蓝蛇端口扫描器 产品手册

更新日期：2025年6月25日

# 【阅读提示】

　　MS Word用户按【Ctrl + F】打开“导航”窗格，点击“标题”选项卡可查看本文档的章节标题。WPS用户可点击“视图”功能选项卡的“页面”按钮查看目录，直接跳转到需要的章节。

# 【先决组件】

　　本软件既能安装在PC机上，也能安装在Windows服务器上。如果是PC机，只能安装在Windows 7 SP1或更先进的Windows系统上。如果您是Windows 7用户，可以通过安装Service Pack 1补丁来升级操作系统。此外，操作系统还需要先安装好《.NET Framework 4.8》、《Microsoft Visual C++ 2022 运行时库》。下面给出各先决组件的非官方下载地址；另外，本软件安装之初也会先检查这些先决组件。

## **《Windows 7** Service **Pack 1（x64）》：**

<https://pan.baidu.com/s/15Ae43SuZ1z_7K_yli5fRSQ?pwd=k8pq>

## 《.NET Framework 4.8》：

<https://pan.baidu.com/s/1q5s6F0EpAbeGowCPLXllJw?pwd=c9ga>

## 《Microsoft Visual C++ 2015-2022 运行时库（x64）》：

<https://pan.baidu.com/s/1Pkb73pWsZNjez34c9s6zkg?pwd=7nqp>

# 【设置Windows系统显示文件扩展名】

　　如图1所示，在资源管理器的“查看”功能区中，勾选红框所示的“文件扩展名”项即可。

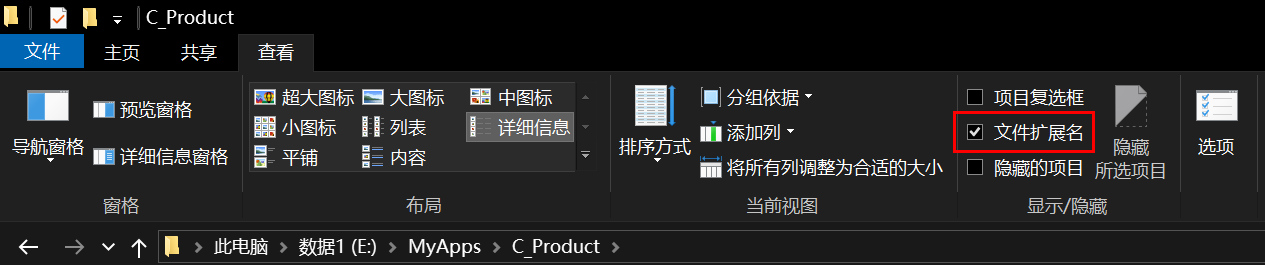


图1 在Windows资源管理器中设置显示“文件扩展名”

# 【开始安装】

　　鼠标悬浮在安装程序文件名上可见文件说明。您只需运行扩展名为“msi”的程序即可开始安装。

　　本安装程序安装前会先检查系统是否已有其它版本的软件，如果有，则先卸载，但卸载不会删除程序设置和用户信息。程序每次启动时都会自动检查是否有新版本，如果有，则提示用户升级。检查等待过程中主界面会有三种彩虹动态效果供用户挑选。

# 【安装程序权限不足】

　　有的用户可能因权限不足而无法写文件到磁盘上，此时可以以管理员身份运行命令提示符（又叫“命令行”），在命令行程序中运行安装程序。Win10用户请依次点击系统的“开始”->“Windows 系统”->右击“命令提示符”->“更多”->“以管理员身份运行”。接着输入安装程序所在目录的盘符，按回车。再输入安装程序所在目录的路径，按回车。最后输入安装程序的文件名，按回车。在安装程序的“选择安装文件夹”页面中，在“为自己还是为所有使用该计算机的人安装”选项中，选择“只有我”选项；即可。

# 【功能模块说明】

　　本产品共有“基于地址扫描端口”“基于端口扫描地址”“端口字典”“程序设置”四大模块，此外还有一个“查询域名的IP地址”模块，下面将分别介绍。

## 帮助提示

　　首先，本功能模块陈述主要介绍产品特性，不能涵盖全部使用说明。由于本软件持续迭代升级，最终的使用说明应以软件的文本说明和帮助提示为准，**用户请把鼠标悬浮在有疑惑的控件上来获取**。

