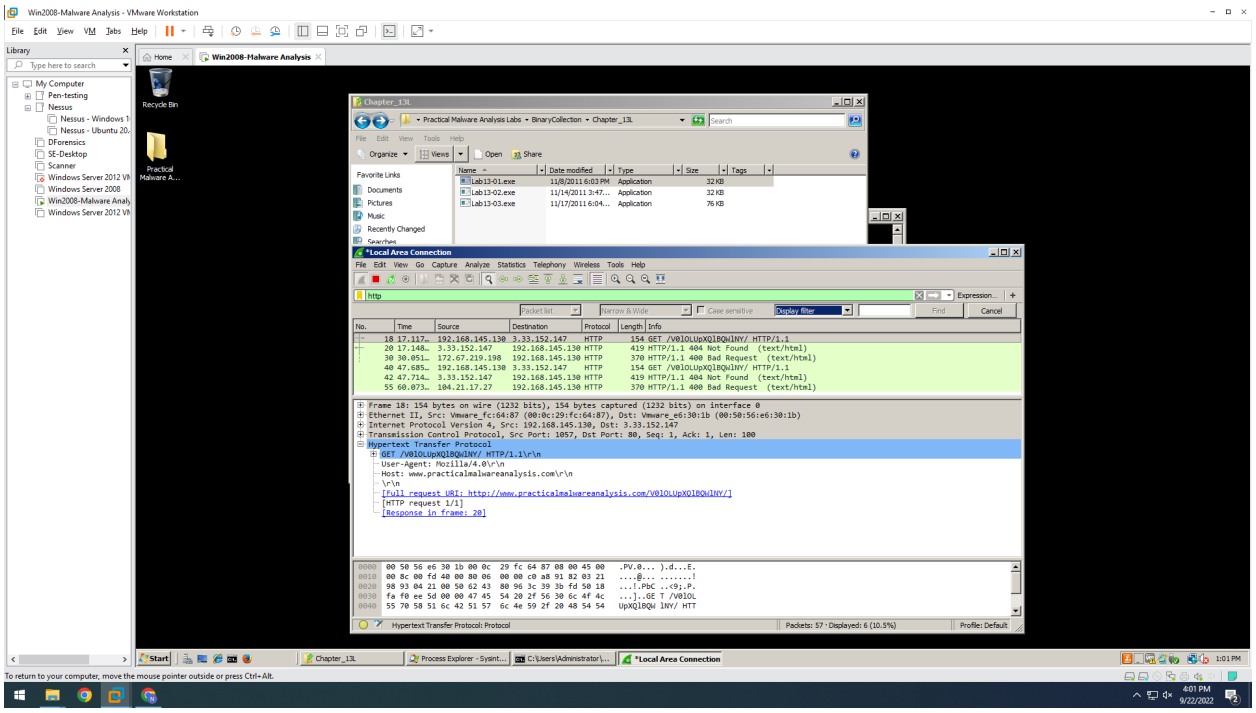
10/25/2022

Introduction: In this lab, we will encode data utilizing various strategies such as beacons, strings, and IDA Pro tools.

Procedure :

