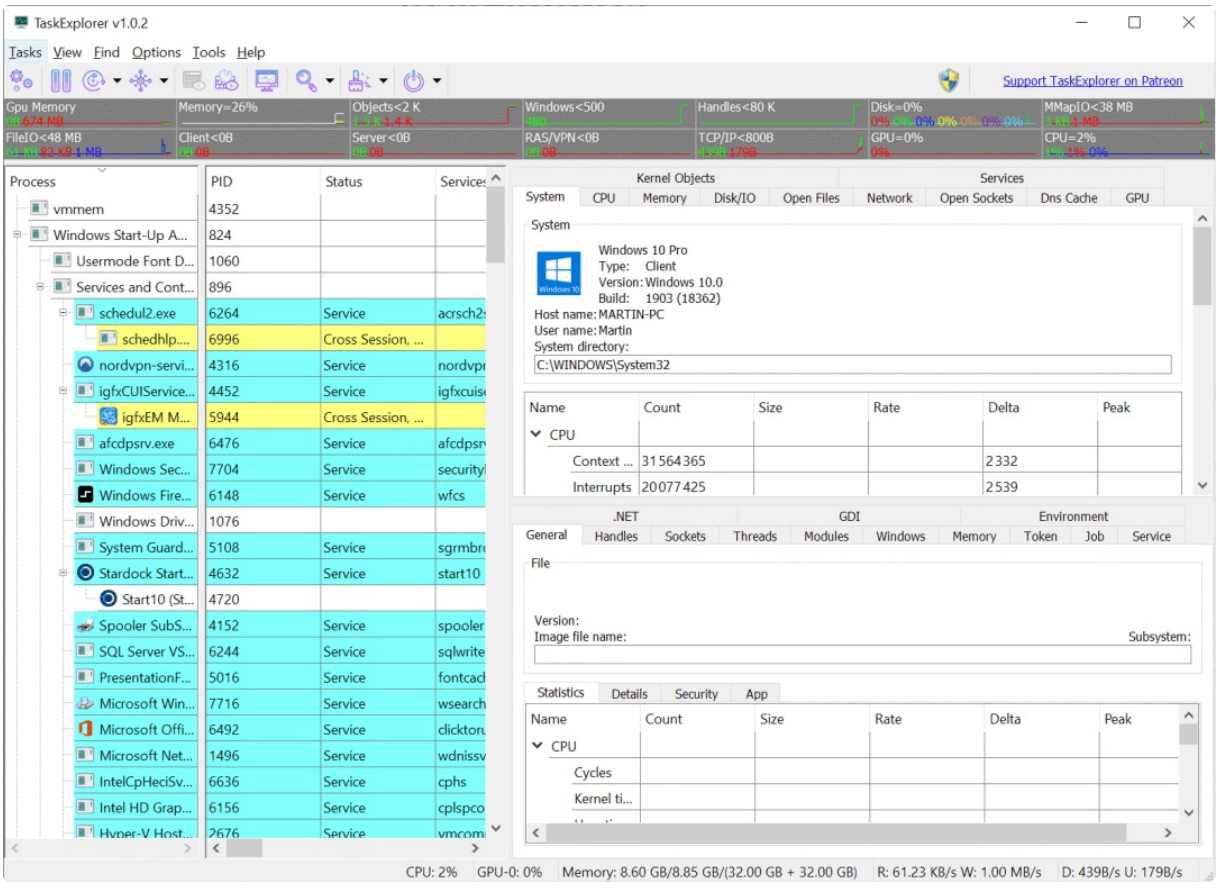
微软该学学了！从Win7到Win11

最近在 GitHub 上看到一个挺有意思的项目，叫 TaskExplorer，算是一个加强版的任务管理器吧，它不只是能看哪些程序在跑，还能把每个程序背后在干什么，都给你看得清清楚楚。有时候电脑卡了，或者某个软件行为怪怪的，用系统自带的任务管理器，总觉得差点意思，只能看到谁在吃 CPU，谁在占内存，但具体为啥吃这么多，说不清楚

TaskExplorer 就把这些黑盒子给打开了，线程在干嘛，文件读写到哪了，网络连了谁，都能直接看，对于想折腾下电脑，或者排查点问题的人来说，这工具算是挺顺手的。