## “基于地址扫描端口”



图2 “基于地址扫描端口”面板

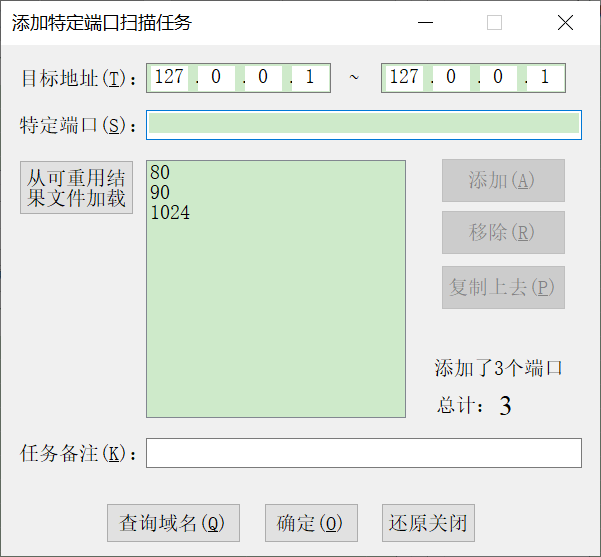
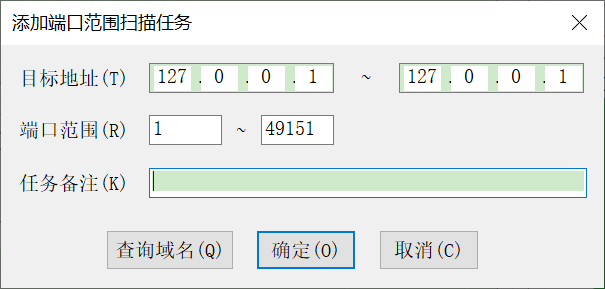


图3（左） “添加端口范围扫描任务”对话框

图4（右） “添加特定端口扫描任务”对话框

　　“基于地址扫描端口”面板（如图2所示）用于按地址扫描端口，即一个地址为一个任务，一个任务包含多个端口。开始时，用户点击“添加”按钮的下拉箭头，可以分别“添加端口范围扫描任务”（第I大类第i小类任务）和“添加特定端口扫描任务”（第I大类第ii小类任务），如图3和图4所示。虽然它们的第一行有个起始和终止的目标范围，但用户如果只需要扫描一个目标地址，在填写起始地址后，转移焦点时起始地址会自动带到终止地址的编辑框中。其中第ii小类的任务对话框的第二行是输入文本框，用户在其中输入以半角逗号或空格分隔的端口数字，点击“添加”按钮后，这些端口号才被添加目标列表中。另外添加目标地址时，程序也会检查是否包含本机地址（地址的主机段全0）、广播地址（地址的主机段全1）和所有主机地址（子网段和主机段全1），并提示用户。本程序支持批量添加，用户输入一个目标地址范围即能添加这个范围内的连续多个任务；也支持批量移除，用户可以一次移除选中的若干个任务。两个比较少见的高效操作是复制添加和批量修改：用户选中一个任务后，添加按钮会变成“复制添加”，此时用户点击此按钮就能弹出以该任务为蓝本的对应的添加对话框，由此免去用户填写大量重复的数据；此外，用户可以选择若干小类相同的任务，点击“修改”，即能同时修改这些任务的目标端口。多个扫描任务合称一个“作业”，作业内任务的顺序可以随时调整。用户编辑好后可以“保存”作业，方便下次“载入”以重新扫描。在系统资源管理器中，用户可以通过双击保存的作业直接启动程序，打开该作业。

　　如果一个任务正在进行，则程序会自动选中该任务；如果一个任务已经完成，则该任务项会打勾；如果一个第一大类的任务的目标地址PING不通，且用户在设置中没有勾选“即使PING失败，也要对该主机扫描端口”的选项，则该任务项会打叉。在扫描过程中用户不能修改作业的各种信息，但如果暂停作业，用户可以修改已执行任务的备注、未执行任务的各种信息，可以添加新任务，可以移除未执行任务或调整它们的执行顺序。如果用户希望面板在作业结束后恢复到初始状态，可以点击“清空”按钮，此时增加任务时的自增长编号也会重新从1开始。