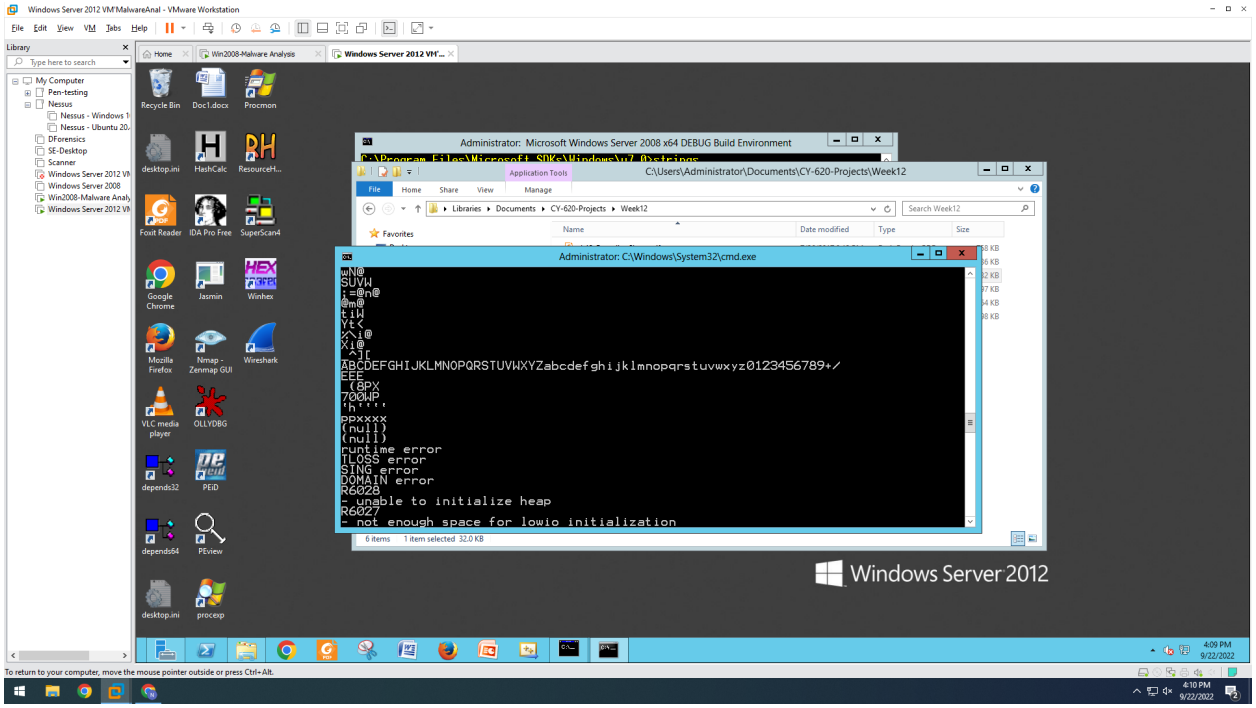
Beacons

- Launch the Lab13-01.exe file in windows XP.
- Open the Wireshark and capture the beacon.
- Go to filter and type HTTP and hit capture.



