(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106203105 B
(45)授权公告日 2019.07.09

(21)申请号 201610483699.0

(22)申请日 2012.10.16

(65)同一申请的已公布的文献号
申请公布号 CN 106203105 A

(43)申请公布日 2016.12.07

(62)分案原申请数据
201210393609.0 2012.10.16

(73)专利权人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
专利权人 奇智软件(北京)有限公司

(72)发明人 苗汇泉 宁敢

(74)专利代理机构 北京鼎佳达知识产权代理事务所(普通合伙) 11348
代理人 王伟锋 刘铁生

(51)Int.Cl.
G06F 21/56(2013.01)

(56)对比文件
CN 101079689 A,2007.11.28,全文.
陈敏.智能手机反病毒引擎设计及其重要模块的实现.《中国优秀硕士学位论文全文数据库》.2011,(第4期),第1-81页.

审查员 潘秋羽

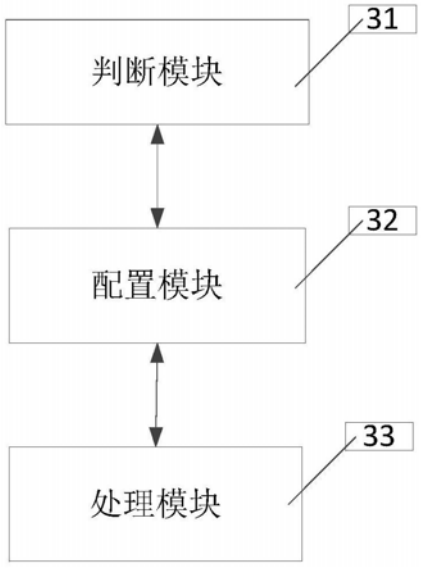
权利要求书1页 说明书6页 附图2页

(54)发明名称

文件管理方法和装置

(57)摘要

本发明公开了一种文件管理方法和装置,该装置包括:判断模块,用于对移动设备的存储空间进行扫描,判断所述存储空间中是否包含需要处理的文件;配置模块,用于在判断包含需要处理的文件的情况下,在所述存储空间中创建文件夹,并将所述需要处理的文件放入所述文件夹中;处理模块,用于根据指示对所述文件夹中存储的文件进行处理;其中,所述判断模块用于判断所述存储空间是否包含可疑文件和/或恶意文件;并判断所述存储空间包含可疑文件和/或恶意文件的情况下,将所述存储空间中的可疑文件和/或恶意文件确定为需要处理的文件。采用本发明的技术方案能够有效恢复或查阅移动设备原存储的文件,避免操作无法进行的问题。



CN 106203105 B

1.一种文件管理方法,用于对U盘上的文件进行管理,其包括:

服务器对U盘存储空间内的文件进行云查杀扫描,获得被扫描文件的后台文件等级,同时在服务器中,设置文件对应的文件等级码,所获得的文件等级与所设置的文件等级码进行对比,判断所述存储空间中是否包含需要处理的文件;

如果包含需要处理的文件,则在所述存储空间中创建文件夹,并将所述需要处理的文件放入所述文件夹中;

根据指示对所述文件夹中存储的文件进行处理;

其中,判断所述存储空间中是否包含需要处理的文件包括:

判断所述存储空间是否包含可疑文件和/或恶意文件;

如果所述存储空间包含可疑文件和/或恶意文件,则将所述存储空间中的可疑文件和/或恶意文件确定为需要处理的文件。

2.根据权利要求1所述的文件管理方法,其特征在于,在将所述需要处理的文件放入所述文件夹中之后,所述文件管理方法进一步包括:

接收来自用户的指示,根据所述指示确定对所述文件夹中的文件需要进行的处理。

3.根据权利要求2所述的文件管理方法,其特征在于,在来自用户的指示为恢复所述文件夹中的文件的情况下,对所述文件夹中的文件进行处理包括:

将所述文件夹中的文件恢复到原存储位置。

4.根据权利要求2所述的文件管理方法,其特征在于,在来自用户的指示为删除所述文件夹中的文件的情况下,对所述文件夹中的文件进行处理包括:

将所述文件夹中的文件删除。

5.一种文件管理装置,用于对U盘上的文件进行管理,其包括:

