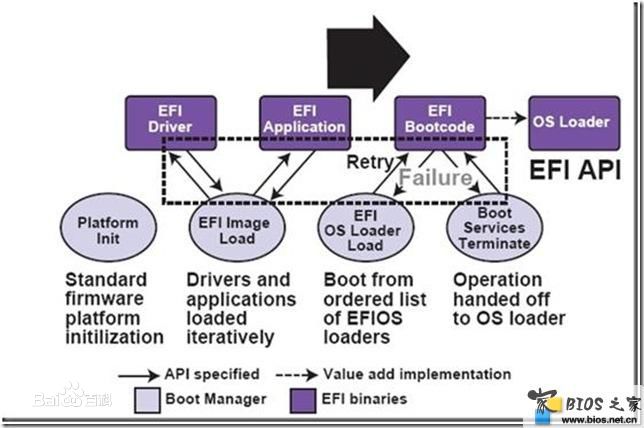
新型[UEFI](https://baike.baidu.com/item/UEFI)，全称“统一的可扩展固件接口”(Unified Extensible Firmware Interface)， 是一种详细描述类型接口的标准。这种接口用于操作系统自动从预启动的操作环境，加载到一种操作系统上。可扩展固件接口（Extensible Firmware Interface，EFI）是 Intel 为 PC 固件的[体系结构](https://baike.baidu.com/item/%E4%BD%93%E7%B3%BB%E7%BB%93%E6%9E%84)、接口和服务提出的建议标准。其主要目的是为了提供一组在 OS 加载之前（启动前）在所有平台上一致的、正确指定的启动服务，被看做是有近20多年历史的 BIOS 的继任者。



大纲目录：

1. Windows下直接运行Dll的三种方式

2. UEFI模块.efi和.Dll的关系（[DLL与UEFI的故事之二：通过实例观察DLL文件与EFI文件的关系](https://zhuanlan.zhihu.com/p/30106517)）

3. Windows下Dll的重定位与UEFI驱动的重定位

4. Dll与UEFI模块的安全性考量

5. Dll hell

在Windows系统中，Dll的使用已经遍及各个角落。众所周知dll是被映射到exe进程的地址空间中去，换句话说，它可以被认为寄生在exe之上，没有自己独立存在的可能。但是有很多软件安装后并没有exe文件，而仅仅是几个dll文件，他们的主人Host是Windows已经为它们安排好了的容身之所：svchost.exe、dllhost.exe和rundll32.exe。



在win10 insider build 14942中加入了新的特性：当内存为3.5GB+的时候，svchost会被切分为每个service一个单独的线程。这回导致进程的明显增加，但也会带来好处：稳定性增加、安全性增加、透明和减少管理成本。

大部分COM组件是以DLL形式存在，对于本地模式的组件一般是有EXE存在，所以它本身就已经是一个进程。对于远程DLL，我们必须找一个进程，这个进程必须包含了调度代码以实现基本的调度。这个进程就是dllhost.exe。这是COM默认的DLL代理。

xplorer不信任基于COM的扩展插件，毕竟谁都可以遵照接口写个插件

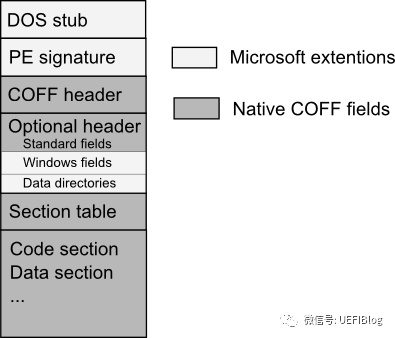
而糟糕的插件宕机后会连累explorer被关掉。

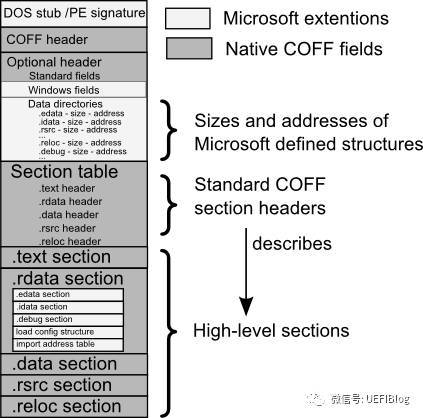
**rundll32.exe**

自从windows9x年代后，Rundll32.exe和Rundll.exe就广为大众所熟识。顾名思义，rundll就是运行dll。这个dll并不是普通的dll, 而是要符合rundll接口规范

rundll32.exe它是Windows系统自带的一个直接执行DLL中导出函数的小工具，很多工具和语言都利用它来执行一些有趣的功能

DLL和EFI文件在本质上一样的。事实上，Visual Studio编译工具链编译efi模块首先就是生成的dll文件，再被处理成了efi文件。它们都是符合PE/COFF格式的文件。





前文（DLL与UEFI的故事之一：Windows下运行Dll的三种方式）介绍了Explorer利用“COM Surrogate”来容纳它的扩展addins。这些addins统称ShellExt，它们基于COM接口，功能十分丰富，可以显示缩略图、显示详细内容、预览、添加特殊右键菜单等等。