(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 109033313 B
(45)授权公告日 2020.09.25

(21)申请号 201810786552.8
(22)申请日 2018.07.17
(65)同一申请的已公布的文献号
申请公布号 CN 109033313 A
(43)申请公布日 2018.12.18
(73)专利权人 北京明朝万达科技股份有限公司
地址 100097 北京市海淀区蓝靛厂南路25号嘉友国际大厦区2层
(72)发明人 龚剑 孙加光 喻波 王志海 魏效征 安鹏
(51)Int.Cl.
G06F 16/18(2019.01)
G06F 16/13(2019.01)

(56)对比文件
CN 105389509 A,2016.03.09
CN 108009430 A,2018.05.08
CN 108052833 A,2018.05.18
CN 106446707 A,2017.02.22
US 9465937 B1,2016.10.11
李锁雷等.《公安内网敏感信息监测系统技术研究》.《警察技术》.2017,正文第1段-倒数第1段.

审查员 张秀娟

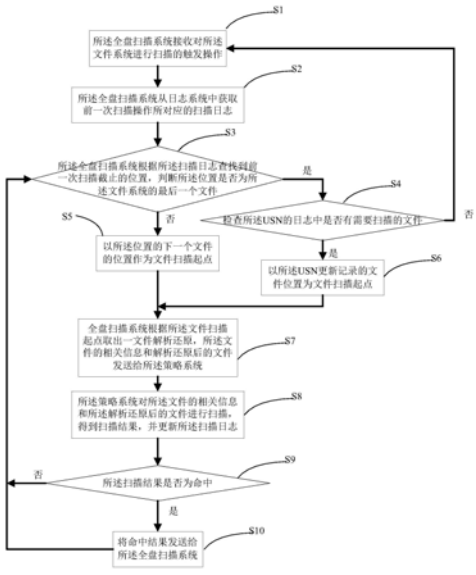
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种应用USN实现全盘扫描功能的方法和终端设备

(57)摘要

本发明公开了一种应用USN实现全盘扫描功能的方法和终端设备，该方法包括：全盘扫描系统接收对文件系统进行扫描的触发操作；从日志系统中获取前一次扫描操作所对应的扫描日志；根据文件扫描起点，依次取出一文件解析还原，所述文件的相关信息和解析还原后的文件发送给策略系统；所述策略系统对所述文件的相关信息和所述解析还原后的文件进行扫描，得到扫描结果，并更新所述扫描日志；如果所述扫描结果是命中，则将命中结果发送给所述全盘扫描系统。所述方法和终端设备应用了更新序列号USN和策略规则来实现全盘扫描，提高了全盘扫描的安全性和灵活性。



CN 109033313 B

1.一种应用更新序列号USN实现全盘扫描的方法,用于对终端的文件进行扫描,其特征在于,所述终端部署有全盘扫描系统和策略系统,执行下述步骤:

步骤1:所述全盘扫描系统接收对文件系统进行扫描的触发操作;

步骤2:所述全盘扫描系统从日志系统中获取前一次扫描操作所对应的扫描日志;

步骤3:所述全盘扫描系统根据所述扫描日志查找到前一次扫描截止的位置,判断所述位置是否为所述文件系统的最后一个文件,如果为是,则转步骤4;如果为否,则以所述位置的下一个文件的位置作为文件扫描起点,转步骤5;

步骤4:检查所述USN的日志中是否有需要扫描的记录,如果是,则以所述USN更新记录的文件位置为文件扫描起点,如果否,则所述扫描全部完成,转步骤1;

步骤5:全盘扫描系统根据所述文件扫描起点取出一文件解析还原,所述文件的相关信息和解析还原后的文件发送给策略系统;

步骤6:所述策略系统对所述文件的相关信息和所述解析还原后的文件进行扫描,得到扫描结果,并更新所述扫描日志;

步骤7:所述扫描结果是否为命中,如果是,则将命中结果发送给所述全盘扫描系统,并转步骤2;如果否,则转步骤2;

所述策略系统包括以下至少一种策略规则,并以所述策略规则对文件进行扫描:

(1)检索策略规则,所述检索策略规则包括一系列人员、设备或者目录的名单或者数据标识符,对满足所述名单或者所述数据标识符的所述文件的相关信息或者所述解析还原后的文件,进行扫描;

