

- 简介
- 基本使用
  - 使用捕获按钮进行捕获
  - 终止捕获
  - 保存
- 设置开机监控
  - 设置
  - 保存

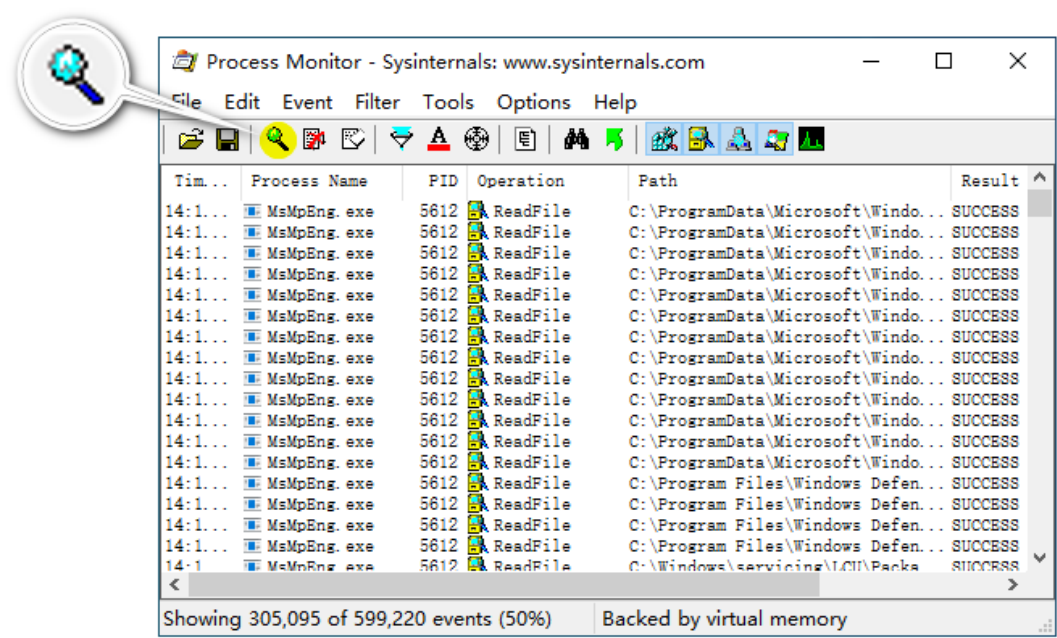
# 简介

[Procmon-进程监视器](#) 是 Windows 的高级监视工具，可显示实时文件系统、注册表和进程/线程活动。它结合了两个旧版 Sysinternals 实用工具（Filemon 和 Regmon）的功能，并添加了广泛的增强功能列表，包括丰富的非破坏性筛选、全面的事件属性（如会话 ID 和用户名）、可靠的进程信息、具有每个操作的集成符号支持的全线程堆栈、同时记录到文件等等。其独特强大的功能将使进程监视器成为系统故障排除和恶意软件搜寻工具包中的核心实用工具。

