WFP：

注册callout及子层如下：

那一层可以获取哪一些数据：

回调使用的内核监控事件如下：

1） 进程事件

PsSetCreateProcessNotifyRoutineEx

采集EPROCESS和PPS\_CREATE\_NOTIFY\_INFO 和\_FILE\_OBJECT数据结构：

进程启动时候，数据如下：

PPS\_CREATE\_NOTIFY\_INFO ：进程名 - PID - CommandLine(进程参数)

EPROCESS：DirectoryTableBase（进程页目录地址）

进程退出时候，数据如下：

PPS\_CREATE\_NOTIFY\_INFO ：进程名 - PID

2） 线程事件

PsSetCreateThreadNotifyRoutineEx

3） 注册表事件

CmRegisterCallbackEx

4） 模块事件

PsSetLoadImageNotifyRoutineEx

5） 驱动事件

IoRegisterBootDriverCallback

SeRegisterImageVerificationCallback

6）Session

IoRegisterContainerNotification

7）NMI

KeRegisterNmiCallback

8）关机

IoRegisterShutdownNotification

9）电源管理

PoRegisterPowerSettingCallback

10）WMI

IoWMISetNotificationCallback

11）其他

ObRegisterCallbacks、ObUnRegisterCallbacks

ExRegisterCallback(Callback\ProcessorAdd)

KeRegisterBoundCallback

FsRtlRegisterFileSystemFilterCallbacks

IoRegisterFsRegistrationChange

KeRegisterProcessorChangeCallback

应用层系统数据采集：<https://github.com/TimelifeCzy/Windows-emergency-servicetools>

文件技术方案：