(2)白名单策略规则,所述白名单策略规则包括一系列人员、设备或者目录的名单,对符合所述名单或者所述数据标识符的所述扫描的所述文件的相关信息或者所述解析还原后的文件,免于扫描。

2.如权利要求1所述的方法,其特征在于,所述全盘扫描系统接收所述策略系统返回的结果,将所述扫描的结果存储到所述日志系统中。

3.如权利要求1所述的方法,其特征在于,所述更新所述扫描日志包括:

将当前扫描文件的文件索引表的索引添加到所述扫描日志的记录中。

4.如权利要求1所述的方法,其特征在于,所述全盘扫描系统接收对所述文件进行扫描的触发操作前,还包括:

步骤1.1:用户开启全盘扫描功能,所述全盘扫描系统对终端文件系统的所有文件建立索引表,所述索引的结果缓存到全盘扫描系统的用户数据文件中。

5.如权利要求1所述的方法,其特征在于,所述策略系统对所述文件的相关信息和所述解析还原后的文件进行扫描前,包括:

步骤6.1:管理员或用户设置所述策略系统,配置扫描的时间段;

当时间满足所述配置扫描的时间段时,触发全盘扫描系统对所述文件信息进行扫描;或者采取手动方式触发全盘扫描系统对所述文件信息进行扫描。

6.如权利要求1所述的方法,其特征在于,所述策略系统对所述文件的相关信息和所述解析还原后的文件进行扫描包括:针对所述文件相关信息的扫描,或者针对所述解析还原后的文件内容进行扫描。

7.如权利要求1所述的方法,其特征在于,所述策略系统中预设一些常用的敏感内容的

数据标识符，所述数据标识符包括：身份证信息、营业执照信息、和/或银行卡号，并提供正向关键字、反向关键字、模糊关键字以及正则表达式规则，以便于配置策略规则。

8.如权利要求1所述的方法，其特征在于，检查所述USN的日志中是否有需要扫描的文件，包括：

检查所述USN中的记录中对应的文件是否已经被正在进行的扫描过程扫描过，如果是，则所述记录对应的文件不需要扫描，如果否，则所述记录对应的文件需要扫描。

9.如权利要求1所述的方法，其特征在于，所述触发操作包括以下任一种：

(1)具有参数的触发操作，所述参数用于修改所述步骤2中所述前一次扫描操作的扫描日志；

(2)无参数触发操作，即不修改所述步骤2中所述前一次扫描操作的扫描日志；

其中，所述修改所述步骤2中所述前一次扫描操作的扫描日志是指修改所述前一次扫描截止的位置。

10.一种应用USN实现全盘扫描的终端设备，其特征在于，所述终端设备部署有全盘扫描系统和策略系统；

所述全盘扫描系统接收对文件系统进行扫描的触发操作；

所述全盘扫描系统从日志系统中获取前一次扫描操作所对应的扫描日志；

所述全盘扫描系统根据所述扫描日志查找到前一次扫描截止的位置为所述文件系统的最后一个文件，检查所述USN的日志中是否有需要扫描的记录，如果是，则以所述USN更新记录的文件位置为文件扫描起点，如果否，则所述扫描全部完成；

所述全盘扫描系统根据所述扫描日志查找到前一次扫描截止的位置不是所述文件系统的最后一个文件，则以所述位置的下一个文件的位置作为文件扫描起点，根据所述文件扫描起点取出一文件解析还原，所述文件的相关信息和解析还原后的文件发送给策略系统；

所述策略系统对所述文件的相关信息和所述解析还原后的文件进行扫描，得到扫描结果，并更新所述扫描日志，如果所述扫描结果命中，则将命中结果发送给所述全盘扫描系统；

所述策略系统包括以下至少一种策略规则，并以所述策略规则对文件进行扫描：

(1)检索策略规则，所述检索策略规则包括一系列人员、设备或者目录的名单或者数据标识符，对满足所述名单或者所述数据标识符的所述文件的相关信息或者所述解析还原后的文件，进行扫描；

(2)白名单策略规则，所述白名单策略规则包括一系列人员、设备或者目录的名单，对符合所述名单或者所述数据标识符的所述扫描的所述文件的相关信息或者所述解析还原后的文件，免于扫描。

