Để **tắt ASLR** bằng cách chỉnh cấu hình PE file, bạn cần sửa cờ DYNAMIC\_BASE trong header của file PE. Quy trình dưới đây sẽ hướng dẫn bạn thực hiện việc này bằng công cụ như *CFF Explorer* hoặc các công cụ tương tự:

**Hướng dẫn tắt ASLR trong file PE:**

1. **Tải và mở file bằng CFF Explorer:**
   * Tải *CFF Explorer* từ internet (công cụ miễn phí, nằm trong *NTCore Explorer Suite*).
   * Mở file PE bạn muốn chỉnh sửa bằng CFF Explorer.
2. **Tìm mục cấu hình PE Header:**
   * Trong giao diện của CFF Explorer:
     + Mở mục **NT Headers > Optional Header**.
     + Tìm đến phần **DLL Characteristics**.
3. **Xác định bit của DYNAMIC\_BASE:**
   * Bit DYNAMIC\_BASE (ASLR) thường nằm ở giá trị **0x40** trong trường **DLL Characteristics**.
   * Nếu bit này được bật, giá trị trong trường này sẽ bao gồm 0x40.
4. **Tắt ASLR:**
   * Bỏ tick (uncheck) hoặc sửa giá trị của trường **DLL Characteristics** để loại bỏ bit 0x40.
     + Ví dụ: Nếu giá trị hiện tại là 0x8140, bạn sửa thành 0x8100.
5. **Lưu file:**
   * Sau khi chỉnh sửa, lưu file PE.
   * File này giờ đã không còn hỗ trợ ASLR, và địa chỉ bộ nhớ của nó sẽ không thay đổi giữa các lần chạy.