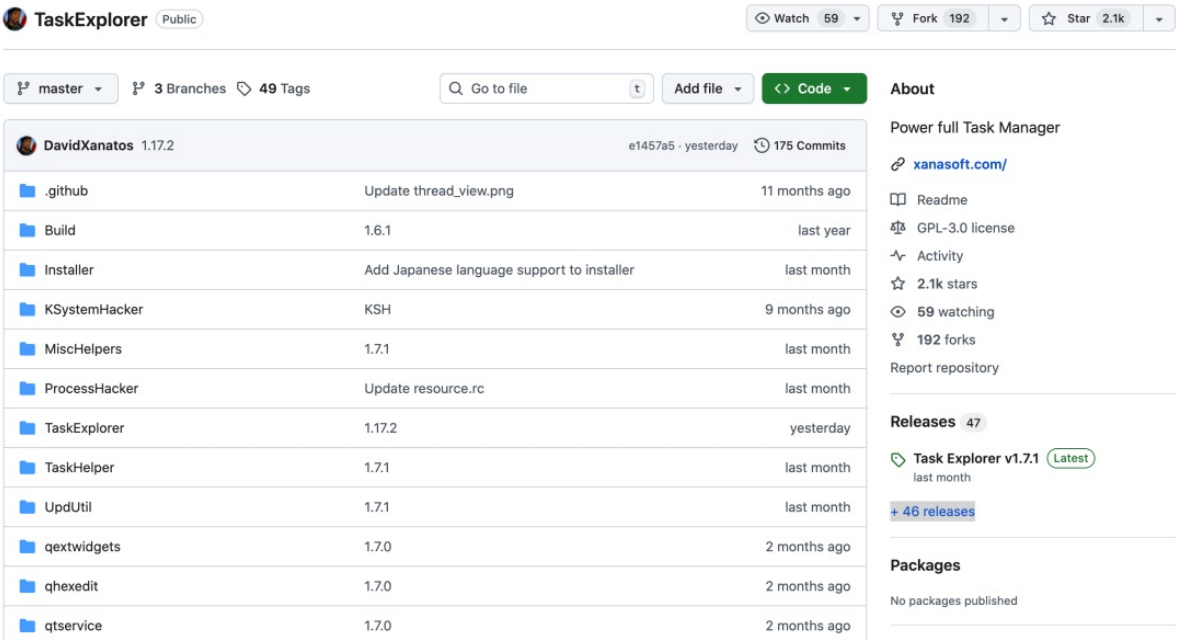
TaskExplorer是什么



> TaskExplorer 是一个面向 Windows 的、深度集成的系统监控与管理工具，它超越了传统任务管理器的简单进程列表，致力于提供进程行为的全景透视。通过其高效的界面设计，用户可以在一个窗口内实时洞察进程的线程栈、内存数据、文件句柄、网络连接等底层细节，旨在成为技术用户和系统管理员进行故障诊断、性能分析和安全审查的得力助手