11.一种应用USN实现全盘扫描的终端设备，其特征在于，包括：处理器，存储器，所述处理器执行所述存储器 上的程序实现如权利要求1-9任一项所述的方法。

一种应用USN实现全盘扫描功能的方法和终端设备

技术领域

[0001] 本公开属于计算机领域，具体地说，是一种应用USN实现全盘扫描功能的方法和终端设备。

背景技术

[0002] 在计算机应用中，常常需要对由磁盘或者硬盘构成的存储系统中的文件进行扫描，最常见的扫描方式是全盘扫描，传统的全盘扫描通过枚举待扫描的存储系统中的文件，比如先从存储系统的根目录枚举文件，枚举以后再一个一个的传送给后面的扫描引擎，一个或多个扫描引擎在扫描文件之后得出一个扫描结果。但这种扫描方式比较浪费时间，并且消耗系统资源。为了克服全盘扫描的不足，专利WO2017084557A1提出了一种用于查杀病毒的文件扫描方法，该方法利用递增日志记录前次扫描的截止位置实现递增扫描查杀病毒，以减少传统全盘扫描的扫描时间。

[0003] 与此同时，无论是传统的全盘扫描，还是递增方式的全盘扫描，现有技术提供的扫描通常是病毒扫描引擎，只能对用户提供一个基于已有病毒库的扫描结果，没有考虑到很多企业用户比较关注对敏感信息的扫描，即扫描的策略不能够根据用户的需求定制；并且，为了保证扫描结果的准确性，大多会要求终端提供上网的功能，而这对敏感数据要求比较高的用户，也会存在潜在的安全风险。

[0004] 另外，如果扫描后的文件发生新的文件操作，如添加、删除或者修改等文件操作时，现有的全盘扫描并不能知晓这些操作是否发生在扫描后，因此会遗漏对这些文件做再次扫描的操作，也会带来数据安全风险。

发明内容

[0005] 鉴于解决现有技术中存在的上述问题，本公开的目的在于提供一种应用USN实现全盘扫描功能的方法和终端设备。

[0006] 本公开提供了一种应用更新序列号USN实现全盘扫描的方法，用于对终端的文件进行扫描，其特征在于所述终端部署有全盘扫描系统和策略系统，执行下述步骤：

[0007] 步骤1：所述全盘扫描系统接收对所述文件系统进行扫描的触发操作；

[0008] 步骤2：所述全盘扫描系统从日志系统中获取前一次扫描操作所对应的扫描日志；

[0009] 步骤3：所述全盘扫描系统根据所述扫描日志查找到前一次扫描截止的位置，判断所述位置是否为所述文件系统的最后一个文件，如果为是，则转步骤4；如果为否，则以所述位置的下一个文件的位置作为文件扫描起点，转步骤5；

[0010] 步骤4：检查所述USN的日志中是否有需要扫描的记录，如果是，则以所述USN更新记录的文件位置为文件扫描起点，如果否，则所述扫描全部完成，转步骤1；

[0011] 步骤5：全盘扫描系统根据所述文件扫描起点取出一文件解析还原，所述文件的相关信息和解析还原后的文件发送给策略系统；

[0012] 步骤6：所述策略系统对所述文件的相关信息和所述解析还原后的文件进行扫描，

得到扫描结果，并更新所述扫描日志；

[0013] 步骤7：所述扫描结果是否为命中，如果是，则将命中结果发送给所述全盘扫描系统，并转步骤2；如果否，则转步骤2。

[0014] 本公开提供的所述方法中的策略系统可配置成对敏感信息的扫描策略，则能防护数据泄密(泄露)。

[0015] 另外，本公开提供的所述方法能够避免更新文件“逃避”扫描的情况，例如：当扫描完一个文件后，所述文件又发生更新，此时，这个更新文件就不会被再次扫描，从而“逃避”了扫描，当更新的内容属于非法信息时，就会给系统带来安全隐患，而本公开提供的技术方案由于还需要检查USN日志中的信息，因此，即使被一个文件被扫描后在发生更新，但这个更新的信息会被记录在USN日志中，因此更新文件的原始文件即使被扫描后，但只要其发生了更新，也会被再次扫描，即实现增量扫描，从而有效避免上述安全隐患。