　　右方的列表显示的是扫描进度，用户可以随时暂停或停止作业。而系统任务栏上的应用图标也会随扫描进度的变化而变化，从而让用户在不看界面时也能知道作业进度；而且系统托盘图标也会示意当前是“开始”、“暂停”还是“结束”状态。当一个作业有多个任务时，应用图标的进度是作业进度，表示已完成多少个任务；而当一个作业只有一个任务时，应用图标的进度是任务进度，第I大类作业表示已扫描多少个端口，第II大类作业表示已扫描多少个地址。如果用户暂停作业，程序会缓存当前扫描作业、作业进度、扫描结果，这样用户可以退出程序；下次启动时，程序会自动加载缓存，用户可以继续原来的作业。如果用户停止作业，则进度列表中未完成的项目会打叉，而已完成的项目则会打勾。另外，如果进程不幸崩溃，程序能够自动缓存当前工作状态并询问用户是否要重启；但我们仍然希望用户可以把这一崩溃现象报告给本工作室，让我们改进。

　　下方的“扫描结果”则列出扫描过程中发现的开放的端口，如果该端口在程序的端口字典中，则会连带给出其对应的应用层协议。但要注意的是，该应用层协议未必是目标主机真正开放的协议，目标主机可以不遵守公共约定，可以“挂羊头卖狗肉”。而“应用层扫描”一列则给出目标主机的真正的协议，如果本程序能够扫描出来。在扫描过程中，扫描结果是实时地按任务编号和端口号顺序插入到列表中的，用户可以不待扫描完全完成，就复制想要的扫描结果的地址和端口号，或者点击“HTTP(S)访问”，在浏览器中访问它们。控制行的最右侧实时显示了扫描的结果数量。如果有多个任务而用户想关注其中一个，可以点击“任务编号”下拉列表，从中一个任务，这样结果列表会暂时只列出此任务的结果。如果用户设置了“扫描结束后自动输出报告”，则这些结果会记录到一个新文件里。用户可以在扫描结束后打开、重命名和删除该文件，以及把文件另存为其它位置的其它格式。

