内核

> 内核是操作系统最基本、最核心的部分，它负责管理系统的进程、内存、设备驱动程序、文件系统等系统资源，提供系统服务给应用程序使用。

模式

- 实模式(Real-address mode)
  - 16位CPU模式，应用程序和系统程序在一块内存中运行，没有保护机制
  - 应用和系统都可以直接访问硬件
- 保护模式(Protected-mode)
  - 32位CPU模式，应用程序和系统程序分别运行在各自独立的内存空间中，有保护机制
  - 硬件通过系统管理
- 虚拟8086模式(Virtual-8086 mode)

驱动程序

> 驱动程序是操作系统与硬件设备之间的接口，它负责控制硬件设备，实现硬件设备的读写操作。
> 由于需要与硬件交互所以具有ring0权限

- 驱动程序分为内核驱动程序和硬件驱动程序
  - 内核驱动程序是操作系统的一部分，它负责和操作系统交互
  - 硬件驱动程序是硬件设备制造商提供的驱动程序，它负责控制硬件设备，实现硬件设备的读写操作

驱动开发

- https://learn.microsoft.com/zh-cn/windows-hardware/drivers/download-the-wdk
- KMDF: Kernel Mode Driver Framework
  - 框架，用于开发硬件驱动

- NT驱动模型
  - 内核驱动程序开发模型

```
// Hello.c
#include <ntddk.h>

VOID Unload(__in struct _DRIVER_OBJECT  *DriverObject){
    // 声明未使用变量，不然会报错
    UNREFERENCED_PARAMETER(DriverObject);
    DbgPrint("Unload Hello World!");
}

NTSTATUS DriverEntry(
    __in struct _DRIVER_OBJECT  *DriverObject,
    __in PUNICODE_STRING  RegistryPath
    )
{
    UNREFERENCED_PARAMETER(RegistryPath);
    DbgPrint("Hello World!");
    // 注册卸载函数
    DriverObject->DriverUnload = Unload;
    return STATUS_SUCCESS;
}
```

```
TARGETNAME=Hello
TARGETTYPE=DRIVER
SOURCES=Hello.c
```

- 编译
  - 不能有中文路径
  - 使用指令 `build` 编译