دوره ی آموزش ساختار فایلهای PE

Site: onhexgroup.ir

Youtube: onhexgroup

Telegram: onhex_ir

X: onhexgroup

Github: onhexgroup

ارائه شده توسط

onhexgroup

Telegram: onhex_ir

File Header

- **COFF File Header** هم میگن.
- اطلاعاتی در خصوص ساختار خود فایل میده.
- در فایل **winnt.h** با عنوان **IMAGE_FILE_HEADER** تعریف شده.

Github: onhexgroup

ساختار
File Header

- **Machine**: معماری که اجرایی میتونه روش اجرا بشه. ۲ مقدارش مهمه:
  - 0x8664 برای AMD64
  - 0x14c برای i386
  - سایر موارد
- **NumberOfSections**: تعداد Sectionها
- **TimeDateStamp** : تاریخ و زمان ایجاد فایل . در فرمت یونیکس (تعداد ثانیه ها از ساعت ۰۰:۰۰ ، یک ژانویه ۱۹۷۰)

Site: onhexgroup.ir

ساختار
File Header

- **PointerToSymbolTable** : آفست به جدول سیمبولهای COFF – منسوخ شده (COFF debugging information)
- **NumberOfSymbols**: تعداد وردیهای جدول سیمبولهای COFF – منسوخ شده. (COFF debugging information)
- **SizeOfOptionalHeader**: سایز Optional Header
- **Characteristics**: برخی از ویژگی های فایل رو ارائه میده. مثلا اینکه اجرایی هستش، سیستمی، **DLL** و ... . لیست کامل