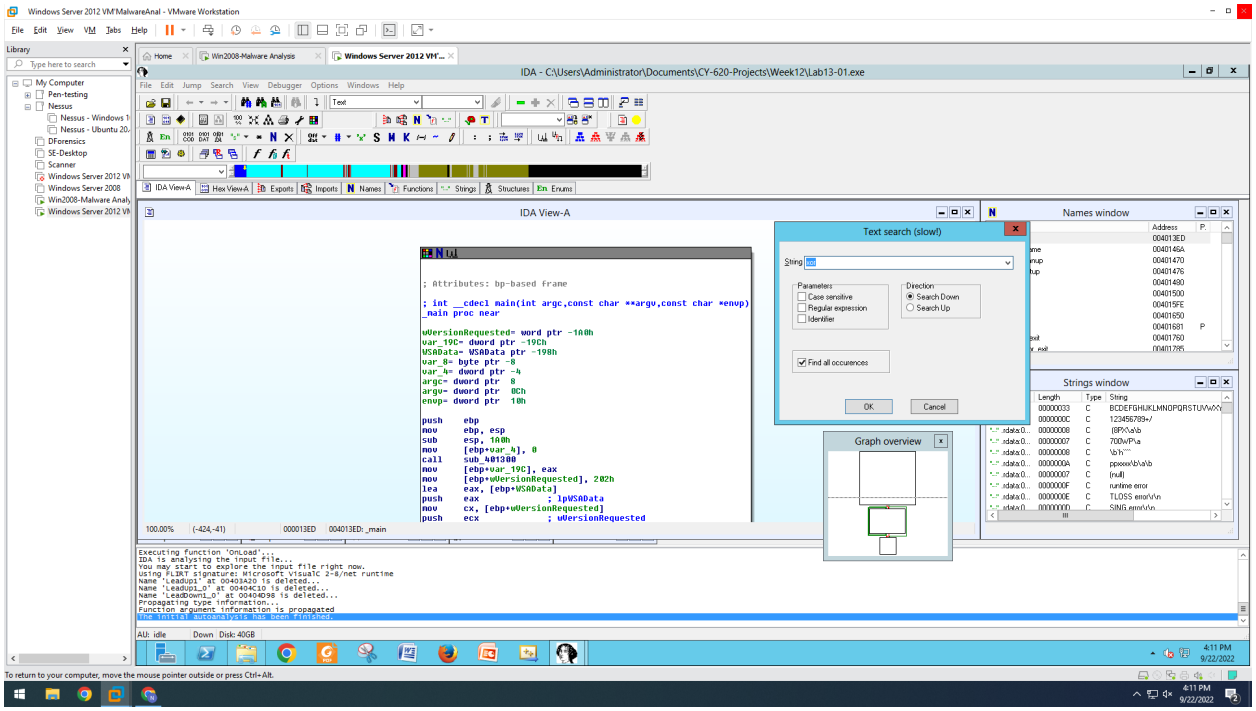
Strings

- Now we will examine the strings in the Lab13-01.exe file.