开源成就

- **Star数** GitHub 上已经吸引了 **2.1k** 星

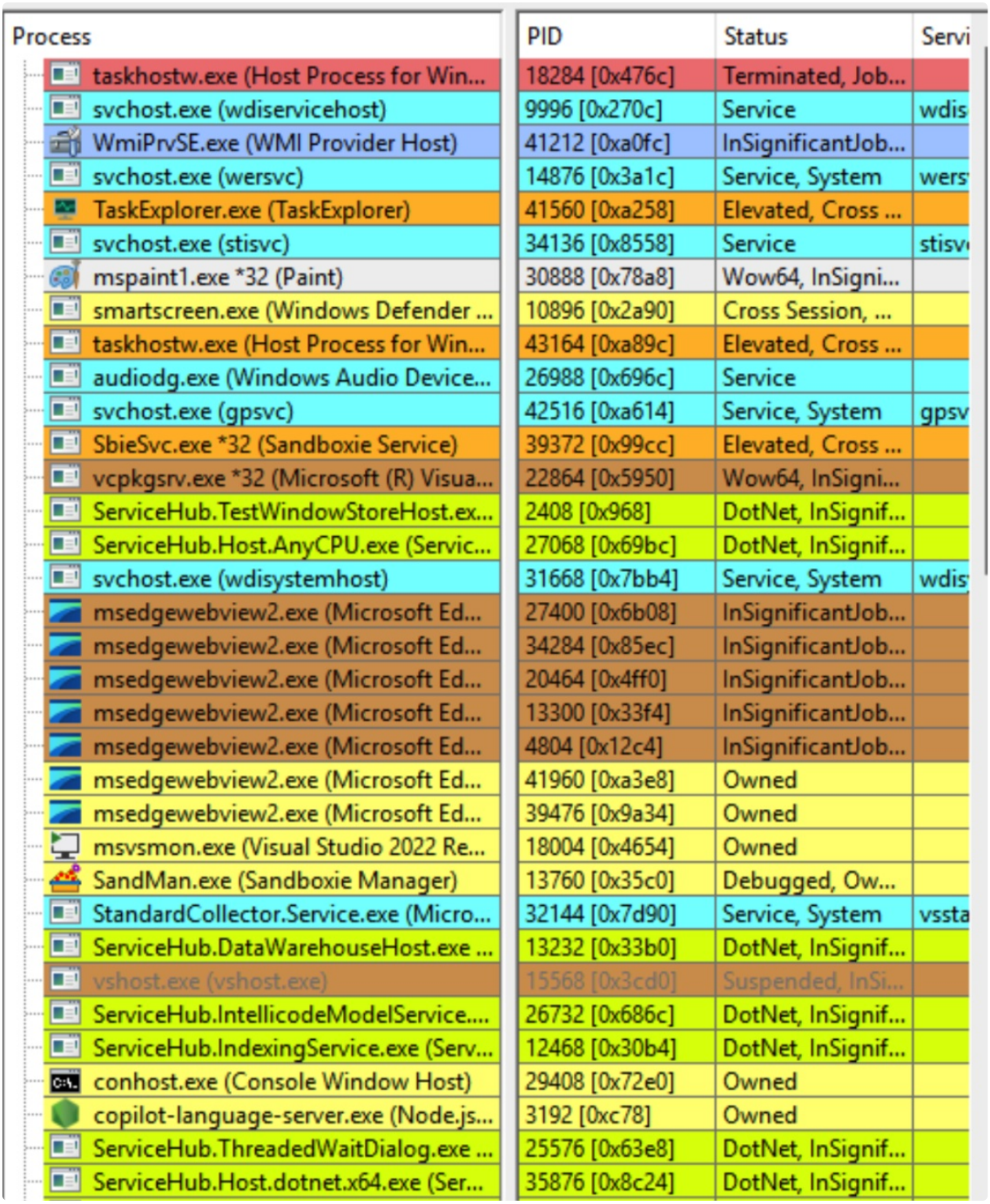


- 主开发语言　C 和 C++

核心功能

线程堆栈透视

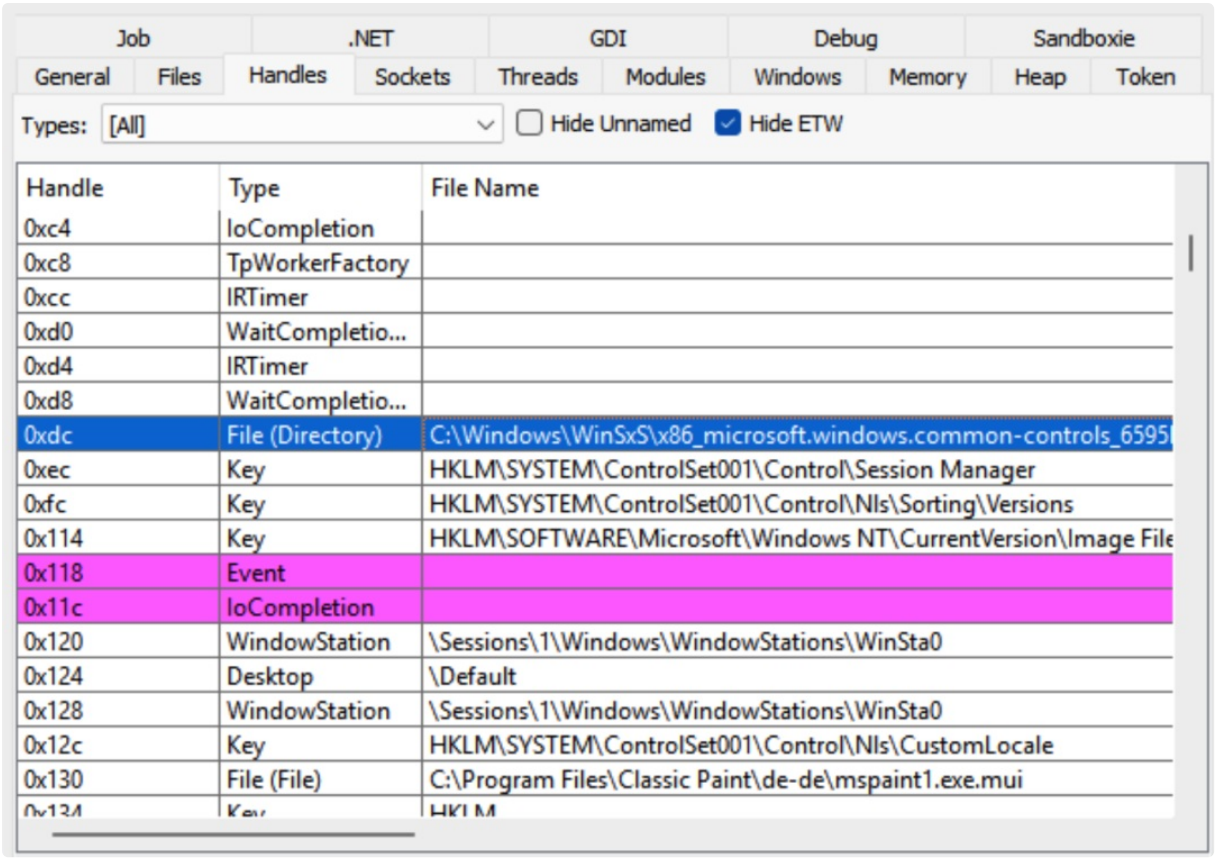
选中一个进程后，直接就能看到它下面每个线程的调用堆栈，这功能对于排查程序卡死或者响应慢特别有用，你一眼就能看出来线程卡在哪个函数调用上等磁盘读写，还是等网络回应，还是锁住了，不用再去开其他调试工具



Process	PID	Status	Servi
taskhostw.exe (Host Process for Win...	18284 [0x476c]	Terminated, Job...	
svchost.exe (wdiservicehost)	9996 [0x270c]	Service	wdis
WmiPrvSE.exe (WMI Provider Host)	41212 [0xa0fc]	InSignificantJob...	
svchost.exe (wersvc)	14876 [0x3a1c]	Service, System	wers
TaskExplorer.exe (TaskExplorer)	41560 [0xa258]	Elevated, Cross ...	
svchost.exe (stisvc)	34136 [0x8558]	Service	stisv
mspaint1.exe *32 (Paint)	30888 [0x78a8]	Wow64, InSigni...	
smartscreen.exe (Windows Defender ...	10896 [0x2a90]	Cross Session, ...	
taskhostw.exe (Host Process for Win...	43164 [0xa89c]	Elevated, Cross ...	
audiodg.exe (Windows Audio Device...	26988 [0x696c]	Service	
svchost.exe (gpsvc)	42516 [0xa614]	Service, System	gpsv
SbieSvc.exe *32 (Sandboxie Service)	39372 [0x99cc]	Elevated, Cross ...	
vcpkgsrv.exe *32 (Microsoft (R) Visua...	22864 [0x5950]	Wow64, InSigni...	
ServiceHub.TestWindowStoreHost.ex...	2408 [0x968]	DotNet, InSignif...	
ServiceHub.Host.AnyCPU.exe (Servic...	27068 [0x69bc]	DotNet, InSignif...	
