Thực hành 2: Chèn mã vào file PE

1. Phần mềm hỗ trợ

* CFF Explore để xem và sửa nội dung tham số trong file PE.
* HxD để đọc và sửa nội dung file PE.
* IDA Pro để kiểm tra mã hợp ngữ của chương trình muốn chèn

1. Thực hành

Mở Notepad.exe bằng CFF Explore:

* Optional Header:
  + AddressOfEntryPoint: 0000739D.
  + ImageBase: 01000000.

→ Địa chỉ ảo (virtual address) bằng cách cộng 2 giá trị trên : 0100739D.

* Section Header: có 3 dòng mỗi dòng có chứa 4 thông tin cần thiết:
  + VirtualSize: khai báo kích thước của section khi được load vào bộ nhớ.
  + VirtualAddress(VA): địa chỉ của section khi được load vào bộ nhớ.
  + RawSize: kích thước của section trong PE file.
  + RawAddress(RA): địa chỉ của section trong file PE.

Mở Notepad.exe bằng HxD: Nhận thấy cuối file vẫn còn bộ nhớ nên ta không cần thêm tạo thêm bộ nhớ.

* Chọn địa chỉ 00010D40 để lưu mã hợp ngữ, 00010D80 để lưu caption và 00010DA0 để lưu Text.
* Từ công thức Offset = RA – Section RA = VA – Secton VA (1)
* Tìm các giá trị X, Y, Z:

Address function MessageBoxW: 01001268

* + Ta có: Caption Address – RA + imageBase = X – VA ta tính được X = (Captions Address – RA + imageBase) + VA. X= (00010D80 – 00008400) + 0000B000 = 01013980.
  + Y: 010139A0.

ta tính được new\_entry\_point = địa chỉ bắt đầu mã hợp ngữ - RA + VA = 00010D40 – 00008400 + 0000B000 = 00013940.

Jump Address = 00010D54

Jump\_instruction\_VA = Jump Address – RA + imageBase + VA = 00010D54 – 00008400 +01000000 + 000B0000 = 01013954

Relative\_VA =(old\_entry\_point) - 5 - jump\_instruction\_VA = 0100739D – 5 - 01013954 = FFFF 3A44

* Thiết lập quay về AddreessOfEntryPoint ban đâu:
  + Old\_entry\_point = 0100739D.

Push 0 ; 6a 00

Push caption ; 68 80390101

Push text ; 68 A0390101

Push 0 ; 6a 00

Call [MessageBoxW] ; ff15 68120101

Jmp Original\_Entry\_Point; e9 443A FFFF

Caption(virut :D): 56 00 69 00 72 00 75 00 74 00 00 00

Text( Tran Huu Tien – 13521072): 54 00 72 00 61 00 6E 00 20 00 48 00 75 00 75 00 20 00 54 00 69 00 65 00 6E 00 20 00 2D 00 20 00 31 00 33 00 35 00 32 00 31 00 30 00 37 00 32 00 00 00