[0016] 在上述技术方案的基础上，进一步的，所述全盘扫描系统接收所述策略系统返回的结果，将所述扫描的结果存储到所述日志系统中。

[0017] 在上述技术方案的基础上，进一步的，所述更新所述扫描日志包括：

[0018] 将当前扫描文件的位置添加到所述扫描日志的记录中。

[0019] 在上述技术方案的基础上，进一步的，所述全盘扫描系统接收对所述文件进行扫描的触发操作前，还包括：

[0020] 步骤1.1：用户开启全盘扫描功能，所述全盘扫描系统对终端文件系统的所有文件建立索引表，所述索引的结果缓存到全盘扫描系统的用户数据文件中。

[0021] 在上述技术方案的基础上，进一步的，所述位置包括文件索引表的索引。

[0022] 在上述技术方案的基础上，进一步的，所述策略系统对所述文件的相关信息和所述解析还原后的文件进行扫描前，包括：

[0023] 步骤6.1：管理员或用户设置所述策略系统，配置扫描的时间段。

[0024] 在上述技术方案的基础上，进一步的，当时间满足所述配置扫描的时间段时，触发全盘扫描系统对所述文件信息进行扫描；或者采取手动方式触发全盘扫描系统对所述文件信息进行扫描。

[0025] 在上述技术方案的基础上，进一步的，所述文件的相关信息包括至少以下一种：(1)存储位置、(2)名字、(3)作者、(4)大小、(5)类型。

[0026] 在上述技术方案的基础上，进一步的，所述策略系统对所述文件的相关信息和所述解析还原后的文件进行扫描包括：针对所述文件相关信息的扫描，或者针对所述解析还原后的文件的文件内容进行扫描。

[0027] 在上述技术方案的基础上，进一步的，所述策略系统包括以下至少一种策略规则，并以所述策略规则对文件进行扫描：

[0028] (1)检索策略，所述检索策略包括一系列人员、设备或者目录的名单或者数据标识符，对满足所述名单或者所述数据标识符的所述文件的相关信息或者所述解析还原后的文件，进行扫描；

[0029] (2)白名单策略，所述白名单策略包括一系列人员、设备或者目录的名单或者数据标识符，对符合所述名单或者所述数据标识符的所述扫描的所述文件的相关信息或者所述解析还原后的文件，免于扫描。

[0030] 在上述技术方案的基础上，进一步的，所述策略系统中预设一些常用的敏感内容的数据标识符，所述数据标识符包括：身份证信息、营业执照信息、和/或银行卡号，并提供正向关键字、反向关键字、模糊关键字以及正则表达式规则，以便于配置策略规则。

[0031] 在上述技术方案的基础上，进一步的，所述全盘扫描系统接收到命中结果时，执行包括以下至少一种特殊操作：

[0032] (1)在终端上弹窗提醒；(2)发送提醒邮件。

[0033] 在上述技术方案的基础上，进一步的，检查所述USN的日志中是否有需要扫描的文件，包括：

[0034] 检查所述USN中的记录中对应的文件是否已经被正在进行的扫描过程扫描过，如果是，则所述记录对应的文件不需要扫描，如果否，则所述记录对应的文件需要扫描。

[0035] 当扫描后的文件发生新的文件操作时，如：添加、删除和修改等，均会在USN日志予以记录，如记录下修改时间和修改内容，此时，通过所述修改时间和修改内容能够判断出发生新的操作后的文件是否被扫描过，如果没有被扫描，则需要后续的增量扫描，以防止扫描后文件发生更新而缺乏再次扫描所带来的数据风险。

[0036] 在上述技术方案的基础上，进一步的，所述触发操作包括以下任一种：

[0037] (1)具有参数的触发操作，所述参数用于修改所述步骤2中所述前一次扫描操作的扫描日志；

[0038] (2)无参数触发操作，即不修改所述步骤2中所述前一次扫描操作的扫描日志；

[0039] 其中，所述修改所述步骤2中所述前一次扫描操作的扫描日志是指修改所述前一次扫描截止的位置。

[0040] 通过触发操作的两种形式，提高触发操作的灵活性。当触发操作具有参数时，所述参数是由管理员或者用户设置的文件索引，修改步骤2中所述前一次扫描操作的扫描日志，实现定制化的扫描，例如：当需要从文件系统的第一个或者某个指定位置的文件开始对其之后的文件逐一扫描时，通过设置所述参数指定这个文件的位置，实现定制化的文件扫描。

[0041] 另一方面，本公开还提供了一种应用USN实现全盘扫描的终端设备，其特征在于包括：处理器，存储器，所述处理器执行所述储存器上的程序实现上述应用USN实现全盘扫描功能的方法。

