دوره ی آموزش ساختار فایلهای PE

Site: onhexgroup.ir

Youtube: onhexgroup

Telegram: onhex_ir

X: onhexgroup

Github: onhexgroup

ارائه شده توسط

onhexgroup

Site: onhexgroup.ir

دوره رایگان آموزش PE

- دوره از دو فصل تشکیل شده:
  - فصل اول: آشنایی با ساختار فایلهای **PE**
  - فصل دوم: کاربرد ساختار فایلهای **PE**

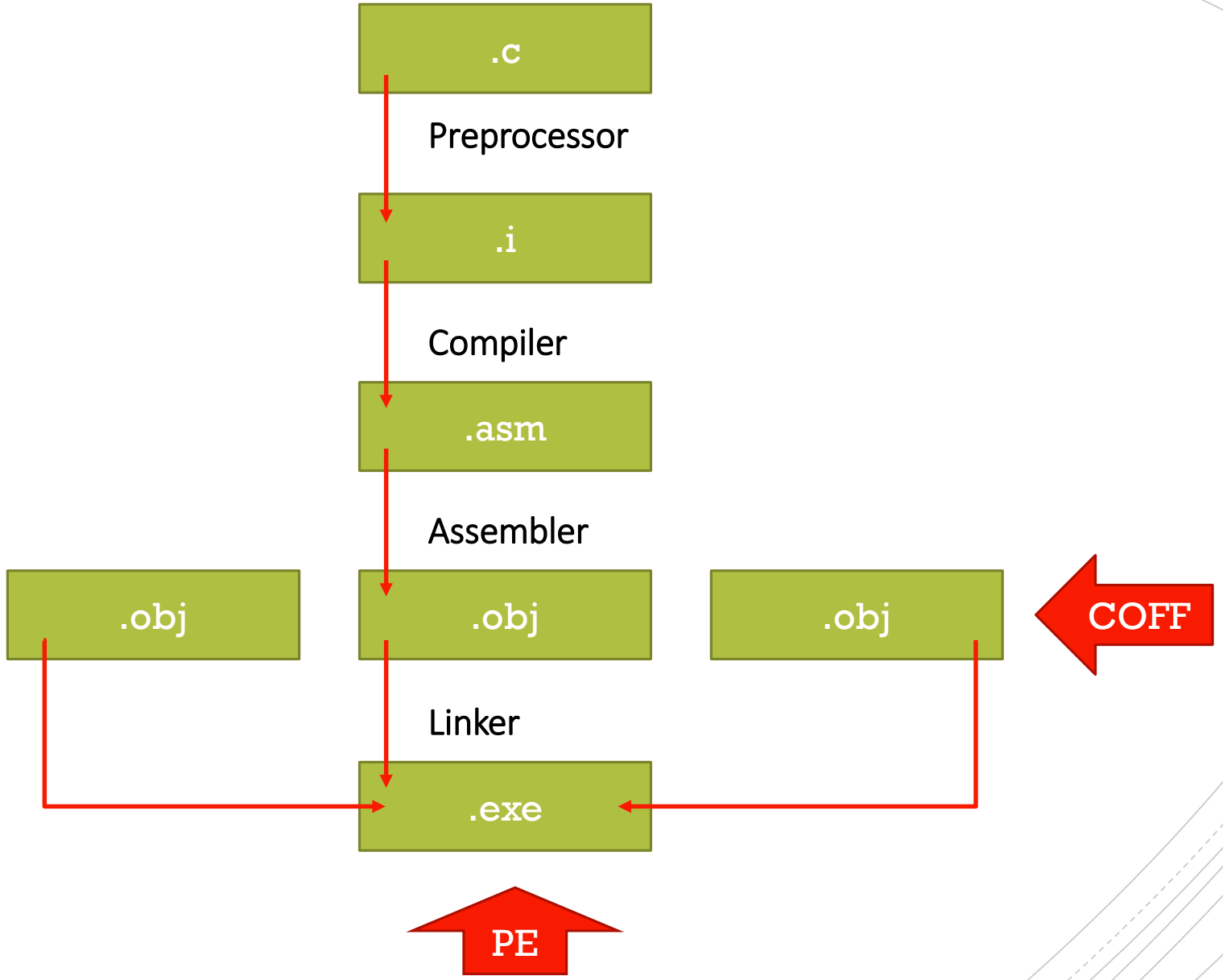
Youtube: onhexgroup

PE چیست

- **PE** مخفف **Portable Executable**
- فرمت اجرایی در ویندوز
- مبتنی بر **COFF** (**Common Object File Format**)
- **COFF** فرمت استاندارد برای فایلهای **object** هستش که خروجی اولیه کامپایلرها هستن و بصورت مستقیم قابل اجرا نیستن.
- فایلهای **EXE, DLL** و درایورها و ... فایل **PE** هستن.
- در مستندات مایکروسافت معمولا از **image** برای **PE** و از **object file** برای **COFF** استفاده میشه.