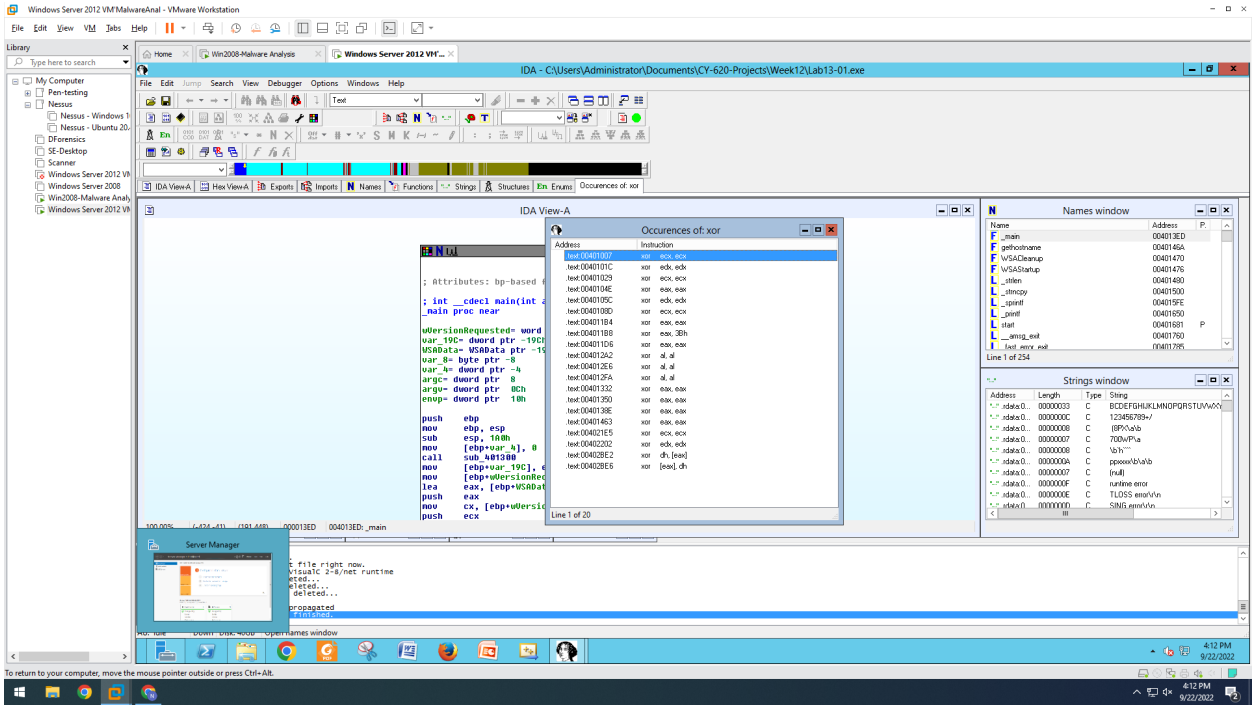


IDA Pro

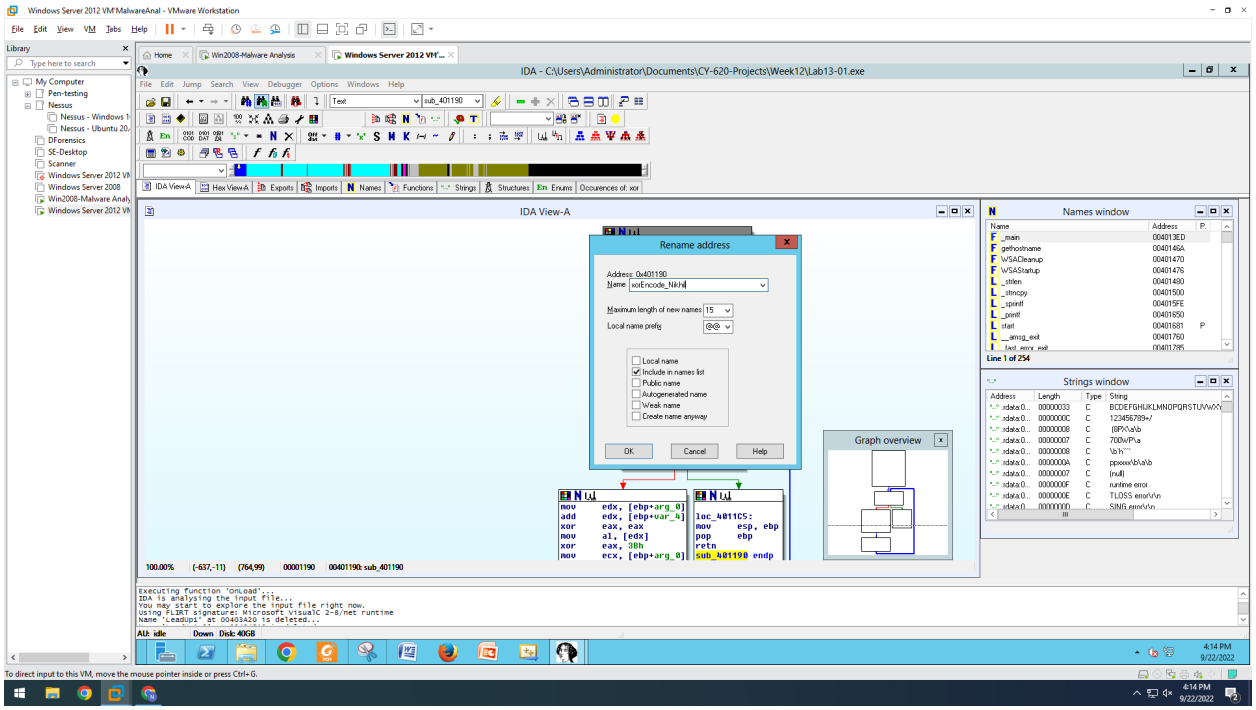
- Now open the Lab13-01.exe file in the IDA Pro.
- Click options>General, tick the line prefixes and Ok.
- Click the IDA View-A and then from the menu bar click Search>text.
- In the Empty string type “xor” and check Find all Occurrences and hit ok.



