* 0x0000739D: AddressOfEntryPoint là một thuộc tính trong tệp PE (Portable Executable) chỉ địa chỉ tương đối của điểm nhập của chương trình. Điểm nhập là lệnh đầu tiên được thực thi khi chương trình bắt đầu
* 0x01000000: Image Base là một giá trị địa chỉ được lưu trong tệp PE để cho biết địa chỉ ưu tiên nạp vào bộ nhớ ảo khi tệp PE được chạy
* 0x0000739D+0x01000000 = 0x0100739D(VA)
* Z=01001268: Z là địa chỉ hàm MessageBoxW được iport từ thư viện user32.dll
* Giá trị X có thể tính được bằng công thức:

+ VA: là địa chỉ thực tế của một phần tử bộ nhớ sau khi nó được nạp vào

+ Offset = RA – Section RA = VA – Section VA

+ 0x00011040(RA) – 0x00008400(Section RA) = X – 0x000B000(Section VA)

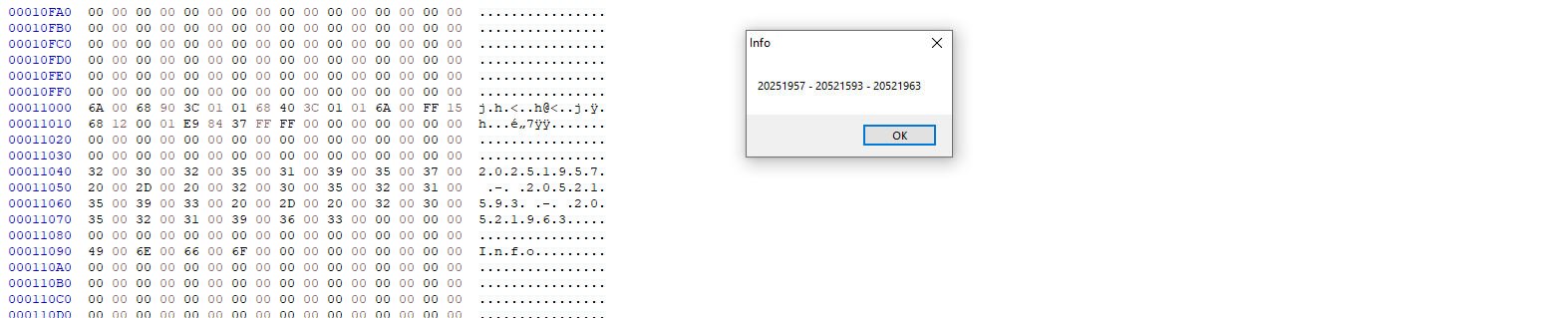
* X=0x00013C40+ImageBase= 0x01013C40
* Y=0x01013C60
* New\_entry\_point = 0x00011000 - 0x00008400(Section RA) + 0x000B000(Section VA) = 0x00013C00
* Relative\_VA là địa chỉ tương đối so với image base của tệp PE. Relative\_VA có thể khác với virtual address (VA), là địa chỉ thực tế của một phần tử trong bộ nhớ sau khi nó được nạp vào. Có thể tính VA bằng cách cộng image base cho relative\_VA

Jmp\_instruction\_VA = New\_entry\_point + 0x14(Số Byte của 5 câu lệnh assembly) + ImageBase = 0x01013C14

* Relative\_VA = 0x0000739D – 5(Số câu lệnh assembly) – 0x01013C14(Jmp\_instruction\_VA) = 0xFFFF3784

Ảnh có chứa bàn

Mô tả được tạo tự động



* Bài 5

Ảnh có chứa bàn

Mô tả được tạo tự động

* Ta chọn vùng nhớ trống này để chèn mã
* 00010D50: Nơi bắt đầu chèn
* 00010D90: Lưu Caption
* 00010DB0: Lưu text
* Ta có
* Z = 01001268
* X = 00010D90 - 0x00008400(Section RA) + 0x000B000(Section VA) + 01000000(ImageBase) = 01013990
* Y = 00010DB0 - 0x00008400(Section RA) + 0x000B000(Section VA) + 01000000(ImageBase) = 010139B0
* New\_entry\_point = 00010D50 - 0x00008400(Section RA) + 0x000B000(Section VA) = 00013950
* Jmp\_instruction\_VA = 00013950 + 0x14(Số Byte của 5 câu lệnh assembly) + ImageBase = 01013964
* Relative\_VA = 0x0000739D + 01000000(ImageBase) - 5 – 01013964(Jmp\_instruction\_VA) =FFFF3A34
* push 0 ; 6a 00

push Caption ; 68 90390101

push Text ; 68 B0390101

push 0 ; 6a00

call [MessageBoxW] ; ff15 68120001

jmp Origianl\_Entry\_Point ; e9 343AFFFF

Ảnh có chứa bàn

Mô tả được tạo tự động

Ảnh có chứa bàn

Mô tả được tạo tự động

* Calc
* Ta chọn vùng nhớ trống để chèn mã
* 00017040: Nơi bắt đầu chèn
* 00017070: Lưu caption
* 000170B0: Lưu text
* Ta có
* Z: 01001268
* X = 00017070 - 00013600 (Section RA) + 00016000 (Section VA) + 01000000(ImageBase) = 01019A70
* Y = 000170B0 - 00013600 (Section RA) + 00016000 (Section VA) + 01000000(ImageBase) = 01019AB0
* New\_entry\_point = 00017040 - 00013600 (Section RA) + 00016000 (Section VA) = 00019A40
* Jmp\_instruction\_VA = 00019A40 + 0x14(Số Byte của 5 câu lệnh assembly) + ImageBase = 01019A54
* Relative\_VA = 00012475 +01000000(ImageBase) - 5 – 01019A54 (Jmp\_instruction\_VA) = FFFF8A1C
* push 0 ; 6a 00

push Caption ; 68 709A0101

push Text ; 68 B09A0101

push 0 ; 6a00

call [MessageBoxW] ; ff15 68120001 A8110001

jmp Origianl\_Entry\_Point ; e9 1C8AFFFF