svchost.exe (wdisystemhost)	31668 [0x7bb4]	Service, System	wdis
msedgewebview2.exe (Microsoft Ed...	27400 [0x6b08]	InSignificantJob...	
msedgewebview2.exe (Microsoft Ed...	34284 [0x85ec]	InSignificantJob...	
msedgewebview2.exe (Microsoft Ed...	20464 [0x4ff0]	InSignificantJob...	
msedgewebview2.exe (Microsoft Ed...	13300 [0x33f4]	InSignificantJob...	
msedgewebview2.exe (Microsoft Ed...	4804 [0x12c4]	InSignificantJob...	
msedgewebview2.exe (Microsoft Ed...	41960 [0xa3e8]	Owned	
msedgewebview2.exe (Microsoft Ed...	39476 [0x9a34]	Owned	
msvsmon.exe (Visual Studio 2022 Re...	18004 [0x4654]	Owned	
SandMan.exe (Sandboxie Manager)	13760 [0x35c0]	Debugged, Ow...	
StandardCollector.Service.exe (Micro...	32144 [0x7d90]	Service, System	vssta
ServiceHub.DataWarehouseHost.exe ...	13232 [0x33b0]	DotNet, InSignif...	
vshost.exe (vshost.exe)	15568 [0x3cd0]	Suspended, InSi...	
ServiceHub.IntellicodeModelService....	26732 [0x686c]	DotNet, InSignif...	
ServiceHub.IndexingService.exe (Serv...	12468 [0x30b4]	DotNet, InSignif...	
conhost.exe (Console Window Host)	29408 [0x72e0]	Owned	
copilot-language-server.exe (Node.js...	3192 [0xc78]	Owned	
ServiceHub.ThreadedWaitDialog.exe ...	25576 [0x63e8]	DotNet, InSignif...	
ServiceHub.Host.dotnet.x64.exe (Ser...	35876 [0x8c24]	DotNet, InSignif...	