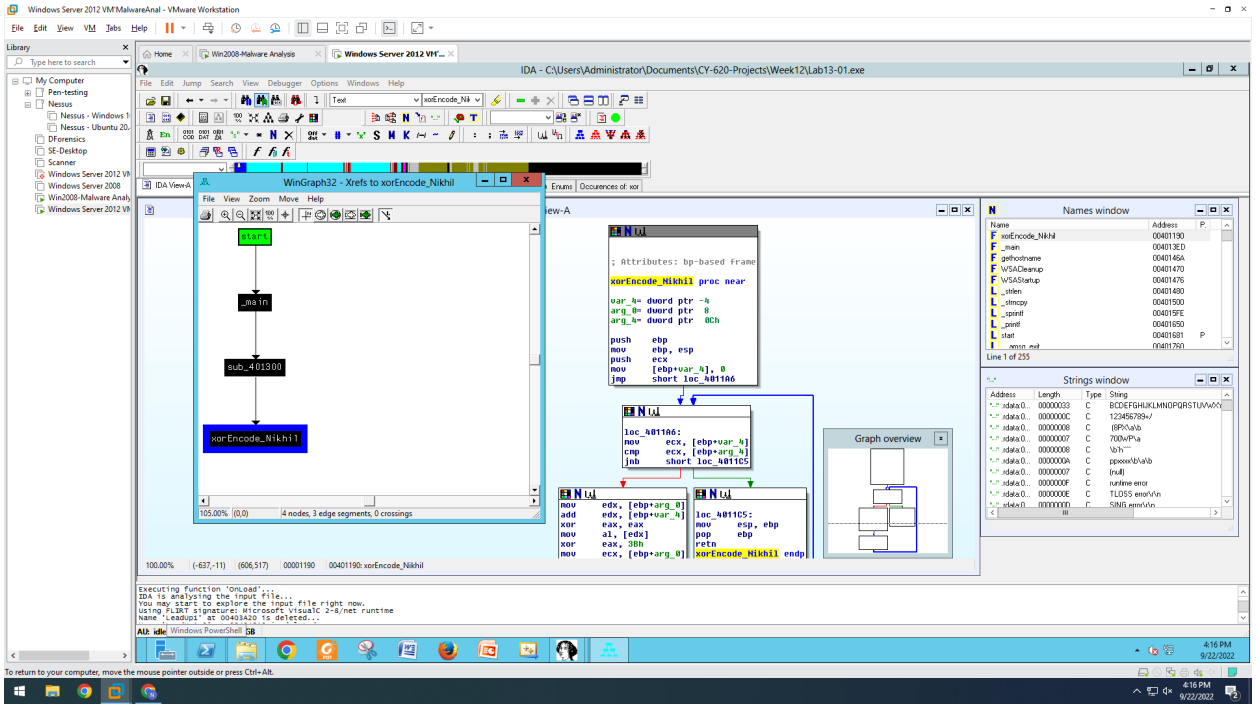
- Now you will see the list of xor's command, double click the xor eax, 3Bh instruction.



