Executable File Format

* Compiler , linker

+ Loader

* Sao chép các thành phần và tái tổ chức trên Ram
* Điểm đầu vào (điểm bắt đầu ct) : điểm địa chỉ trên Ram mà ct đc sao chép và bỏ lên nó
* Load các lib cần dùng để chạy ct

.dll :

PE (.exe)

* PE Header : chứa các trường thông tin của file PE
* Dos header : xem có tương thích vs dos hay k
* Relocation : tái định vị trên bộ nhớ Ram
* Phần import: **chứa các thông tin về các thư viện** cần được liên kết động (dynamic link libraries) **để chương trình có thể sử dụng** các hàm của các thư viện này.
* Phần export: chứa các **thông tin về các hàm và biến** được xuất từ chương trình để các **chương trình khác có thể sử dụng chúng.**
* Phần các section: chứa mã máy (machine code), dữ liệu, thông tin ký hiệu (symbol), và các thông tin khác cần thiết cho chương trình hoặc thư viện.
* Phần các segment: chứa thông tin về bố cục của chương trình trong bộ nhớ, bao gồm các vùng nhớ thực (thường được chỉ định bởi các phần section) và các vùng nhớ ảo (ví dụ như heap và stack).
* Dead space : vị trí trống (vt đầu , giữa các hàng) bị lợi dụng để chèn mã độc
* Api : đọc , mở file các thứ : có địa chỉ nhất định trong hệ điều hành
* IAT section: chứa các api ct đang sử dụng và nó nằm ở chỗ nào

ELF format

* Phần header: chứa thông tin tổng quan về file, bao gồm kiểu file, kiến trúc (architecture) của CPU, số lượng phần trong file, địa chỉ bắt đầu của chương trình, và các thông tin khác.
* Phần các section: chứa mã máy (machine code), dữ liệu, thông tin ký hiệu (symbol), và các thông tin khác cần thiết cho chương trình hoặc thư viện.
* Phần các segment: chứa thông tin về bố cục của chương trình trong bộ nhớ, bao gồm các vùng nhớ thực (thường được chỉ định bởi các phần section) và các vùng nhớ ảo (ví dụ như heap và stack).
* Phần relocation: chứa thông tin tái đặt vị trí (relocation) cần thiết để hệ điều hành thực hiện cập nhật các địa chỉ của các symbol khi chương trình hoặc thư viện được chạy trên một máy tính khác với máy tính được sử dụng để biên dịch.
* Phần symbol: chứa thông tin về các ký hiệu (symbols) được sử dụng trong chương trình hoặc thư viện, bao gồm tên của ký hiệu và địa chỉ tương ứng của nó.

Metric number :

DLL

1. Header: Điều khiển việc tải và sử dụng các tài nguyên trong DLL.
2. Export table: Chứa các tham chiếu đến các hàm và biến được xuất từ DLL để các ứng dụng khác có thể sử dụng.
3. Code section: Chứa mã thực thi của các hàm trong DLL.
4. Data section: Chứa các tài nguyên và dữ liệu được sử dụng bởi các hàm trong DLL.
5. Resources: Chứa các tài nguyên như biểu tượng, hình ảnh, âm thanh được sử dụng bởi các ứng dụng.
6. Import table: Chứa các tham chiếu đến các hàm và biến được sử dụng trong DLL từ các DLL khác.