[0042] 与现有技术方案相比，本公开至少具有以下有益效果：

[0043] 以取得下述至少一种技术效果：

[0044] (1)由于本公开的技术方案由于利用了Windows操作系统的NTFS(New Technology File System，新技术文件系统)文件系统的USN(Update Service Number Journal or Change Journal，更新序列号)接口，快速的对待扫描盘里边的所有文件简历索引，并利用USN的特性，可以及时知道文件系统的变更，从而实现一个更加快捷的增量扫描的功能；

[0045] (2)本公开的技术方案由于提供了一个策略系统，系统管理员可以对管控的所有终端下发一组策略，且终端用户不可以停止该类策略，同时也提供了可供终端用户自定义的一些针对敏感信息的策略规则给扫描引擎，扫描引擎会根据策略生成一个用户文件系统的图谱，其对敏感文件进行归档，从而形成针对每一个用户文件系统的敏感信息图谱；

[0046] (3)本公开的技术方案由于还预设了一些常用的敏感内容的数据标识符，比如身份证信息，营业执照信息，银行卡号等，并提供了正向关键字、反向关键字、模糊关键字以及

正则表达式规则,方便管理员或用户配置敏感信息策略规则;

[0047] (4)本公开的技术方案不仅可以将扫描结果提示给用户,还可以对扫描出的敏感信息较多的用户,向系统管理员或者相关的管理人员发送提醒邮件,提高了安全性;

[0048] (5)本公开的技术方案能作为全盘扫描引擎,提供一些供其他应用使用的接口,比如终端DLP系统中的U盘管控功能,打印管控功能等,可以服务整个终端DLP的扫描需求。

附图说明

[0049] 图1是本公开所述的应用USN实现全盘扫描功能的方法的流程示意图。

[0050] 图2是本公开所述的应用USN实现全盘扫描功能的终端的概略性结构示意图。

[0051] 下面对本公开进一步详细说明。但下述的实例仅仅是为了便于理解本公开的技术方案,所列举的简易例子,并不代表或限制本公开的权利要求的保护范围,本公开的保护范围以权利要求书为准。

具体实施方式

[0052] 下面结合附图并通过具体实施方式来进一步说明本公开的技术方案。

[0053] 为更好地说明本公开,便于理解本公开的技术方案,本公开的典型但非限制性的实施例如下:这里需要特别说明的是本公开说明书所列的实施方式仅是为了说明问题方便而给出的示例性实施方法,其不得理解为是本公开唯一正确的实施方式,更不得理解为是对本公开保护范围的限制性说明。

[0054] 如图1所示,为本公开所述的应用USN实现全盘扫描功能的方法一个具体实施方式的流程示意图,其步骤如下:

[0055] 用于对终端的文件进行扫描,其特征在于所述终端部署有全盘扫描系统和策略系统,执行下述步骤:

[0056] S1:所述全盘扫描系统接收对所述文件系统进行扫描的触发操作;

[0057] S2:所述全盘扫描系统从日志系统中获取前一次扫描操作所对应的扫描日志;

[0058] S3:所述全盘扫描系统根据所述扫描日志查找到前一次扫描截止的位置,判断所述位置是否为所述文件系统的最后一个文件,如果为是,则转S4;如果为否,则执行S5,以所述位置的下一个文件的位置作为文件的扫描起点,然后转S7;

[0059] S4:检查所述USN的日志中是否有需要扫描的文件,如果否,表明所述文件系统的所有文件全部扫描完,转S1,等待新的扫描触发命令;如果是,则执行S6,以所述USN更新记录的文件位置为文件扫描起点,然后转S7;

[0060] S7:全盘扫描系统根据所述文件扫描起点取出一文件解析还原,所述文件的相关信息和解析还原后的文件发送给策略系统;

[0061] S8:所述策略系统对所述文件的相关信息和所述解析还原后的文件进行扫描,得到扫描结果,并更新所述扫描日志;