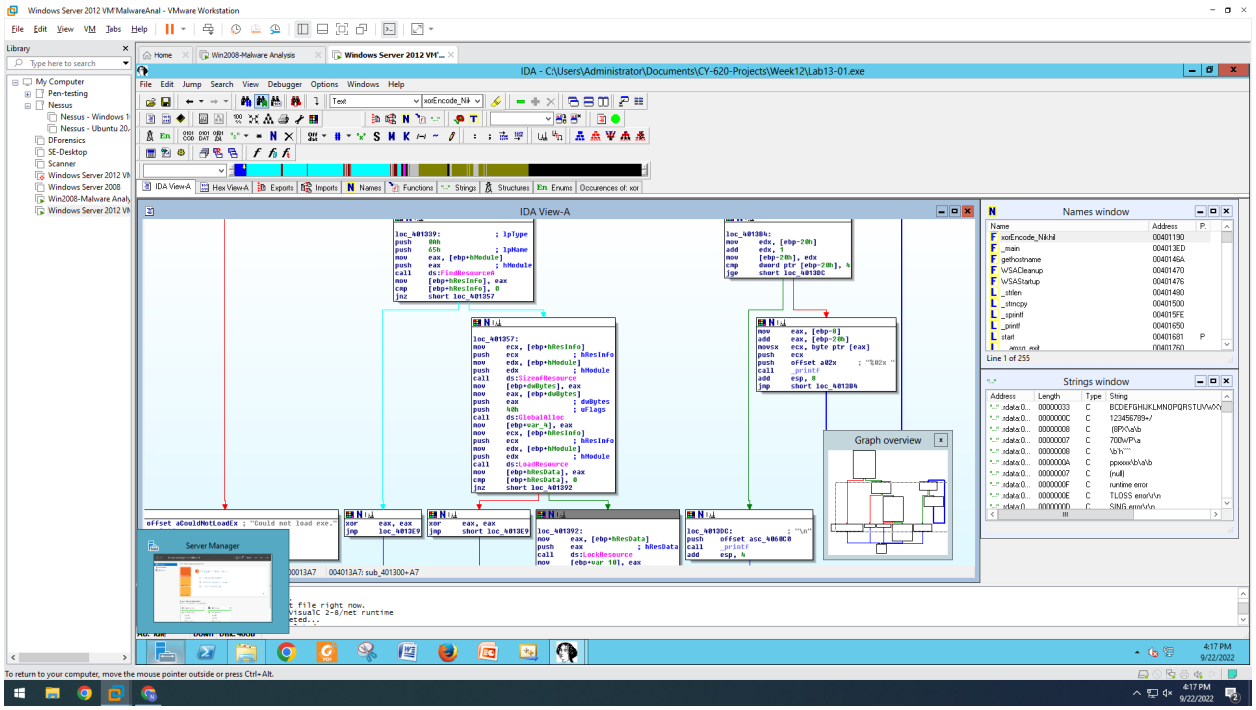
- Now you see the XOR encodings and search for the sub_401190 right click on it and rename it to xorEncode_Nikhil and click the chart of xrefs to.



- Take a screenshot of that chart and save it.