## 基本使用

### 使用捕获按钮进行捕获

单击捕获按钮进行捕获




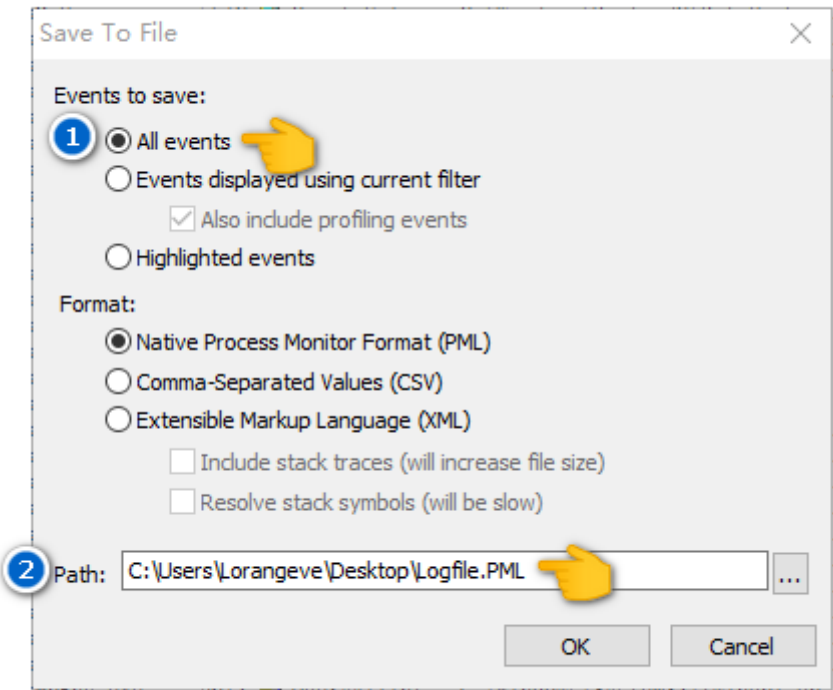
### 终止捕获

进行捕获后，再次单击捕获按钮终止捕获

从  到  为一次捕获。

# 保存


单击  弹出保存窗口；

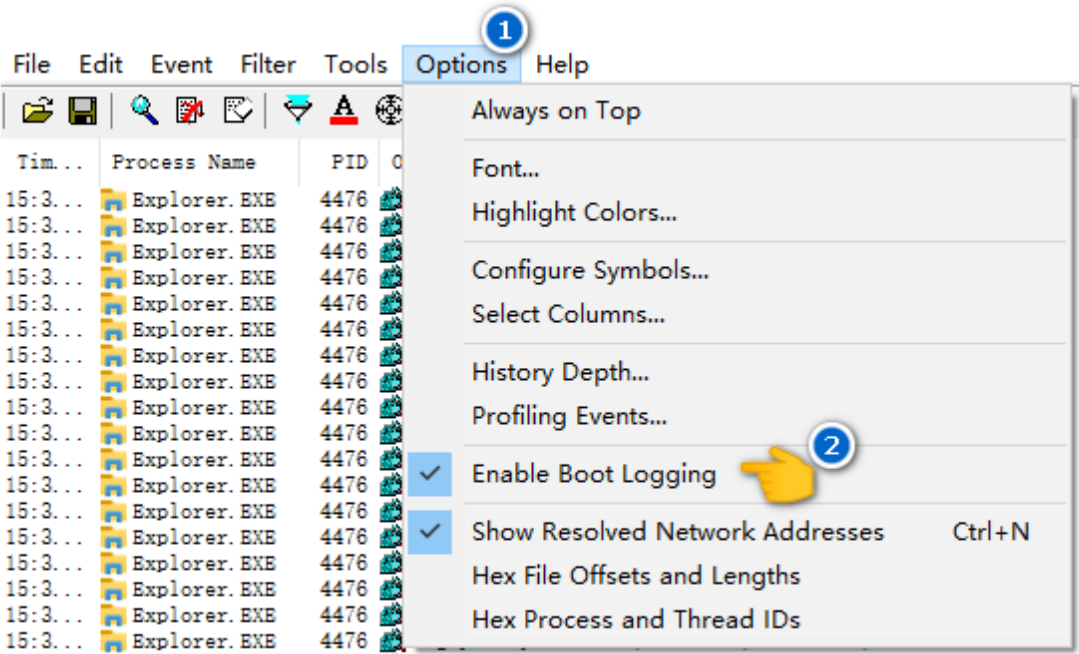



设置①All Event 全部事件 ②Path 保存路径，然后保存。

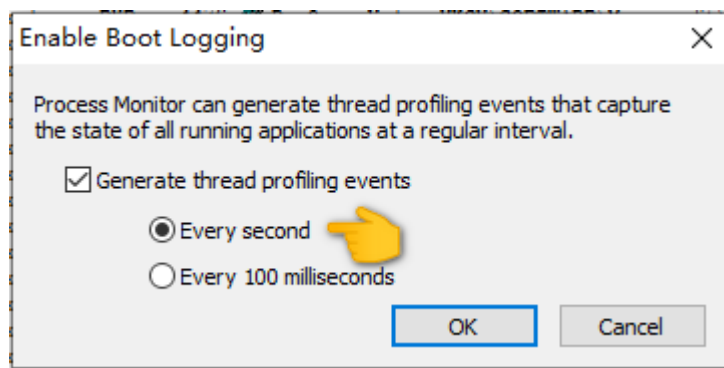
# 设置开机监控

## 设置

选择 Options 菜单  Enable Boot Logging 选项



在弹出的窗口中勾选： Generate thread profiling events  Every sencond



## 保存

重启机器后，再次打开 Procmon，会弹出保存日志的提示，点击确认保存（取消将丢弃日志）。