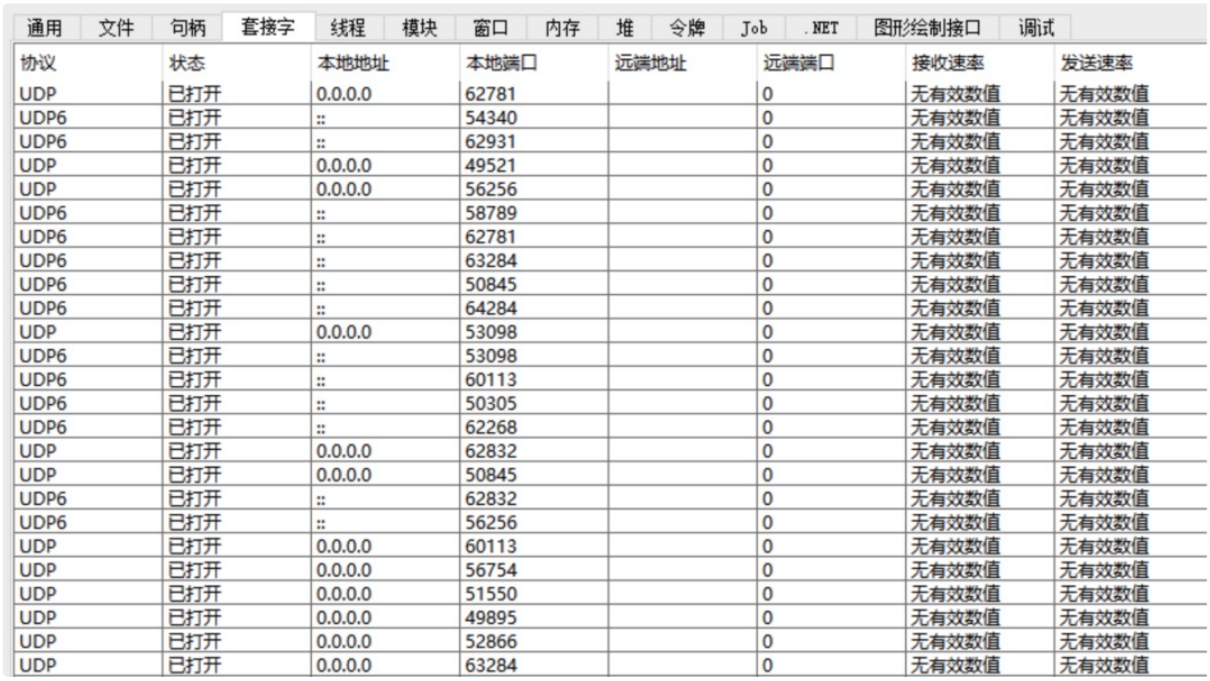
内存查看与编辑

提供了一个内置的十六进制内存编辑器，能直接查看和修改指定进程的内存数据，还支持字符串搜索，这对于分析程序内部数据结构、或者进行一些简单的内存补丁实验来说，算是把专业调试器的部分功能给搬过来了，不过操作上要直观不少