## “基于端口扫描地址”

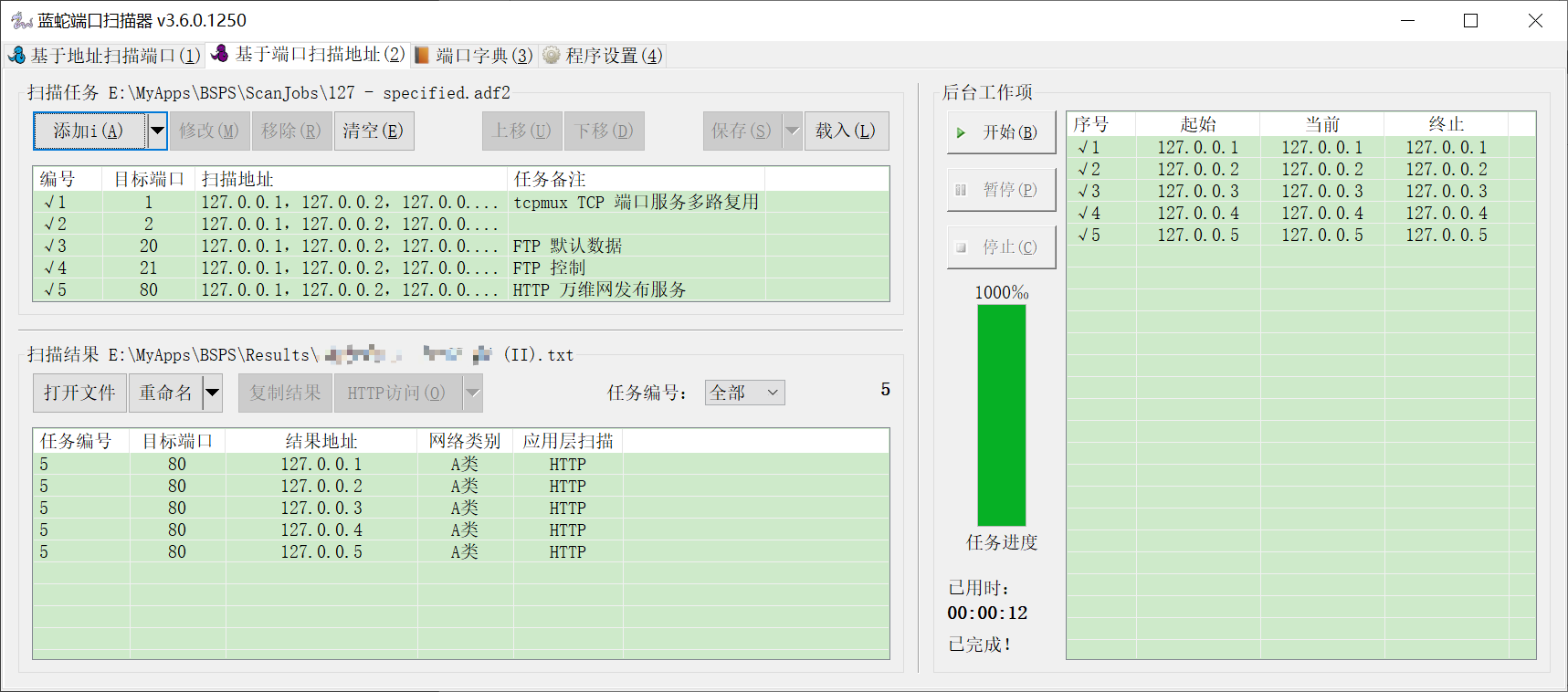


图5 “基于端口扫描地址”面板

　　“基于端口扫描地址” 面板（如图5所示）用于按端口扫描地址，即一个端口为一个任务，一个任务包含多个地址。在该面板中，用户拖动垂直的和水平的分割线可以调整三个区域的相对大小。用户调整任务列表各列的宽度后程序也会记住，下次启动时它们会自动调整为用户所调的宽度。

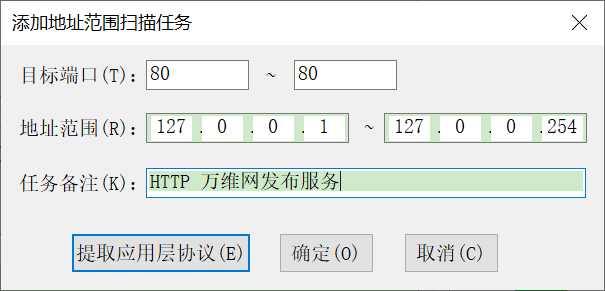
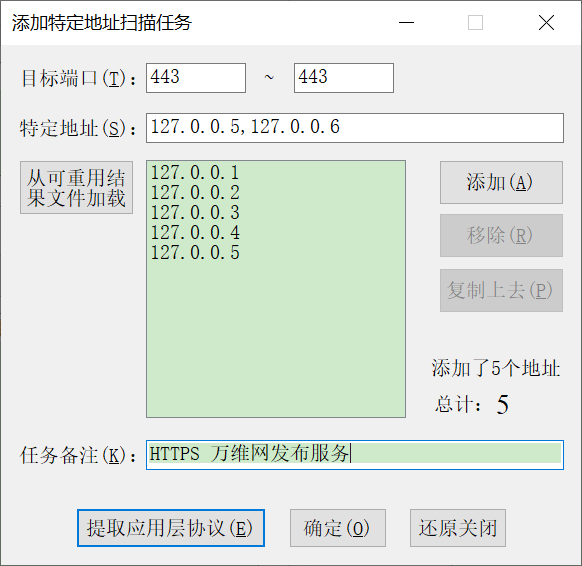
 

图6（左） “添加地址范围扫描任务”对话框

图7（右） “添加特定地址扫描任务”对话框

　　开始时，用户点击“添加”按钮的下拉箭头，可以分别“添加地址范围扫描任务”（第II大类第i小类任务）和“添加特定地址扫描任务”（第II大类第ii小类任务），如图6和图7所示。它们的功能和第I大类任务的类似。此后用户若要再添加相同类型的任务，只需点击“添加”按钮即可。另外，两大类的第ii小类的任务对话框可以根据需要调整大小，下次打开时对话框的大小是上次调整的大小；如果要恢复默认大小，可以点击“还原关闭”按钮。