[0062] S9:所述扫描结果是否为命中,如果是,则执行S10,将命中结果发送给所述全盘扫描系统,然后转S2;如果否,则转步骤2。

[0063] 作为更优的实施例,所述策略系统可配置成对敏感信息的扫描策略,则能防护数据泄密(泄露)。

[0064] 本实施例能够避免更新文件“逃避”扫描的情况，例如：当扫描完一个文件后，所述文件又发生更新，此时，这个更新文件就不会被再次扫描，从而“逃避”了扫描操作，当更新的内容属于非法信息时，就会给系统带来安全隐患，而本实施例由于还需要检查USN日志中的信息，因此，即使被一个文件被扫描后在发生更新，但这个更新的信息会被记录在USN日志中，因此更新文件的原始文件即使被扫描后，但只要其发生了更新，也会被再次扫描，即实现增量扫描，有效避免上述安全隐患。

[0065] 作为更优的实施例，所述策略系统包括以下至少一种策略规则，并以所述策略规则对文件进行扫描：(1)检索策略规则，所述检索策略包括一系列人员、设备或者目录的名单，对满足所述名单的所述文件的相关信息或者所述解析还原后的文件，进行扫描；(2)白名单策略规则，所述白名单策略包括一系列人员、设备或者目录的名单，对符合所述名单的所述扫描的所述文件的相关信息或者所述解析还原后的文件，免于扫描。通过不同的策略规则实现不同的扫描方式，以满足不同用户的扫描应用需求。

[0066] 作为更优的实施例，所述策略系统中预设一些常用的敏感内容的数据标识符，所述数据标识符包括：身份证信息、营业执照信息、和/或银行卡号，并提供正向关键字、反向关键字、模糊关键字以及正则表达式规则，以便于配置策略规则。

[0067] 作为更优的实施例，所述检查所述USN的日志中是否有需要扫描的文件，包括：检查所述USN中的记录中对应的文件是否已经被正在进行的扫描过程扫描过，如果是，则所述记录对应的文件不需要扫描，如果否，则所述记录对应的文件需要扫描。

[0068] 当扫描后的文件发生新的文件操作时，如：添加、删除和修改等，均会在USN日志予以记录，如记录下修改时间和修改内容，此时，通过所述修改时间和修改内容能够判断出发生新的操作后的文件是否被扫描过，如果没有被扫描，则需要后续的增量扫描，以防止扫描后文件发生更新而缺乏再次扫描所带来的数据风险。

[0069] 作为更优的实施例，所述触发操作包括以下任一种：(1)具有参数的触发操作，所述参数用于修改所述步骤2中所述前一次扫描操作的扫描日志；(2)无参数触发操作，即不修改所述步骤2中所述前一次扫描操作的扫描日志；其中，所述修改所述步骤2中所述前一次扫描操作的扫描日志是指修改所述前一次扫描截止的位置。例如：全盘扫描完成后，扫描日志中记录的是文件系统的最后一个文件的位置，即表明全盘扫描已经完成，且没有发生过任何文件的新操作，即USN日志中也没有新的文件记录，此时，当用户希望再次做一次全盘扫描时，如果采用无参数触发操作时，所述全盘扫描操作并不能执行(全盘扫描系统会认为全盘扫描已经全部完成，直接返回到等待接收触发操作的状态中)；因此，需要采用具有参数的触发操作，重新指定扫描文件的起始位置，即通过设置的参数修改步骤2中前一次扫描操作的扫描日志，实现定制化的再次全盘扫描。

[0070] 本实施例通过触发操作的两种形式，提高触发操作的灵活性。当触发操作具有参数时，所述参数是由管理员或者用户设置的文件索引，修改步骤2中所述前一次扫描操作的扫描日志，实现定制化的扫描，例如：当需要从文件系统的第一个或者某个指定位置的文件开始对其之后的文件逐一扫描时，通过设置所述参数指定这个文件的位置，实现定制化的文件扫描。

[0071] 作为本公开的另一个方面，本公开还提供一种应用USN实现全盘扫描功能的终端。图2是图示根据本公开实施例的终端设备的硬件结构示意图。终端设备可以以各种形式来

实施，本公开中的终端设备可以包括但不限于诸如移动电话、智能电话、笔记本电脑、数字广播接收器、PDA(个人数字助理)、PAD(平板电脑)、PMP(便携式多媒体播放器)、导航装置、车载终端设备、车载显示终端、车载电子后视镜等的移动终端设备以及诸如数字TV、台式计算机等等的固定终端设备。如图2所示，终端设备1100可以包括处理器1120、输入单元1130、存储器1140、输出单元1150、等等。图2示出了具有各种组件的终端设备，但是应理解的是，并不要求实施所有示出的组件。可以替代地实施更多或更少的组件。