句柄与文件监控

能把进程打开的所有句柄都列出来，不管是文件、注册表键、还是事件、线程这些内核对象，对于文件句柄，会直接显示完整的路径、当前读写位置和文件大小，这样你就能清楚地知道某个软件到底在读写你的哪些文件，占着哪些资源不放



协议	状态	本地地址	本地端口	远端地址	远端端口	接收速率	发送速率
UDP	已打开	0.0.0.0	62781		0	无有效数值	无有效数值
UDP6	已打开	::	54340		0	无有效数值	无有效数值
UDP6	已打开	::	62931		0	无有效数值	无有效数值
UDP	已打开	0.0.0.0	49521		0	无有效数值	无有效数值
UDP	已打开	0.0.0.0	56256		0	无有效数值	无有效数值
UDP6	已打开	::	58789		0	无有效数值	无有效数值
UDP6	已打开	::	62781		0	无有效数值	无有效数值
UDP6	已打开	::	63284		0	无有效数值	无有效数值
UDP6	已打开	::	50845		0	无有效数值	无有效数值
UDP6	已打开	::	64284		0	无有效数值	无有效数值
UDP	已打开	0.0.0.0	53098		0	无有效数值	无有效数值
UDP6	已打开	::	53098		0	无有效数值	无有效数值
UDP6	已打开	::	60113		0	无有效数值	无有效数值
UDP6	已打开	::	50305		0	无有效数值	无有效数值
UDP6	已打开	::	62268		0	无有效数值	无有效数值
UDP	已打开	0.0.0.0	62832		0	无有效数值	无有效数值
UDP	已打开	0.0.0.0	50845		0	无有效数值	无有效数值
UDP6	已打开	::	62832		0	无有效数值	无有效数值
UDP6	已打开	::	56256		0	无有效数值	无有效数值
UDP	已打开	0.0.0.0	60113		0	无有效数值	无有效数值
UDP	已打开	0.0.0.0	56754		0	无有效数值	无有效数值
UDP	已打开	0.0.0.0	51550		0	无有效数值	无有效数值
UDP	已打开	0.0.0.0	49895		0	无有效数值	无有效数值
UDP	已打开	0.0.0.0	52866		0	无有效数值	无有效数值
UDP	已打开	0.0.0.0	63284		0	无有效数值	无有效数值

