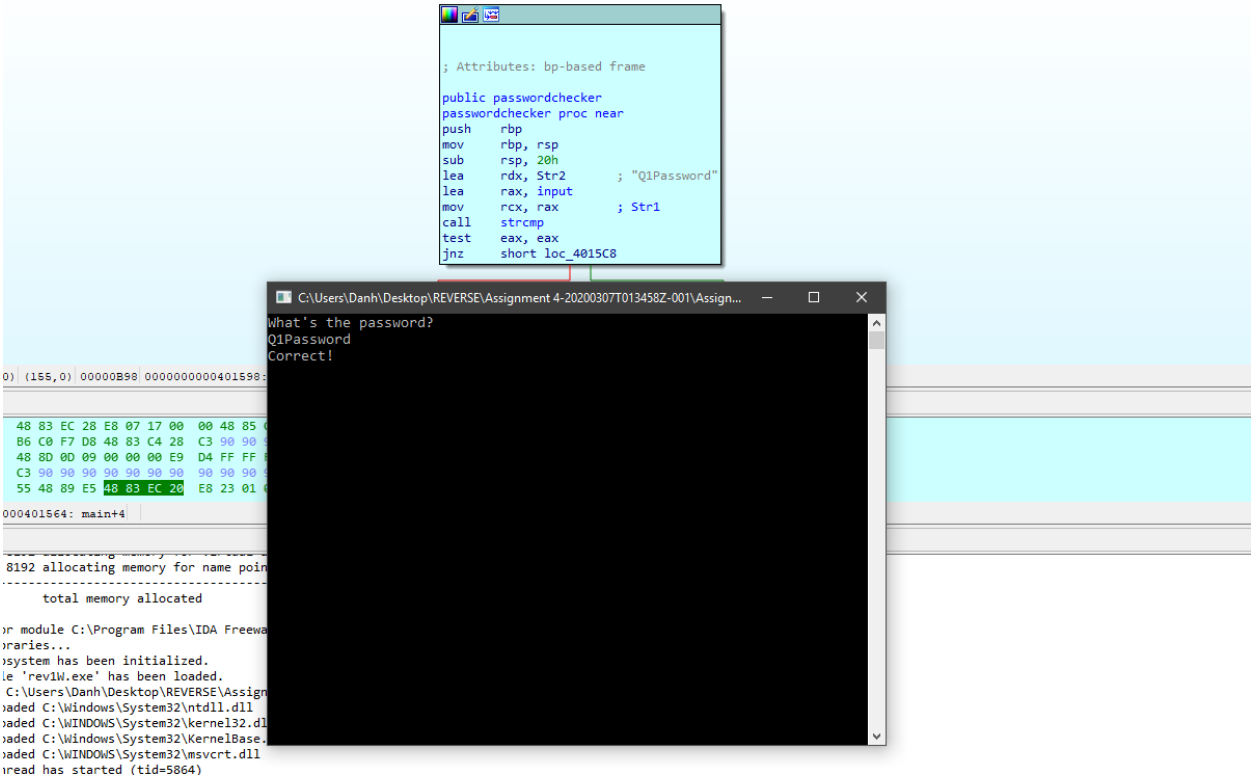
Reverse Engineering

Spring-2020 Semester

Danh Pham

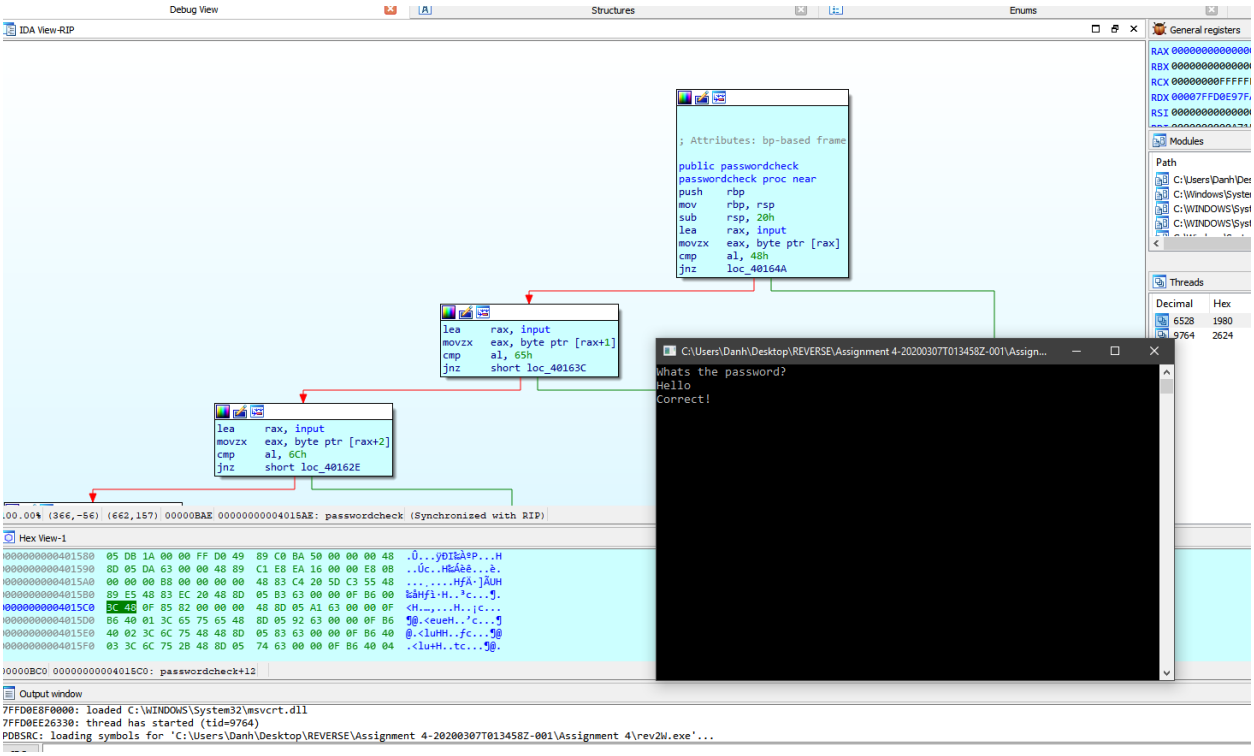
Task1:

Q1Password



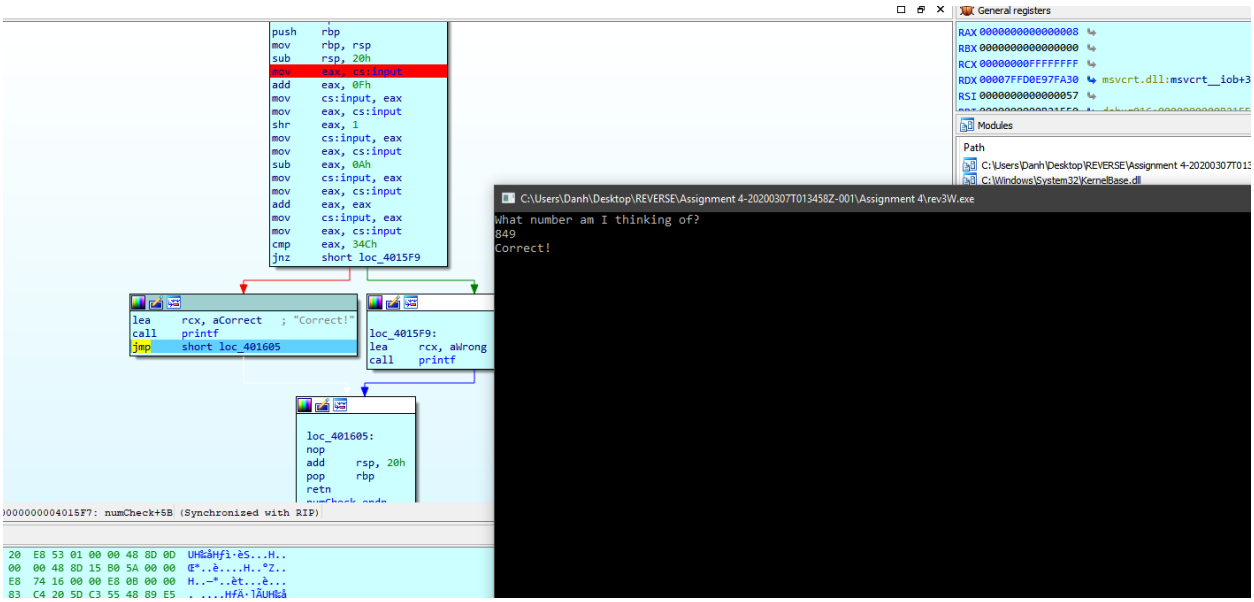
Task2:

Hello


Debug View
Structures
Enums
IDA View-RIP
General registers
Modules
Threads
; Attributes: bp-based frame
public passwordcheck
passwordcheck proc near
push rbp
mov rbp, rsp
sub rsp, 20h
lea rax, input
movzx eax, byte ptr [rax]
cmp al, 48h
jnz loc_40164A
lea rax, input
movzx eax, byte ptr [rax+1]
cmp al, 65h
jnz short loc_40163C
lea rax, input
movzx eax, byte ptr [rax+2]
cmp al, 6Ch
jnz short loc_40162E
C:\Users\Danh\Desktop\REVERSE\Assignment 4-20200307T013458Z-001\Assign...
Whats the password?
Hello
Correct!
Hex View-1
Output window
7FFD0E8F0000: loaded C:\WINDOWS\System32\msvcrt.dll
7FFD0EE26330: thread has started (tid=9764)
PDBSRC: loading symbols for 'C:\Users\Danh\Desktop\REVERSE\Assignment 4-20200307T013458Z-001\Assignment 4\rev2W.exe'...

Task3:

849


push rbp
mov rbp, rsp
sub rsp, 20h
mov eax, cs:input
add eax, 0Fh
mov cs:input, eax
mov eax, cs:input
shr eax, 1
mov cs:input, eax
mov eax, cs:input
sub eax, 0Ah
mov cs:input, eax
mov eax, cs:input
add eax, eax
mov cs:input, eax
mov eax, cs:input
cmp eax, 34Ch
jnz short loc_4015F9
lea rcx, aCorrect ; "Correct!"
call printf
jmp short loc_401605
loc_4015F9:
lea rcx, aWrong
call printf
loc_401605:
nop
add rsp, 20h
pop rbp
retn
General registers
RAX 0000000000000008
RBX 0000000000000000
RCX 00000000FFFFFFFF
RDX 00007FFD0E97FA30 msvcrt.dll:msvcrt__iob+3
RSI 0000000000000057
Modules
Path
C:\Users\Danh\Desktop\REVERSE\Assignment 4-20200307T013458Z-001\Assignment 4\rev3W.exe
What number am I thinking of?
849
Correct!

Task4:

change jz to jnz