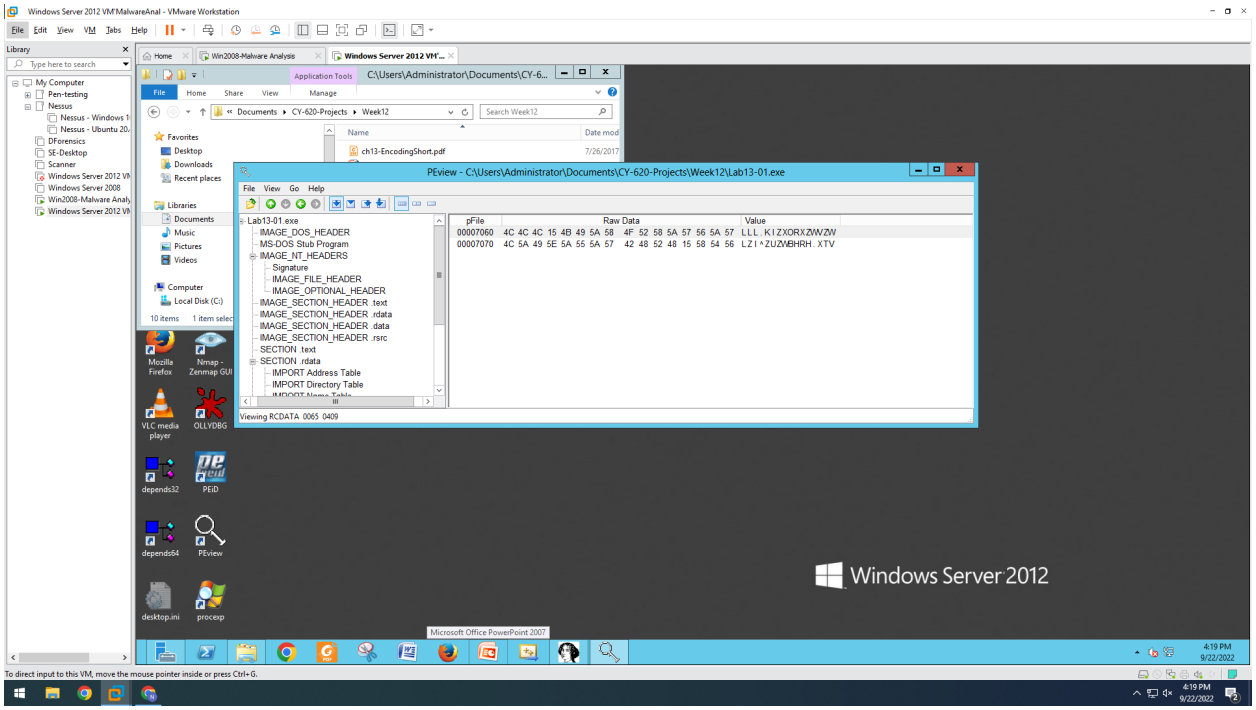


- Now close the chart and right click on xorEncode_Nikhil and click on Jump to xref to operand.. And hit ok.



