دوره مهندسی معکوس نرم افزار

- Site: OnHexGroup.ir
- Youtube: @onhexgroup
- Telegram: onhex_ir
- Twitter: @onhexgroup
- Github: onhexgroup

نسخه ی ۳۲ و ۶۴ بیتی

پلتفرم: ویندوز

ارائه دهنده : **OnhexGroup**

Onhexgroup.ir

نحوه ی اجرای یک برنامه در ویندوز

فایل اجرایی، اجرا میشه

- از طریق دابل کلیک
- کامند لاین
- توسط یک برنامه دیگر
- و ...

Onhexgroup.ir

نحوه ی اجرای یک برنامه در ویندوز

فایل اجرایی، اجرا میشه

لودر ویندوز، هدر فایل رو بررسی میکنه

- لودر مسئول لوود فایل در مموری و آماده سازی اون برای اجراست.
- فایل های اجرایی در ویندوز PE نامیده میشن.
- فایل های PE بخش های مختلفی دارن از جمله هدر

Onhexgroup.ir

نحوه ی اجرای یک برنامه در ویندوز

فایل اجرایی، اجرا میشه

لودر ویندوز، هدر فایل رو بررسی میکنه

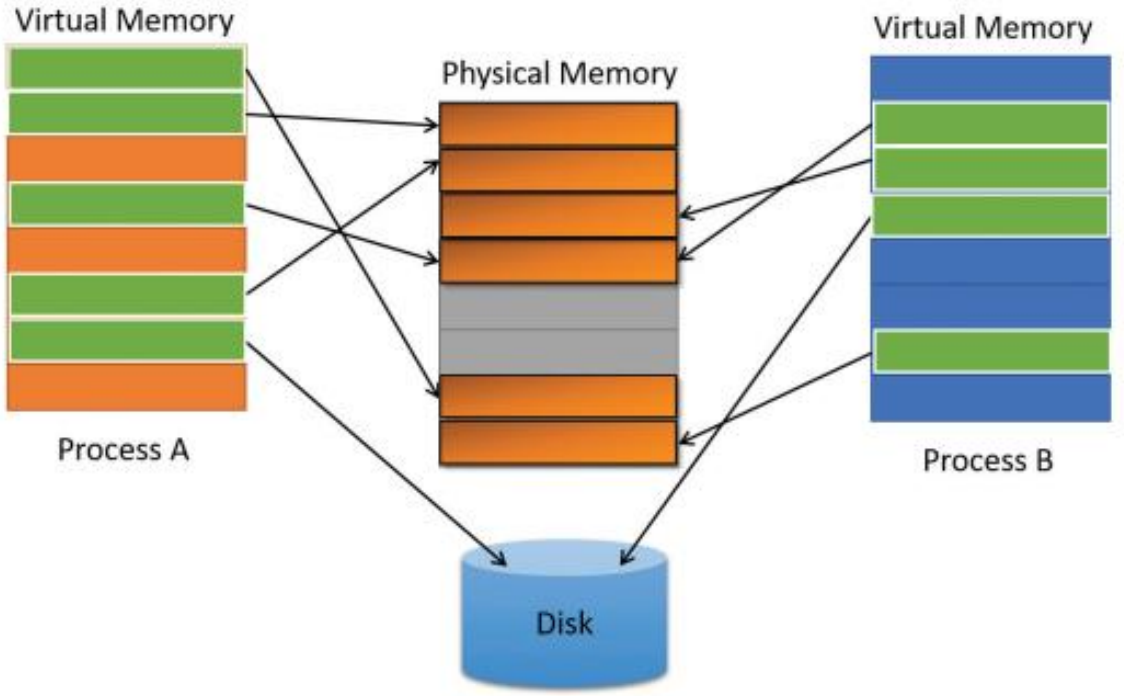
پروسس ایجاد میشه

- لودر یه پروسس ایجاد میکنه و فضای آدرس به اون اختصاص میده.
- پروسس مانند یه قفسه کتاب هستش .