Github: onhexgroup

PE vs COFF



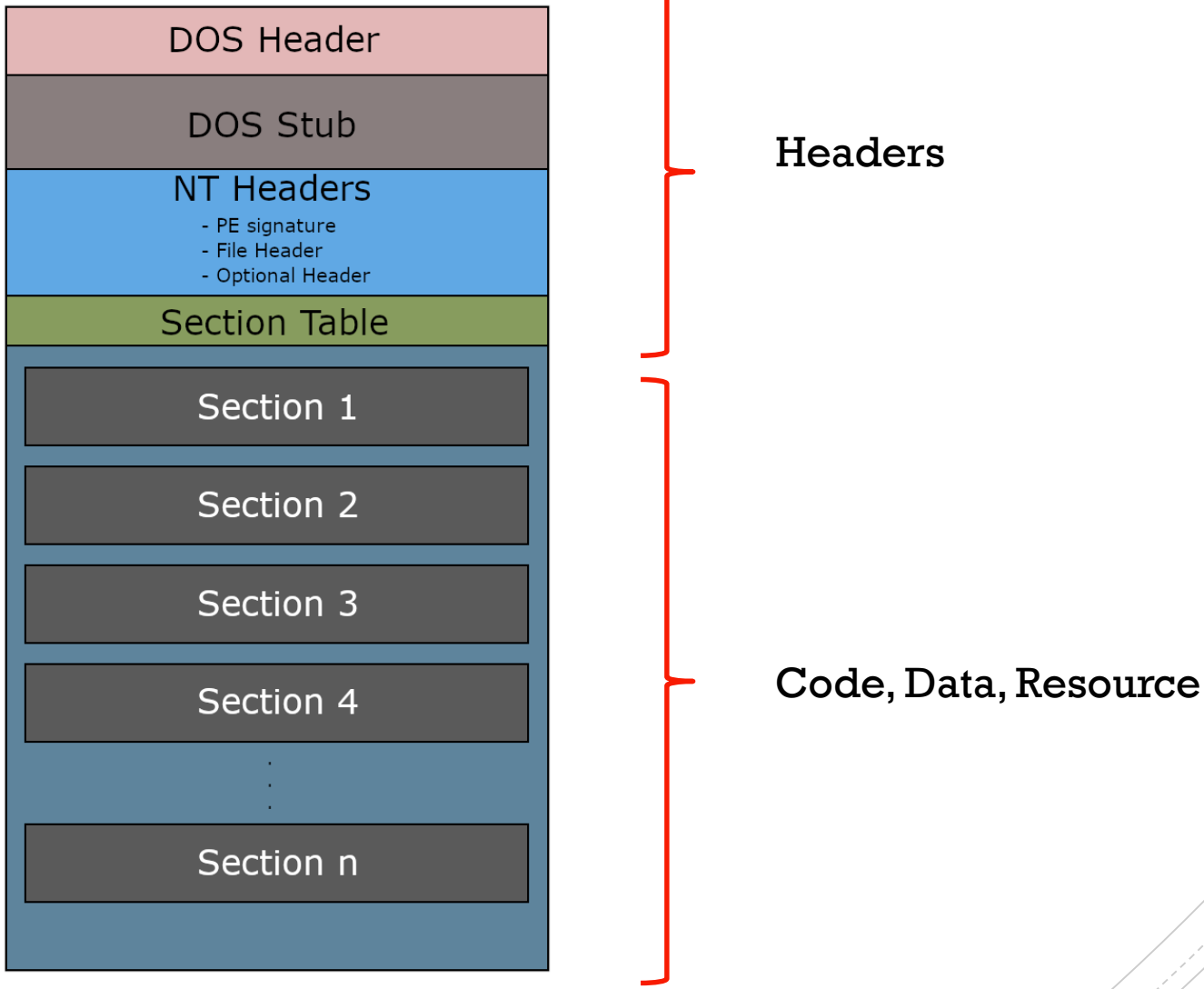
Site: onhexgroup.ir

۳۲ بیتی و ۶۴ بیتی

- فایلهای PE به دو دسته تقسیم میشن:
  - PE32 برای ۳۲ بیتی
  - PE32+ برای ۶۴ بیتی
- این دو نسخه از لحاظ آدرس های مجازی و برخی فیلدها با هم تفاوت دارن.

Youtube: onhexgroup

ساختار کلی PE



x: onhexgroup

اهمیت یادگیری

- درک نحوه ی اجرای برنامه ها و لوودشون در مموری
- تحلیل و دستکاری کدها
- شناسایی مکانیزمهای امنیتی، مبهم سازی، پک شدن، ضد مهندسی معکوس و ...
- اجرای فایلهای **PE** در ابزارهای امنیتی مانند دیباگرها و دیس اسمبلرها و ...