判断模块,服务器对U盘存储空间内的文件进行云查杀扫描,获得被扫描文件的后台文件等级,同时在服务器中,设置文件对应的文件等级码,所获得的文件等级与所设置的文件等级码进行对比,判断所述存储空间中是否包含需要处理的文件;

配置模块,用于在判断包含需要处理的文件的情况下,在所述存储空间中创建文件夹,并将所述需要处理的文件放入所述文件夹中;

处理模块,用于根据指示对所述文件夹中存储的文件进行处理;

其中,所述判断模块用于判断所述存储空间是否包含可疑文件和/或恶意文件;并判断所述存储空间包含可疑文件和/或恶意文件的情况下,将所述存储空间中的可疑文件和/或恶意文件确定为需要处理的文件。

6.根据权利要求5所述的文件管理装置,其特征在于,还包括:

确定模块,用于在将所述需要处理的文件放入所述文件夹中之后,接收来自用户的指示,并根据所述指示确定对所述文件夹中的文件需要进行的处理。

7.根据权利要求6所述的文件管理装置,其特征在于,在来自用户的指示为恢复所述文件夹中的文件的情况下,所述处理模块用于将所述文件夹中的文件恢复到原存储位置。

8.根据权利要求6所述的文件管理装置,其特征在于,在来自用户的指示为删除所述文件夹中的文件的情况下,所述处理模块用于将所述文件夹中的文件删除。

文件管理方法和装置

[0001] 本申请为基于母案《文件管理方法和装置》的分案申请，母案《文件管理方法和装置》的申请号为CN201210393609.0、公开号为CN102915359A。

技术领域

[0002] 本发明涉及计算机领域，具体涉及一种文件管理方法和装置。

背景技术

[0003] 随着计算机技术在社会生活中各个领域的广泛运用，恶意程序(Malwar，malicious software，指任何故意创建用来执行未经授权并通常是有害行为的软件程序)也如同其附属品一样接踵而来。由于这些恶意程序所具有的感染性、复制性及破坏性，其已成为困扰计算机使用的一个重大问题。

[0004] 因此，在网络威胁日益增长的今天，更新病毒特征码成为企业及网民每天必备的工作，从每周一次到每天一次，直至时刻更新，用户期望通过病毒特征码的匹配来避免计算机设备被恶意程序所影响。而传统杀毒软件是将病毒库放在客户端计算机，在客户端进行文件的分析工作，在扫描过程中会反复在本地病毒库中进行比对，占用大量系统资源，并且随着病毒库的不断升级，病毒库的容量越来越大，分析文件时所耗费的时间也越来越长，导致客户端计算机的系统资源占用过多，性能降低，因此，反病毒行业必须寻找新的技术突破。

[0005] “云安全(Cloud Security)”计划是网络时代信息安全的最新体现，它融合了并行处理、网格计算、未知病毒行为判断等新兴技术概念，将“云计算”的理念应用到了安全领域。

[0006] 云查杀是指把病毒库放在服务端，因为服务端的病毒库更新更快、更及时，联网后可以快速的进行查杀的技术。在采用云查杀技术对U盘(移动设备)进行扫描之后，通常的做法是将经过云查杀扫描之后得到的危险(判断为恶意文件)或可疑文件存放在本地计算设备上。

[0007] 由于把对U盘进行云查杀之后得到的危险或可疑文件存放在了本地计算设备上，所以当把U盘从本地计算设备移动到另一台计算设备上时，如果此时要在另一台计算设备上恢复误删的危险或可疑文件，则是办不到的。