Onhexgroup.ir

حافظه مجازی

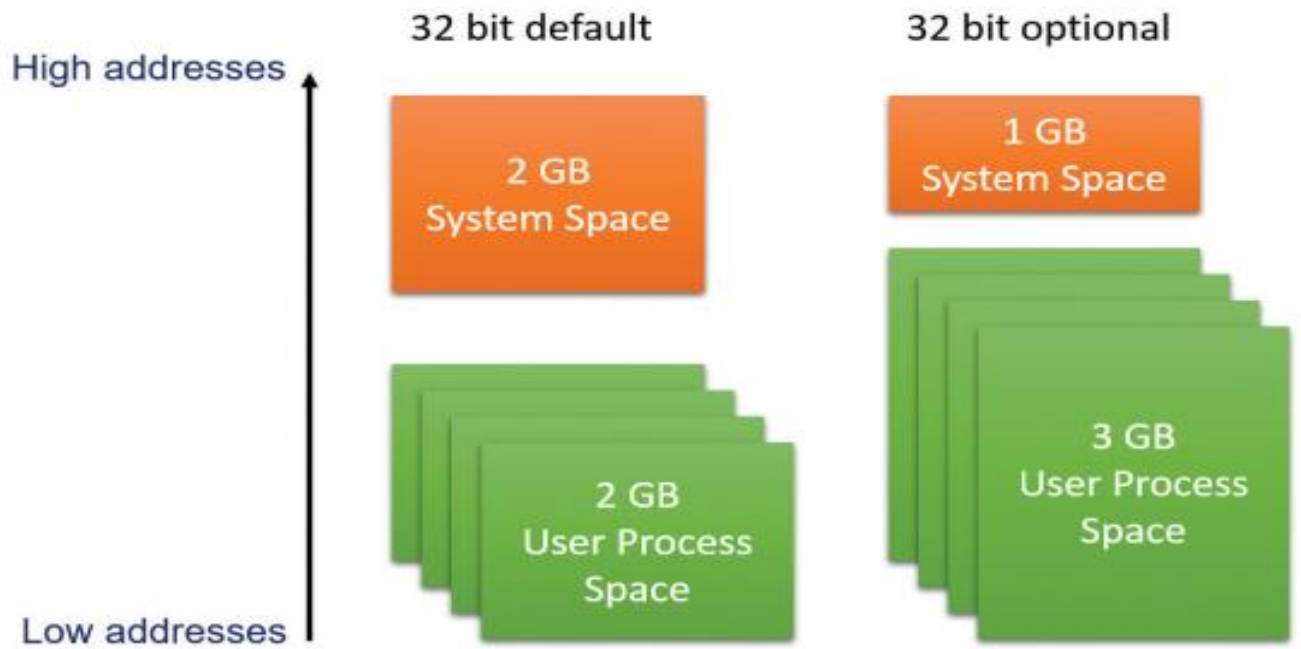
- از دید پروسس آدرس فیزیکی وجود نداره و همه چیز روی حافظه ی مجازی هستش.
- Memory Manager مسئول خواندن، نوشتن و تبدیل آدرس های مجازی به فیزیکی هستش.