网络连接可视化

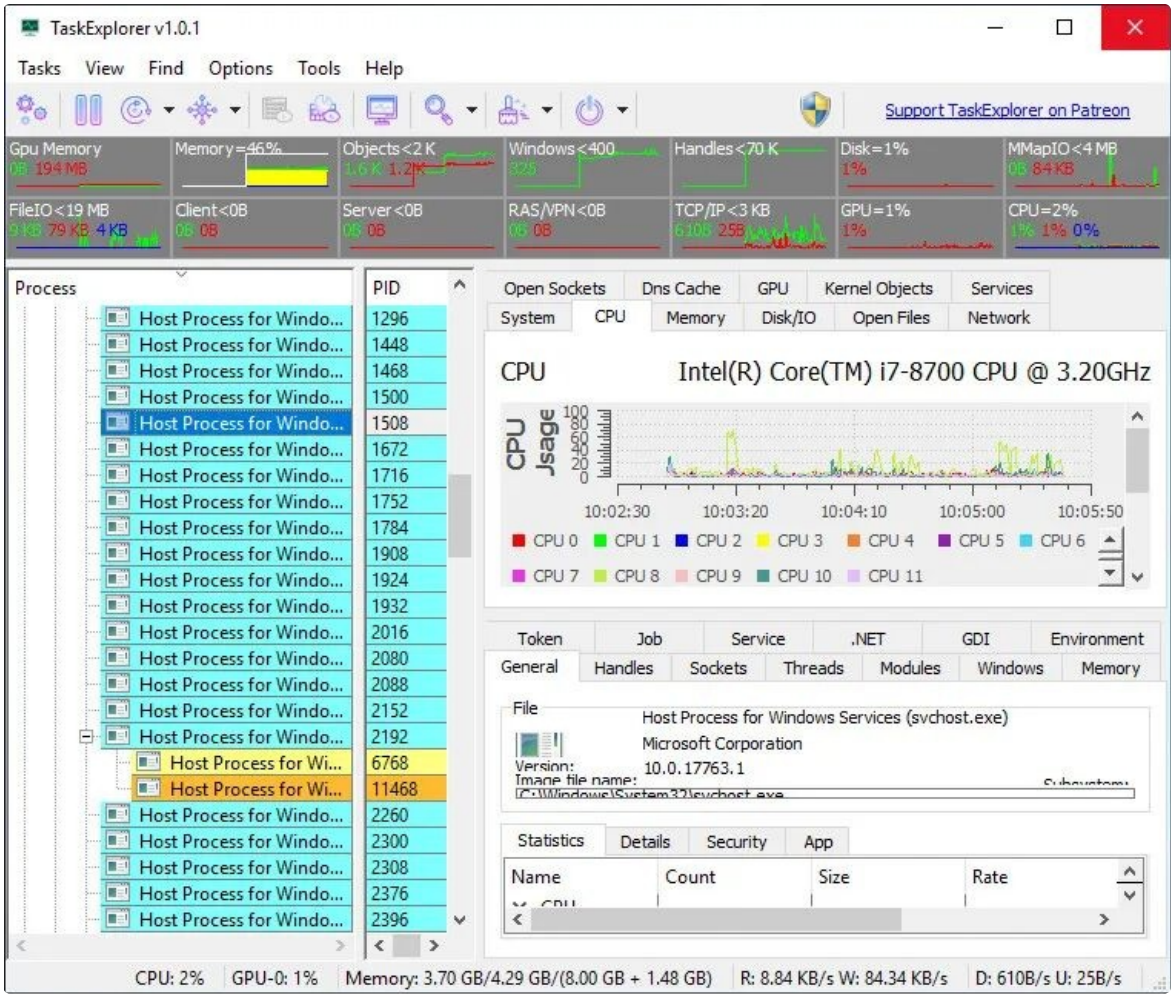
不仅显示 TCP/UDP 端口这些基本信息，还能通过 ETW 事件追踪来“推测”和显示无连接的 UDP 通信对端，同时提供实时的上下行数据速率，这对于分析软件的网络行为、监控后台流量很有帮助，比单纯看资源管理器里的网络占用要具体得多

模块管理与注入

除了列出所有已加载的 DLL 和内存映射文件，它还允许你卸载某些非核心的 DLL，或者向目标进程注入新的 DLL，这给高级用户提供了更强的控制能力，虽然用起来需要谨慎，但在某些调试或安全分析场景下是刚需

系统级资源总览

软件顶部有实时的系统资源图表，显示 CPU、内存、磁盘 I/O、网络和 GPU 的使用情况，下方的系统面板则可以总览全系统的文件、套接字，并能管理系统服务和驱动程序，相当于把一个轻量级的性能监视器和服务管理器给整合了进来，窗口布局还能自由折叠或分离，用起来挺灵活的



安装指南

- 项目提供了完整的源代码，你可以从 GitHub 仓库主页直接下载 ZIP 包，或者用 Git 克隆下来，不过编译它需要配置 Qt 等依赖环境，过程对新手可能有点复杂

- 对于大多数用户，更简单的方式是直接使用作者打包好的安装程序，在 GitHub 的 Releases 页面能找到最新的安装包，比如 `TaskExplorer-v1.17.2-Setup.exe`，下载后像普通软件一样安装即可，它包含了所有必要的驱动和库文件
- 软件需要管理员权限来运行，以便获取所有进程的完整信息，首次运行时可能会提示安装其专用的内核驱动程序，这是实现其深度监控功能所必需的，需要点击确认
- 它支持从 Windows 7 到 Windows 11 的 32 位和 64 位系统，界面支持多国语言，安装程序里可以选择

```
开源地址https://github.com/DavidXanatos/TaskExplorer
```

近期热文:

[刚刚开源！有潜力]

[一定收藏 ！SVIP体验]

[要火火火了！这脑洞我服了]

[刚刚开源！会计直呼内行]

[不越狱！来得太及时]