[0008] 针对相关技术中在计算设备侧存储被隔离的文件而导致难以基于移动设备对文件进行后续其他处理的问题，目前尚未提出有效的解决方案。

发明内容

[0009] 鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的文件管理方法和装置。

[0010] 依据本发明的一个方面，提供了文件管理方法，该文件管理方法包括：

[0011] 对移动设备的存储空间进行扫描，判断存储空间中是否包含需要处理的文件；

[0012] 如果包含需要处理的文件，则在存储空间中创建文件夹，并将需要处理的文件放入文件夹中；

[0013] 根据指示对文件夹中存储的文件进行处理；

[0014] 其中，判断存储空间中是否包含需要处理的文件包括：

[0015] 判断存储空间是否包含可疑文件和/或恶意文件；

[0016] 如果存储空间包含可疑文件和/或恶意文件，则将存储空间中的可疑文件和/或恶意文件确定为需要处理的文件。

[0017] 任选地，在将需要处理的文件放入文件夹中之后，文件管理方法进一步包括：

[0018] 接收来自用户的指示，根据指示确定对文件夹中的文件需要进行的处理。

[0019] 任选地，在来自用户的指示为恢复文件夹中的文件的情况下，对文件夹中的文件进行处理包括：

[0020] 将文件夹中的文件恢复到原存储位置。

[0021] 任选地，在来自用户的指示为删除文件夹中的文件的情况下，对文件夹中的文件进行处理包括：

[0022] 将文件夹中的文件删除。

[0023] 根据本发明的另一方面，提供了一种文件管理装置，该文件管理装置包括：

[0024] 判断模块，用于对移动设备的存储空间进行扫描，判断存储空间中是否包含需要处理的文件；

[0025] 配置模块，用于在判断包含需要处理的文件的情况下，在存储空间中创建文件夹，并将需要处理的文件放入文件夹中；

[0026] 处理模块，用于根据指示对文件夹中存储的文件进行处理；

[0027] 其中，判断模块用于判断存储空间是否包含可疑文件和/或恶意文件；并判断存储空间包含可疑文件和/或恶意文件的情况下，将存储空间中的可疑文件和/或恶意文件确定为需要处理的文件。

[0028] 任选地，该文件管理装置进一步包括：

[0029] 确定模块，用于在将需要处理的文件放入文件夹中之后，接收来自用户的指示，并根据指示确定对文件夹中的文件需要进行的处理。

[0030] 任选地，在来自用户的指示为恢复文件夹中的文件的情况下，处理模块用于将文件夹中的文件恢复到原存储位置。

[0031] 任选地，在来自用户的指示为删除文件夹中的文件的情况下，处理模块用于将文件夹中的文件删除。

[0032] 根据本发明的文件管理方法和装置可以通过对移动设备的存储空间进行扫描，在判断存储空间中有需要处理的文件的情况下，在该移动设备的存储空间中建立文件夹，并将需要处理的文件放入该文件夹中进行处理，由此解决了在计算设备侧存储被隔离的文件而导致难以基于移动设备对文件进行后续其他处理的问题，取得了在移动设备的存储空间中存储需要处理的文件，即使移动设备与其他的计算机连接，同样能够有效恢复或查阅移动设备原存储的文件，避免操作无法进行的问题的有益效果。

[0033] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够

更明显易懂,以下特举本发明的具体实施方式。

附图说明

[0034] 通过阅读下文优选实施方式的详细描述,各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的,而并不认为是对本发明的限制。而且在整个附图中,用相同的参考符号表示相同的部件。在附图中:

[0035] 图1示出了根据本发明一个实施例的文件管理方法的流程图;

[0036] 图2示出了根据本发明一个实施例的文件管理方法执行结果的示意图;以及

[0037] 图3示出了根据本发明一个实施例文件管理装置的框图。

具体实施方式

[0038] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例,然而应当理解,可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反,提供这些实施例是为了能够更透彻地理解本公开,并且能够将本公开的范围完整的传达给本领域的技术人员。

[0039] 根据本发明的实施例,提供了一种文件管理方法。

[0040] 如图1所示,文件管理方法包括:

[0041] 步骤S101,对移动设备的存储空间进行扫描,判断存储空间中是否包含需要处理的文件;

[0042] 步骤S103,如果包含需要处理的文件,则在存储空间中创建文件夹,并将需要处理的文件放入文件夹中;

[0043] 步骤S105,根据指示对文件夹中存储的文件进行处理。

[0044] 其中,判断存储空间中是否包含需要处理的文件包括:

[0045] 判断存储空间是否包含可疑文件和/或恶意文件;

[0046] 如果存储空间包含可疑文件和/或恶意文件,则将存储空间中的可疑文件和/或恶意文件确定为需要处理的文件。

[0047] 并且,在将需要处理的文件放入文件夹中之后,文件管理方法进一步包括:

[0048] 接收来自用户的指示,根据指示确定对文件夹中的文件需要进行的处理。

[0049] 此外,在来自用户的指示为恢复文件夹中的文件的情况下,对文件夹中的文件进行处理包括:

[0050] 将文件夹中的文件恢复到原存储位置。

[0051] 而且,在来自用户的指示为删除文件夹中的文件的情况下,对文件夹中的文件进行处理包括:

[0052] 将文件夹中的文件删除。

[0053] 例如,将移动设备连接到一台计算设备上,服务器联网后扫描用户U盘(移动设备)上的文件,查到文件的md5对应的文件等级;其中,服务器扫描查询后台文件等级,后台保存有不同的文件的md5及对应的文件等级。文件等级主要是根据程序文件内的静态特征,如经由信息-摘要算法(Message-Digest Algorithm 5,简称md5)运算得出的md5验证码,或SHA1码,或循环冗余校验(Cyclic Redundancy Check,简称CRC)码等可唯一标识原程序的特征

码,也可以是程序文件内的静态特征串。

[0054] 首先,在服务器中,设文件对应的文件等级码数值为10-20是白的(即安全文件,或称为可信文件),文件对应的文件等级码数值为30是未知的(即可疑文件),不在白名单(白名单可以是可信任文件的列表),也不在黑名单(黑名单可以是恶意文件的列表),文件对应的文件等级码数值为50-70都是黑的(即恶意文件)。当U盘连接云数据库时,根据文件的md5可以查询到该码数值。

[0055] 然后把找到的危险(恶意)或可疑文件放入隔离区(即在移动设备的存储空间中创建的文件夹)中。应当注意,在一些实施例中,可疑文件也可以不放入隔离区。

[0056] 对于u盘扫描后台采用的等级,主要是根据后台收集到的某个文件的PE文件的等级,若非PE文件的等级>=30,则是可疑文件;若PE文件等级>=50,则是危险(恶意)文件;若PE文件的等级=70,则是木马文件。

[0057] 如图2所示,为对移动设备中的文件的扫描结果。当一台计算设备上插入移动设备时,云查杀扫描并确认文件有异常时,包括文件为可疑文件、危险文件或木马文件。

[0058] 例如,在图2中,文件名为auto.bat的文件为可疑文件,文件名为setup-guiying.exe和文件名为pucgc5951飓风.exe的文件为木马文件。

[0059] 用户可以选择暂不处理、立即处理或立即处理并全面扫描U盘等指令。

[0060] 当用户选择“立即处理”指令后,在u盘创建“隔离文件”的文件夹,将需要处理的文件放入到“隔离文件”的文件夹中进行处理。

[0061] 如果被放入隔离区中的危险或可疑文件被误报或误处理,并且需要恢复该危险或可疑文件时,直接从该隔离区把该危险或可疑文件恢复到其原始位置。

[0062] 根据本发明的实施例,提供了一种文件管理装置。

[0063] 如图3所示,文件管理装置包括:

[0064] 判断模块31,用于对移动设备的存储空间进行扫描,判断存储空间中是否包含需要处理的文件;

[0065] 配置模块32,用于在判断包含需要处理的文件的情况下,在存储空间中创建文件夹,并将需要处理的文件放入文件夹中;

[0066] 处理模块33,用于根据指示对文件夹中存储的文件进行处理。

[0067] 其中,判断模块31用于判断存储空间是否包含可疑文件和/或恶意文件;并判断存储空间包含可疑文件和/或恶意文件的情况下,将存储空间中的可疑文件和/或恶意文件确定为需要处理的文件。

[0068] 并且,该文件管理装置进一步包括:

[0069] 确定模块(图中未示出),用于在将需要处理的文件放入文件夹中之后,接收来自用户的指示,并根据指示确定对文件夹中的文件需要进行的处理。

[0070] 此外,在来自用户的指示为恢复文件夹中的文件的情况下,处理模块33用于将文件夹中的文件恢复到原存储位置。

[0071] 而且,在来自用户的指示为删除文件夹中的文件的情况下,处理模块33用于将文件夹中的文件删除。

[0072] 借助于本发明的技术方案,把例如U盘之类的移动设备连接到任意一台计算设备上,都能够在该台计算设备恢复在该移动设备上先前被误删除的危险(恶意)或可疑文件。