[0072] 其中，控制器1120用于执行本公开所公开的方法，输入单元1130可以根据用户输入的命令生成键输入数据以控制终端设备的各种操作，输出单元1150被提供输出信号。存储器1140可以存储由处理器1120执行的处理和控制操作的软件程序等等，或者可以暂时地存储已经输出或将要输出的数据。存储器1140可以包括至少一种类型的存储介质。而且，终端设备1100可以与通过网络连接执行存储器1140的存储功能的网络存储装置协作。处理器1120通常控制终端设备的总体操作。

[0073] 申请人声明，本公开通过上述实施例来说明本公开的详细结构特征，但本公开并不局限于上述详细结构特征，即不意味着本公开必须依赖上述详细结构特征才能实施。所属技术领域的技术人员应该明了，对本公开的任何改进，对本公开所选用部件的等效替换以及辅助部件的增加、具体方式的选择等，均落在本公开的保护范围和公开范围之内。

[0074] 以上详细描述了本公开的优选实施方式，但是，本公开并不限于上述实施方式中的具体细节，在本公开的技术构思范围内，可以对本公开的技术方案进行多种简单变型，这些简单变型均属于本公开的保护范围。

[0075] 另外需要说明的是，在上述具体实施方式中所描述的各个具体技术特征，在不矛盾的情况下，可以通过任何合适的方式进行组合，为了避免不必要的重复，本公开对各种可能的组合方式不再另行说明。

