**Matryoshka**

matryoshka.idb has my notes from tests 1-4. I 'nopped' the bytes in the first 3 functions, so Ida could recognize them as functions correctly.

matryoshka2.idb has my notes from test 5. It has the memory fix.

KeyGen is a java program that prints the correct password for all 5 tests.

Password 1: ABCDEF123456 + 5 :== FGHIJK6789:;

Password 2: ARCHIEMILLER - position :== AQAEE@GBDC;G

Password 3: GO FLYERS!!! ^ position :== GN"EH\CU[(+\*

Password 4: Volume Serial Number :== B8D3-F792 -1194068078 (on my computer)

Using the "vol c:" command from the command line, I found the Volume Serial Number

of my computer to be B8D3-F792. The assembly function called returns this as an

integer: B8D3F792.

When this gets converted in the sprintf command to a decimal number, it comes back

negative as -1194068078.

Password 5: 7E6ACC4C - This allocates memory from the heap in order to run the

GetAdaptersAddresses function, which creates a linked list of adapter info.

It takes 4 bytes of the first MAC address found 0x2C bytes into the structure,

and compares this with a hexadecimal string entered by the user.

Resources:

HeapAlloc function

https://msdn.microsoft.com/en-us/library/windows/desktop/aa366597(v=vs.85).aspx

GetAdaptersAddresses

https://msdn.microsoft.com/en-us/library/windows/desktop/aa365915(v=vs.85).aspx

IP\_ADAPTER\_ADDRESSES structure

https://msdn.microsoft.com/en-us/library/windows/desktop/aa366058(v=vs.85).aspx

Good example of writing java code to extract networking info, I modified it to

create my KeyGen program.

https://www.mkyong.com/java/how-to-get-mac-address-in-java/

...