　　本面板的其余部分功能和第I大类任务的类似。“扫描任务”和“扫描结果”的组框标题所显示的文件路径如果过长，过长部分会被截断，并省略显示。此外，两个作业面板的多个控制按钮都有双击鼠标对应的快捷操作，用户请把鼠标悬浮在按钮上查看。如果用户只是随便扫描下，可以不用停止作业而退出程序，程序会先进入“正在停止”状态，然后自动清理作业并退出。

## “端口字典”

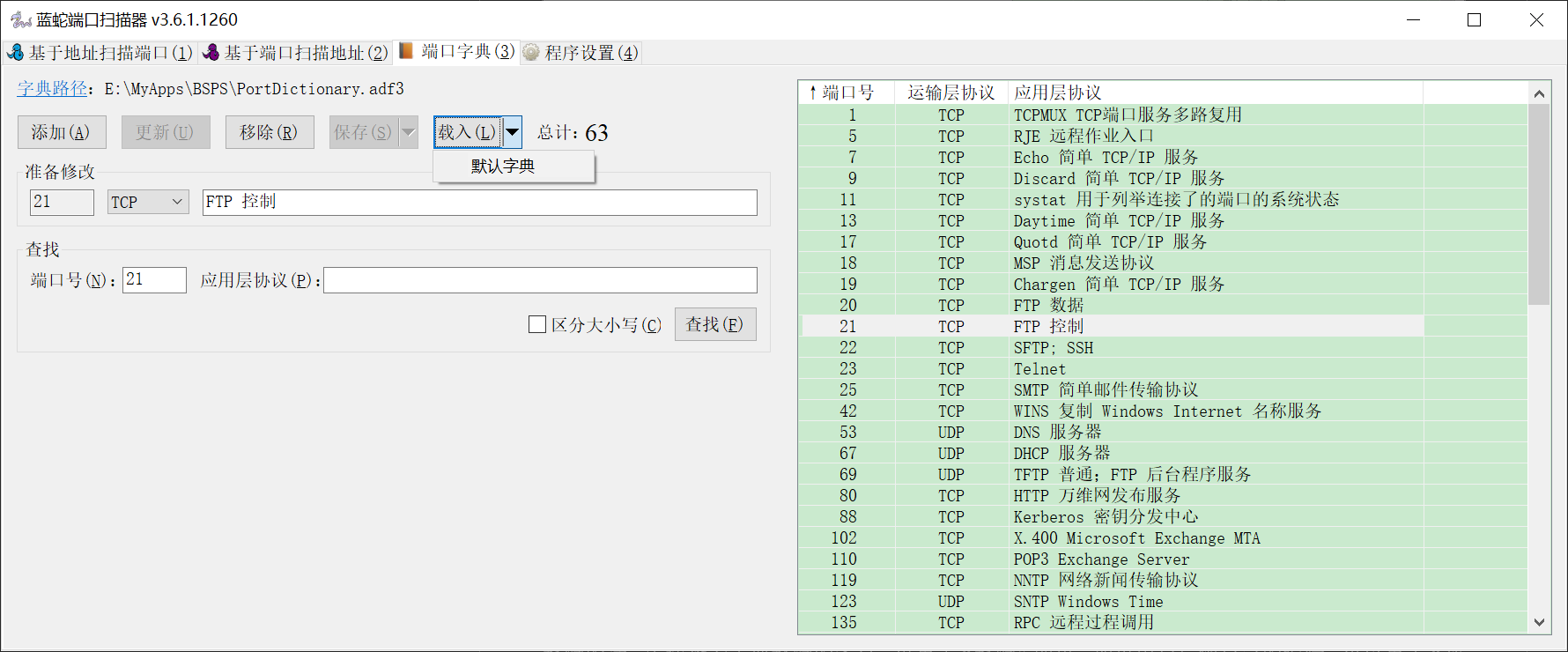


图8 “端口字典”面板

　　“端口字典”面板（如图8所示）主要用于查阅和编辑程序的端口字典。首次使用时，用户可点击“载入”按钮的下拉菜单的“默认字典”项，来加载默认的端口字典，加载后可点击“保存”把它存到一个扩展名为“adf3”的字典文件里；用户点击“字典路径”标签可以打开字典文件所在目录。在新增时，用户先点击“添加”，输入端口条目的端口号、选择运输层协议、输入应用层协议，再点击“插入”；如果已有相同端口号，程序会拒绝插入并提示用户。在修改时，用户先选择一个端口条目，修改运输层协议或应用层协议，再点击“更新”；如果用户在选择一个条目后按逃脱键，可以清空选择，清除左侧区域的端口内容。移除的话，先选择若干要移除的条目，再点击“移除”即可。如果用户后悔自己的编辑，可以点击“载入”，选择原来的端口字典，还原到原来状态。此外，用户可以编辑保存多个端口字典，执行不同作业时载入不同的字典。在系统资源管理器中，用户可以通过双击扩展名为“adf3”的文件来打开端口字典。

　　其次，用户可以通过端口号或应用层协议的文本内容查找端口条目，以了解条目的其它内容。两种查找条件一次只能使用一个，当互相切换焦点时，另一个文本框会被清空。在按应用层协议查找时，可以设置是否对查找内容区分大小写；如果有多个匹配结果，用户可以多次“查找”来循环查看它们。

　　最后，端口字典列表支持排序。用户点击列头可以对条目的某个属性按升序或降序排列。

## “程序设置”



图9 “程序设置”面板