[0076] 此外，本公开的各种不同的实施方式之间也可以进行任意组合，只要其不违背本公开的思想，其同样应当视为本公开所公开的内容。

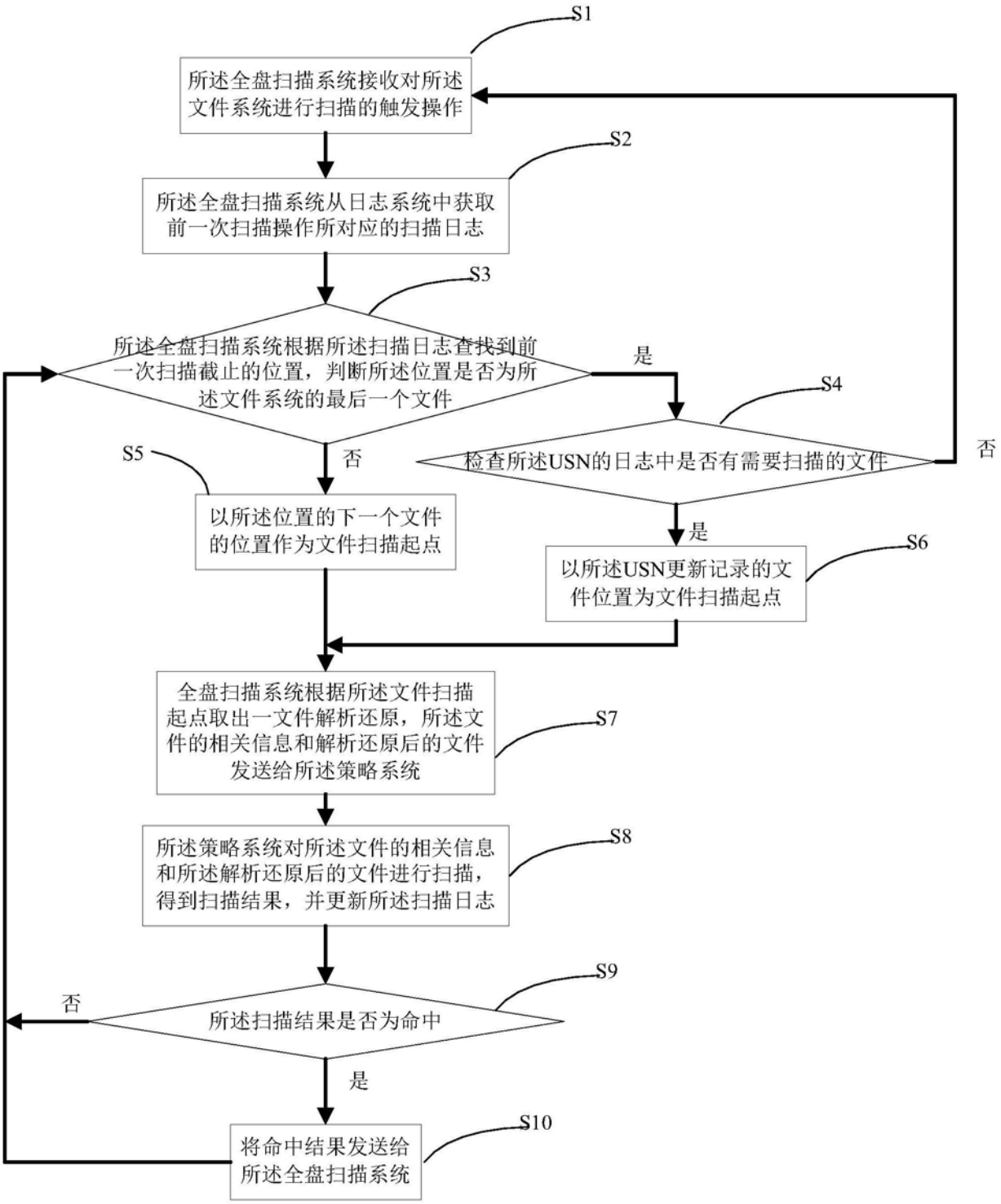

S1
所述全盘扫描系统接收对所述文件系统进行扫描的触发操作
S2
所述全盘扫描系统从日志系统中获取前一次扫描操作所对应的扫描日志
S3
所述全盘扫描系统根据所述扫描日志查找到前一次扫描截止的位置，判断所述位置是否为所述文件系统的最后一个文件
是
否
S4
检查所述USN的日志中是否有需要扫描的文件
否
是
S5
以所述位置的下一个文件的位置作为文件扫描起点
S6
以所述USN更新记录的文件位置为文件扫描起点
S7
全盘扫描系统根据所述文件扫描起点取出一文件解析还原，所述文件的相关信息和解析还原后的文件发送给所述策略系统
S8
所述策略系统对所述文件的相关信息和所述解析还原后的文件进行扫描，得到扫描结果，并更新所述扫描日志
S9
所述扫描结果是否为命中
否
是
S10
将命中结果发送给所述全盘扫描系统

图1

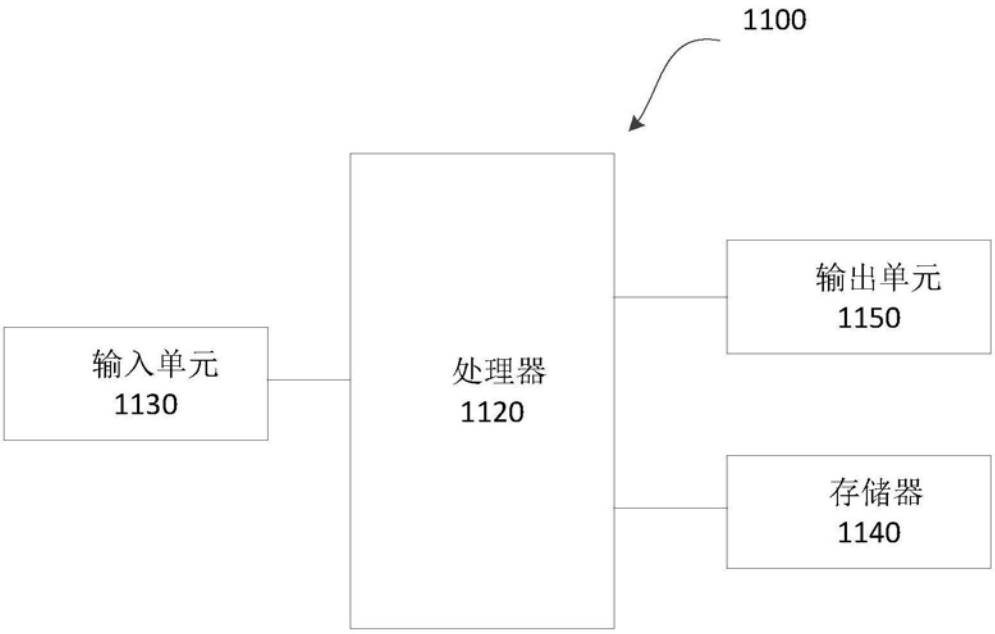


图2