**A3**

**Prob 1**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Graphical user interface, text

Description automatically generated**

1. Imagine you entered a sequence like AAA**AAAA**AAAA, where the A’s colored in red represent the sequence you are seeking.

Why is it not possible to tell exactly which offset your **AAAA** pattern begins at? **1pt**

**The As have several 4 byte sets that overlap so the start point could be several places.**

1. Is it possible to put the bytes that represent characters below **0x20** and above **0x7E** into your non-repeating sequence? If it is not possible explain why? **2pts**

**It would be possible depending on how the bytes were being read back.**

**In our case, because we are representing the data as characters, it could make the data difficult or impossible to interpret.**

1. Will uppercase letters be treated differently from lowercase letters when placed on the stack? Why? **1pts**

**Yes because they have a different binary value.**

**Prob 2**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Graphical user interface, application

Description automatically generated**

**Graphical user interface, text

Description automatically generated**

**Prob 3**

**Sorry I was having trouble keeping the letters and numbers formatted without copying all the instructions, but I answered all the questions in the instructions here.**

1. **print(type(mype22.DOS\_HEADER), '\n', mype22.DOS\_HEADER)**
   1. What is a pefile.Structure?

**A class that can hold information about a pe file**

* 1. Notice the two columns of numbers of the left side of the output. What do the 2 columns of number represent in the output?

**The offset that the information is located at within the file counted in bytes**

* 1. What are the offsets of the **magic number** and the **offset to the PE Header**?

**Dos magic number @ 0x00**

**PE Header @ 0x60**

* 1. How many bytes does the **DOS\_HEADER** use?
     + - 1. **bytes in the DOS\_HEADER**

1. **print(mype22.NT\_HEADERS, mype22.NT\_HEADERS.Signature)**
   1. What is the **Signature** value that is printed? Do the bytes of this output fall into the ascii range? What do the bytes translate to?

**0x4550**

**PE after correcting for little endian**

* 1. Execute the following lines of code. What does the packed value represent?

**Pack the second argument binary info as a short from little endian**

* + 1. What does the number for the machine type mean?

**it specifies what CPU the image file can be run on**

* + 1. What do the characteristics translate to?

**Each bit is a flag that indicates properties of the file**

* + 1. What is the Entry Point address?

**0x5000 is the entry point on Kyjrgz41.exe**

* + 1. What does the entry point address represent?

**The address of the entry point relative to the image base when the executable file is loaded into memory. For program images this is the start address.**

* + 1. What is the image base?

**The preferred address of the first byte of image when loaded into memory; must be a multiple of 64 K.**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

**Text

Description automatically generated**

A screenshot of a computer

Description automatically generated with low confidence

A picture containing text, indoor, green, dark

Description automatically generated

## Questions:

1. What is the significance of the Entry point of an executable file? **2pts**

**The entry point is the start of the program**

1. What is the significance of the Magic number? In other words what is it used for? **1pt**

**a magic number defines the file format and tells the system how to read the file**

1. Why would the PE file format be considered complex? 1pt

**They have a specified structure that tells the reader how to process the file**

1. Is the PE file format the only file format for executables? Name 1 other file format for

executable file on any Operating System? **2pts**

**BIN Binary executable on Windows**

1. Non-executable files like PDFs are considered binary files because like the PE file format they have a specific structure that tells the Reader how to process the file. Are they any other types of binary files like the PDF file? Name 5 file types and example programs that can open them? Also list if python modules are available to parse these types of files? **5pts** *(You can present the result in a table)*

|  |  |  |
| --- | --- | --- |
| file type | program | python module |
| .ogg | windows media player | Hachoir |
| .sqlite | sqlitebrowser | sqlite3 |
| .jpg | windows photo viewer | struct |
| .zip | 7zip | zipfile |
| .mp4 | quicktime | pymp4parse |