“程序设置”面板（如图9所示）用于管理程序的各种设置。在这里，您可以设置关闭主界面时应用程序是退出程序还是隐藏窗口；可以“打开工作目录”以检查程序当前的工作目录；而“使用说明”会给出一些实用小技巧。如果您不关注扫描进度，可以在扫描过程中隐藏窗口，这样可以让程序免除刷新界面的操作，从而提升运行效率。如果中途需要控制全部作业的进度，可以右击系统托盘的程序图标，在弹出的托盘图标菜单中进行控制，如图10所示。如果当前工作目录是程序所在目录，您可以查看《许可协议》等文件。



图10 系统托盘图标菜单



图11 “htm”格式的扫描报告

　　“扫描设置”组框里有三种扫描并行模式，它们以各自的特点提升扫描效率。“多线程”模式每次启动作业较慢，暂停快捷；适合单次使用或执行总工作项数相差较大的多个作业。选择该模式后，再设置“每核线程数”，使程序扫描的总线程数限制在“每核线程数”乘以“CPU总核数”的数量内；如果因系统内存不足而创建线程失败，程序会自动清理线程，用户无需重启。“线程池”模式每次启动作业较快，暂停较慢；适合多次执行总工作项数差不多的一个或多个作业；选择该模式后，可再设置“总工作项数”。“流水线”模式只使用单线程就能并行扫描，暂停快捷，但应用层扫描效率很低；若要扫描应用层，应使用“.xml”输出格式，然后重用该结果文件。选择该模式后，可再设置“最大未决端口数”。注意，这些最值限制涉及多个方面，包括本机的线程和端口资源、通信网络的吞吐量、目标主机的响应端口数量等。并不要认为越大越好，太大可以提升扫描速率，但很容易使扫描结果失真；而且如果目标主机有一定的防扫机制，太大的端口并发量会很容易被目标主机判定为恶意客户端而拒绝回应。此外，用户可以统一设置这些模式的“运输层连接超时时长”，如果超过指定时长没有连接上，则认为该端口没有开放。程序提供了五种应用层扫描选项，如果命中，其结果会显示在扫描面板的结果列表的“应用层扫描”列中；而“连接超时时长”则对应用层扫描选项有效。在扫描时，建议用户把运输层扫描和应用层扫描分开进行，有利于提升效率；具体通过后文所述的“从可重用结果文件（.xml）加载”的方法进行。以上扫描设置在扫描进行时不可修改，但用户可以暂停全部作业以修改除“并行模式”外的其它设置。

