This lab is designed to teach the students how to identify different types of data obfuscation/encoding methods.

Please determine how the contents of the files in the folder “Lab 2 - Data Obfuscation” were encoded and use the proper tools to decode.

Two Python scripts are given to you in the directory lab directory; b64\_decode.py (for decoding base64) and rot13.py (for decoding ROT13). Please use Hexplorer and refer to the ASCII chart on the Desktop called “asciifull.gif,” as needed.

Both 32 and 64-bit Python installers are included; please install the correct version per your operating system. By default, Python will be installed to C:\Python27. Navigate to the “Lab 2 – Data Obfuscation” folder and copy the six text files to C:\Python27.

**base64**

If you think the text is base64 encoded, at the command prompt type:

C:\Python27\python b64\_decode.py and hit enter

Then copy and paste the desired text into the window and hit enter.

**ROT13**

If you think the text is ROT13 encoded, at the command prompt type:

C:\Python27\python rot13.py and hit enter

Then copy and paste the desired text into the windows and hit enter.

**Decimal**

If you think the text is decimal encoded, please refer to the file “asciifull.gif” on the Desktop to decode.

**XOR**

If you think the text is XOR’ed, attempt to determine what it is XOR’ed with (rolling key, single byte, etc.) and use Hexplorer to decode. Drag and drop the text file into Hexplorer and select Edit, Operation, XOR Selection and enter the XOR key.