Telegram: onhex_ir

نکات مهم

- معمولا به فایل **PE** روی دیسک **image** و وقتی در حافظه قرار میگیره بهش ماژول **(Module)** میگن.
- **Process** به یک آدرس ایزوله میگن.
- ساختار یک فایل **PE** روی دیسک مشابه ساختارش در حافظه هستش.

Github: onhexgroup

نکات مهم

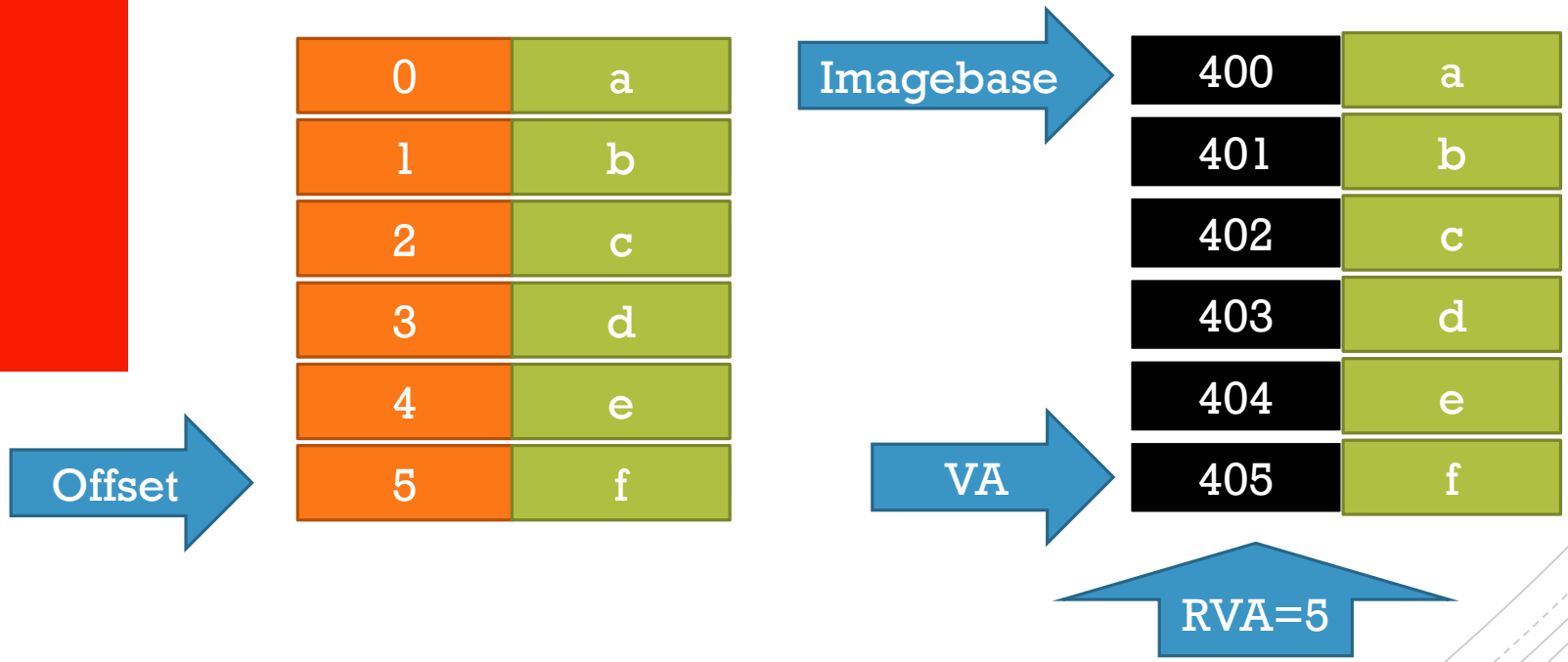
- آفست (**Offset**): موقعیت یک داده در فایل **PE** روی دیسک. معمولا بصورت بایت از ابتدای فایل مشخص میشه.
- آدرس مجازی [**Virtual Address (VA)**] : آدرس مطلق یک داده روی حافظه.
- آدرس مجازی نسبی [**Relative Virtual Address (RVA)**]: آدرس نسبی یک داده روی حافظه براساس **ImageBase** (توسط **Linker** درج میشه ولی ...) .

- فرض کنید یک داده در فاصله ی ۵ بایتی از فایل PE قرار گرفته: (فرض کنید ImageBase=400 و PE دقیقا بهمان شکلی که روی دیسک هستش، در مموری لوود میشه)

Youtube: onhexgroup

نکات مهم

VA = ImageBase + RVA
RVA = VA - ImageBase



Youtube: onhexgroup

ابزارهای مورد نیاز

- ویژوال استدیو ۲۰۲۲
- پایتون 3.x
- VSCODE
- افزونه ی پایتون
- پکیج lief (Library to Instrument Executable Formats)
  - pip install lief
- Pe Bear