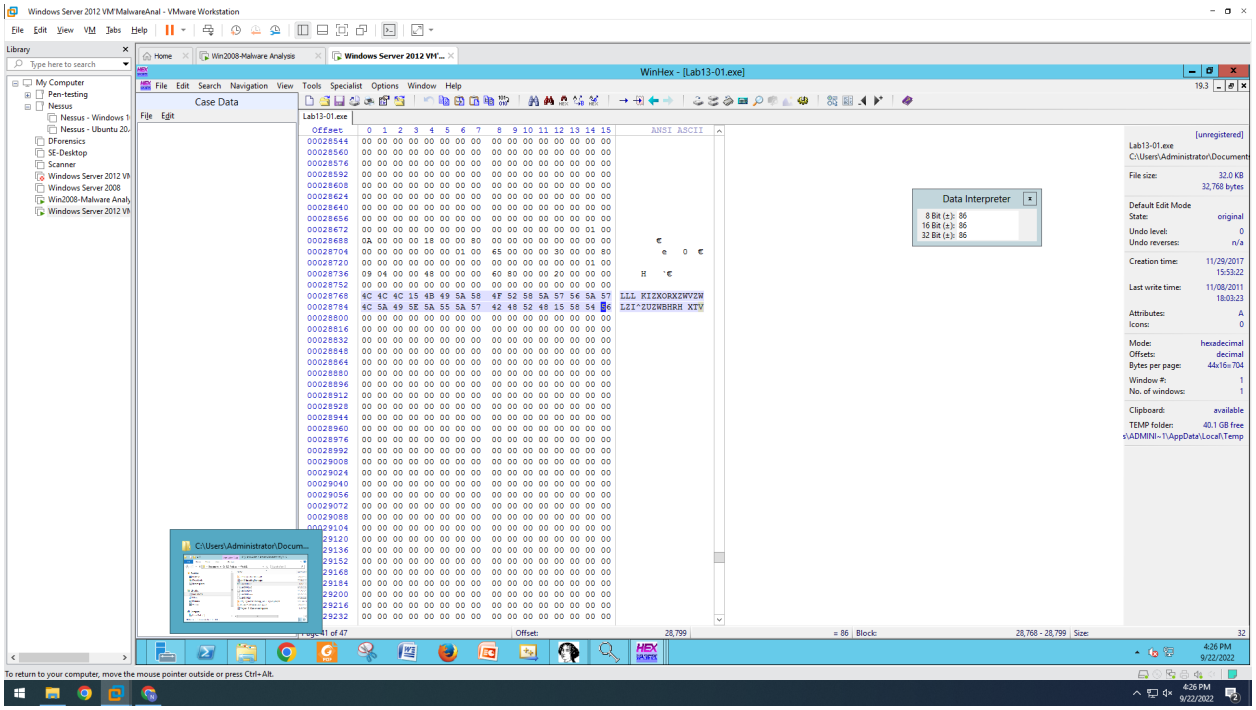
PEview

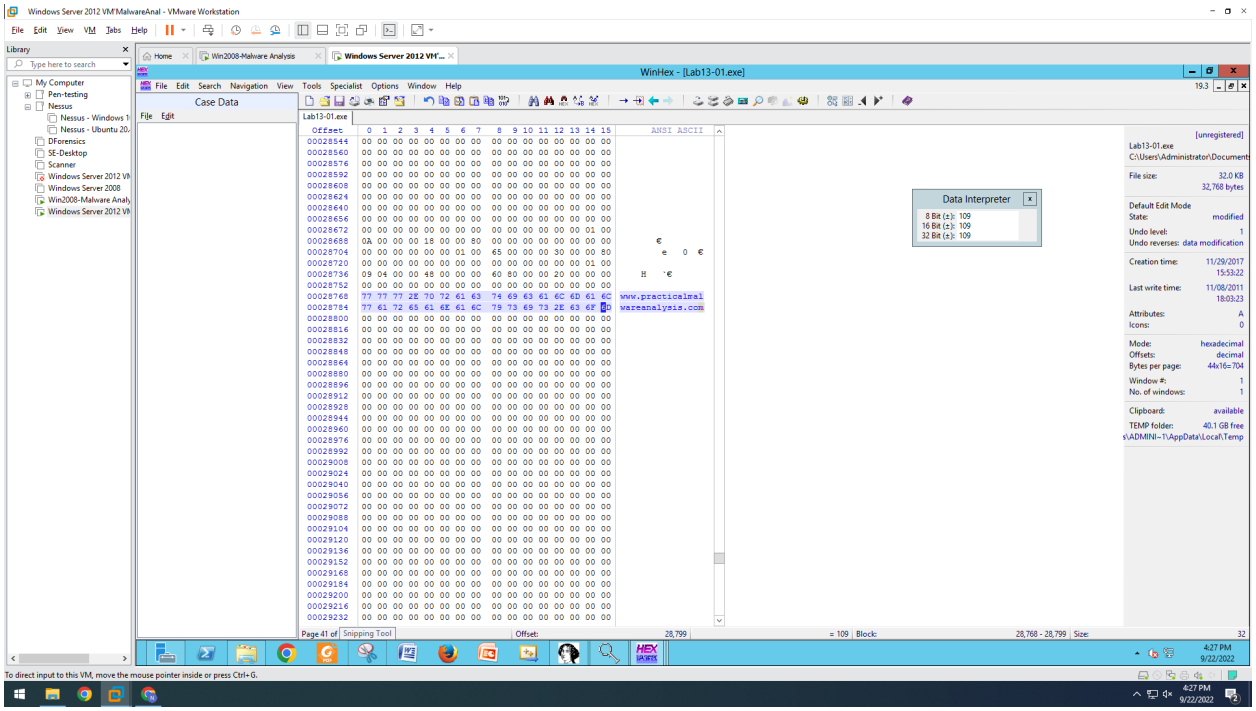
- Open the Lab13-01.exe file in the PEview.
- Now in the left pane, click on RCDATA 0065 0409.
- Now on the right side find the address 00007060 and take a screenshot.



WinHex

- Open the winhex and click on file > open and open the Lab13-01.exe file.
- Highlight bytes 7060 through 707f and edit > modify data.
- A new window will pop up, now check the XOR radio button and enter a key of 3B.





Conclusion: To conclude with the lab, We learned numerous strategies for performing a data encoding method, as well as WinHex.