　　用户可以在“扫描结果”组框里设置扫描结束后自动输出哪种格式的报告。目前有四种格式，每种格式都会按任务排列，显示每个任务的备注、目标，和扫描结果；扫描结果则会列出“结果端口”、“应用层协议”、“应用层扫描”三列内容。在文件末尾，报告还会输出“累计用时”、“结束状态”、“报告时间”和“扫描设置”，以尽可能减轻用户备注的负担。如果结束状态是“停止”，报告会输出是停止在哪个任务，任务的进度是多少。在这四种格式中，“.txt”是普通的文本文件；“.tsv”是制表符分隔值文件，可用Excel打开后编辑；“.htm”是网页文件，它的一个输出样子如图11所示。最后的“.xml”是可重用结果文件，在扫描完运输层端口后，用户可以通过添加第ii小类任务来“从可重用结果文件（.xml）加载”，如图4和图7所示。这样用户可以只重复检查这些确认开放的端口是否保持开放，提升工作效率。如果用户勾选了“自动输出报告”并设置了输出目录，那么开始扫描时，程序会先检查输出目录是否存在，如果不存在，则创建该目录。如果用户不这样设置，也可以在扫描完成后，点击扫描面板的“重命名”按钮的下拉菜单，单击“另存为”菜单项来手动保存结果。

　　最后，用户还可设置“两大类扫描作业都完成之后”程序要执行的操作，如关机、睡眠、休眠和播放音频。如果是播放音频而没有设置音频文件，程序会用系统蜂鸣声来播放一曲《生日快乐》。有的用户的机器的蜂鸣声失效，此时只能用户自己指定一个mp3或wav文件来给程序播放。真正播放之前，用户可以试听播放效果，可以从“系统音量”一行中明确系统音量大小和是否静音；如果电脑声卡或声卡驱动不可用，则这行控件就不可用。

此外，对于“输出目录”和“音频文件”两个路径文本框，如果所给路径非法或者不存在，文本框背景会变成灰色，以提示用户调整。

## 查询域名的IP地址

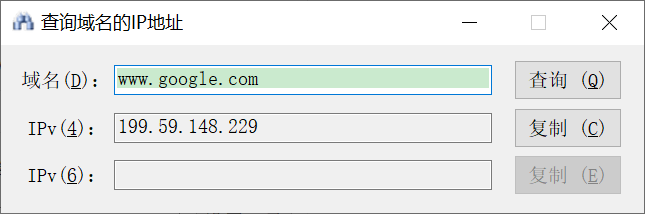


图12 “查询域名的IP地址”对话框

　　如图3、图4的“查询域名”按钮和图10的系统托盘菜单所示，用户可以通过三个途径打开“查询域名的IP地址”对话框（如图12所示）。在该对话框中，用户可以输入要查询的域名，按“查询”按钮后显示该域名对应的IPv4地址和IPv6地址（如果有的话），再单击对应的“复制”按钮复制地址。有的用户复制的地址不能在程序中粘贴，此时可以先粘贴到记事本中（记事本程序可在对话框的图标菜单中打开），再从记事本中复制，就能粘贴到程序中了。

　　本对话框以非模态形式显示，用户无需关闭它也能操作主界面。而如果用户退出程序，它也会被一起关闭。

# 【产品适用对象】

　　服务器管理员、网吧管理员、服务器开发人员、网络安全从业人员和爱好者、企事业单位网络管理员、网络组建商、高校学生，等等。

# 【产品适用场景】

## 检查服务器端口

　　用户可以使用“基于地址扫描端口”面板或“基于端口扫描地址”面板检查一台或多台服务器的指定端口是否开放。程序会自动输出报告，方便用户备案和翻阅。

## 发现主机端口

　　用户可以使用范围端口扫描来发现一台或多台主机开放了哪些端口。

## 发现服务主机

　　用户可以使用“基于端口扫描地址”面板，搭配“应用层”扫描设置，发现哪些主机提供哪些服务。

　　特别指出，以上三种场景本产品都适合大规模操作，因而会很适合大型组织里的例行操作。

## 学习计算机网络知识

　　学生可以通过使用本软件来做一些计算机网络的实验，加深对计算机网络课程的认识和理解，打通计算机网络五层教学协议的知识关联，发现书本上没有讲述的知识点。

## 查询端口字典

　　用户可以使用“端口字典”面板，来查询端口的准确的公共约定。

## 查询域名IP

　　用户可以使用“查询域名的IP地址”对话框，来查询某个域名绑定的IP地址。

## 更多场景

　　期待您的解锁和建议！