[0073] 综上所述，借助于本发明的上述技术方案，通过对移动设备的存储空间进行扫描，在判断存储空间中有需要处理的文件的情况下，在该移动设备的存储空间中建立文件夹，并将需要处理的文件放入该文件夹中进行处理，能够在移动设备的存储空间中存储需要处理的文件，即使移动设备与其他的计算机连接，同样能够有效恢复或查阅移动设备原存储的文件，避免操作无法进行的问题。

[0074] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0075] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0076] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0077] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0078] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0079] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例的文件管理方法和装置中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如，计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式

提供。

[0080] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

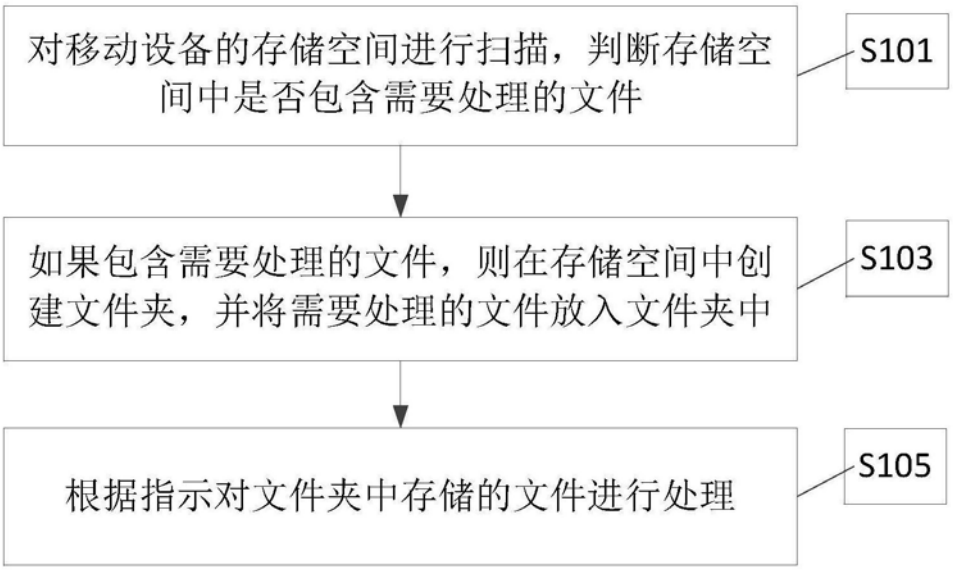

对移动设备的存储空间进行扫描，判断存储空间中是否包含需要处理的文件
S101
如果包含需要处理的文件，则在存储空间中创建文件夹，并将需要处理的文件放入文件夹中
S103
根据指示对文件夹中存储的文件进行处理
S105

图1


发现U盘中有危险文件，建议全面扫描U盘！
auto.bat
I:\auto.bat
可疑文件
添加信任
打开目录
setup-guiying.exe
I:\setup-guiying.exe
木马文件
添加信任
打开目录
pucgc5951飓风.e...
I:\pucgc5951飓风.exe
木马文件
添加信任
打开目录
全选
暂不处理
立即处理
立即处理并全面扫描U盘

图2

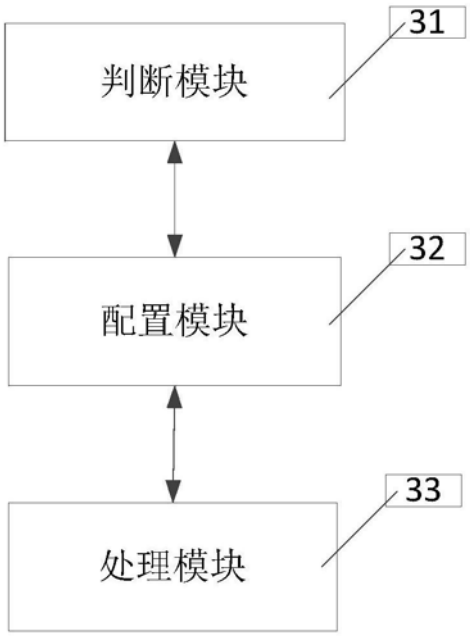


图3