Onhexgroup.ir

آدرس مجازی

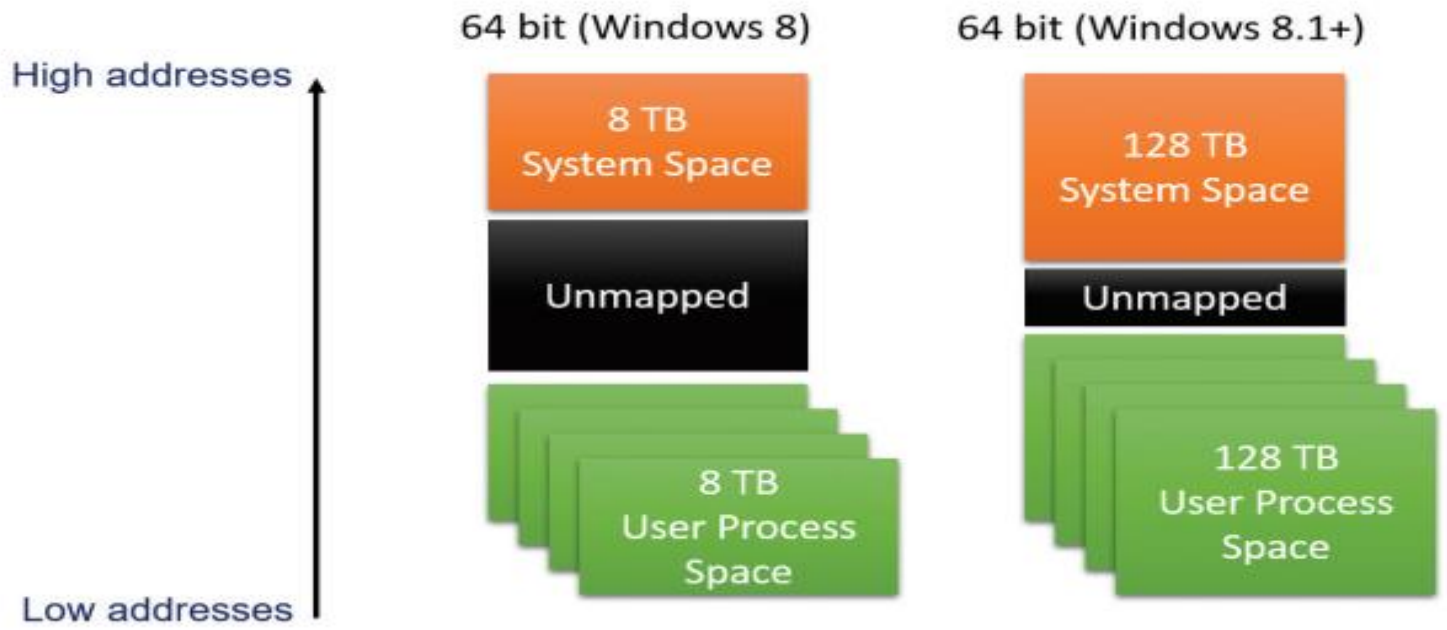
- هر پروسس محدوده آدرس خودش داره:
  - در ۳۲ بیتی ما 2^{32} بایت یعنی۴ گیگ فضا داریم
    - ۲ گیگ کاربر از آدرس **0x00000000** تا **0x7fffffff**
    - ۲ گیگ کرنل از آدرس **0x80000000** تا **0xffffffff**



Onhexgroup.ir

آدرس مجازی

- هر پروسس محدوده آدرس خودش داره:
- در ۶۴ بیتی ما 2^{64} بایت آدرس داریم. (16 exabytes)
  - آدرس کاربر از 0x00000000`00000000 تا 0x00007FFF`FFFFFFFF
  - آدرس کرنل از 0x00008000`00000000 تا 0xFFFFFFFF`FFFFFFFF



فایل اجرایی، اجرا میشه

لودر ویندوز، هدر فایل رو بررسی میکنه

پروسس ایجاد میشه

لودر شروع به نگاشت Sectionها میکنه

Onhexgroup.ir

نحوه ی اجرای یک برنامه در ویندوز

- لودر هر Section رو در جای مناسب نگاشت میکنه.
- هر فایل حاوی بخش های مختلفی هست: کد ، متغیرها، منابع و ...
- دستورات برای اجرا در CPU از طریق مموری خوانده میشه

Onhexgroup.ir

نحوه ی اجرای یک برنامه در ویندوز

فایل اجرایی، اجرا میشه

لودر ویندوز، هدر فایل رو بررسی میکنه

پروسس ایجاد میشه

لودر شروع به نگاشت **Section**ها میکنه

اجرا به EP منتقل میشه

- اجرا به Entry Point منتقل میشه.
- EP در هدر فایل مشخص شده

Onhexgroup.ir

منابع

- https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/user-space-and-system-space
- https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/accessing-memory-by-virtual-address
- https://learn.microsoft.com/en-us/windows-hardware/drivers/gettingstarted/virtual-address-spaces
- https://learn.microsoft.com/en-us/windows/win32/memory/memory-limits-for-windows-releases#memory-and-address-space-limits