Compiler: .c, .cpp, .s -> .o (object file).VD: gcc, clang, vc\_compilerCTP.exe

Linker: kết hợp .o thành excutable file (.exe, .out).VD: GNU ld, lld, LINK.exe

Loader: Nạp chương trình từ ổ đĩa vào bộ nhớ dể bắt đầu tiến trình

+ Executable loader: load executable files: VD: execve (system call)

+ Dynamic linking load: load dynamic labraries.VD: ld-linux.so

Executable file format:

- ELF: on unix

- PE: on Windows

- Mach-O on OS X

ELF Structure

ELF Header: basic identification information of this file

● Program header table: location of text and data sections

● Text section: the code

● Relocation information: for relocatable text and data sections

Data sections:

– .rodata: read-only

– .bss: uninitialized global

variables

– .data: initialized global

variables

● Example of other sections:

– .dynamic: dynamic linking information

– .got: global offset table

– .init; proces

Symbol table: locate program symbolic definition (e.g., exported function name)

● Section header table: location and information of each section

**.text, .data, .init, .dynamic directly copied to memory**

Analyze ELF tool: readelf, objdump: the disassemblr, hexdup: raw hexadecimal dump

A screenshot of a cell phone

Description automatically generated

Trường quan trọng trong DOS Header:

 **e\_magic**: Magic number, luôn là 0x5A4D (MZ trong ASCII), chỉ ra rằng đây là một file thực thi DOS hợp lệ.

 **e\_lfanew**: Offset đến NT Header (PE Header), giúp Windows loader tìm đúng vị trí để bắt đầu đọc thông tin PE.

There are dead spaces in executable files

– The beginning of ELF files

– Empty spaces between functions

– Empty spaces between sections

– Nops in functions

– 1 số linkers căn chỉnh tệp thực thi theo ranh giới trang