(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 105653352 A
(43)申请公布日 2016.06.08

(21)申请号 201511027276.X

(22)申请日 2015.12.31

(71)申请人 公安部第三研究所
地址 200031 上海市徐汇区岳阳路76号

(72)发明人 吴松洋 张旭 刘欣 杨涛
刘善军 王旭鹏 杜琳 张勇

(74)专利代理机构 上海智信专利代理有限公司 31002
代理人 王洁 郑暄

(51)Int.Cl.
G06F 9/455(2006.01)

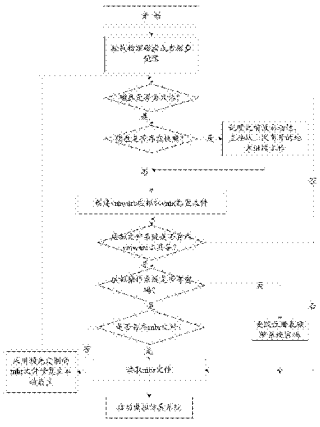
权利要求书2页 说明书5页 附图1页

(54)发明名称

操作系统虚拟仿真取证的方法

(57)摘要

本发明涉及一种操作系统虚拟仿真取证的方法，所述的方法包括以下步骤：将虚拟操作环境下虚拟机中待虚拟仿真取证的磁盘文件格式挂载到服务主机上；在虚拟机关机的状态下获取虚拟机的静态信息；待虚拟仿真取证的磁盘文件格式包括物理磁盘或磁盘镜像；物理磁盘为其支持以USB接口的形式加载物理磁盘；磁盘镜像是为支持以文件的形式加载磁盘镜像。采用该种结构的操作系统虚拟仿真取证的方法，使用物理磁盘或者磁盘镜像，通过在VMware以只读方式仿真启动操作系统，在仿真操作系统中可以查看物理磁盘或者磁盘镜像原始操作系统中的内容，以达到不用损坏物理磁盘或者磁盘镜像来取证的目的，操作简单，应用范围广泛。



CN 105653352 A

1.一种操作系统虚拟仿真取证的方法，其特征在于，所述的方法包括以下步骤：

(1)将虚拟操作环境下虚拟机中待虚拟仿真取证的磁盘文件格式挂载到服务主机上；

(2)在虚拟机关机的状态下获取虚拟机的静态信息。

2.根据权利要求1所述的操作系统虚拟仿真取证的方法，其特征在于，所述的步骤(1)具体包括以下步骤：

(1.1)挂载待虚拟仿真取证的物理磁盘或磁盘镜像；

(1.2)获取虚拟机的工作始点；

(1.3)创建虚拟机vmx配置文件。

3.根据权利要求2所述的操作系统虚拟仿真取证的方法，其特征在于，所述的步骤(1.1)具体为：

挂载待虚拟仿真取证的支持以USB接口加载的物理磁盘或挂载待虚拟仿真取证的支持以文件形式加载的磁盘镜像。

4.根据权利要求2所述的操作系统虚拟仿真取证的方法，其特征在于，所述的步骤(1.2)具体包括以下步骤：

(1.2.1)判断所述的物理磁盘或者所述的磁盘镜像是否为只读模式；

(1.2.2)如果所述的物理磁盘或者所述的磁盘镜像为只读模式，则判断所述的虚拟机是否存在快照；

(1.2.3)如果所述的虚拟机存在快照，则根据从上次离开的地方继续工作，然后继续步骤(1.3)；

(1.2.4)如果所述的虚拟机先前未被启动，则继续步骤(1.3)；

(1.2.5)如果所述的物理磁盘或者所述的磁盘镜像不为只读模式，则继续步骤(2)。

5.根据权利要求2所述的操作系统虚拟仿真取证的方法，其特征在于，所述的步骤(2)具体包括以下步骤：

(2.1)判断所述的虚拟机中是否存在mbr文件；

(2.2)如果所述的虚拟机中存在mbr文件，则读取所述的mbr文件后，启动虚拟机；

(2.3)如果所述的虚拟机中不存在mbr文件，则采用预先定制的mbr文件修复启动主扇区，然后继续步骤(1.2)。

6.根据权利要求5所述的操作系统虚拟仿真取证的方法，其特征在于，所述的步骤(2.1)具体包括以下步骤：

(2.1.1)判断所述的虚拟机中是否存在vmware工具集；

(2.1.2)如果所述的虚拟机中存在vmware工具集，则判断所述的虚拟机是否存在操作密码；

(2.1.3)如果所述的虚拟机存在操作密码，则所述的虚拟机中是否存在mbr文件；

(2.1.4)如果所述的虚拟机中存在mbr文件，则返回所述的虚拟机中存在mbr文件的结果；

(2.1.5)如果所述的虚拟机中不存在mbr文件，则返回所述的虚拟机中不存在mbr文件的结果；

(2.1.6)如果所述的虚拟机不存在操作密码，则更改注册表破解所述的虚拟机的密码，然后继续步骤(2.1.8)；

(2.1.7)如果所述的虚拟机中不存在vmware工具集,则继续步骤(2.1.8);

(2.1.8)读取所述的mbr文件后,启动虚拟机。

操作系统虚拟仿真取证的方法

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及电子数据取证，具体是指一种操作系统虚拟仿真取证的方法。

背景技术

[0002] 待取证操作系统中的各类数据是重要的证据来源，能较全面的对原始证据进行取证。计算机虚拟技术是通过软件来模拟计算机硬件的技术。目前，物理计算机的计算量、存储量有了非常大的进步。计算机上安装了虚拟机之后可以在一台机器上模拟出多台机器的效果，能完成架设多计算机服务程序、隐蔽网络访问等需求，因此，越来越多的数据以及服务被存储和移植到了虚拟计算机上。随之带来的针对虚拟机的数据恢复与取证需要在虚拟机上对物理磁盘或者磁盘镜像磁盘进行系统仿真取证。

发明内容

[0003] 本发明的目的是克服了上述现有技术的缺点，提供了一种解决虚拟操作环境下针对物理磁盘或者磁盘镜像的操作系统仿真问题、采用直接从某个磁盘分区或者整个磁盘来创建一个VMware的虚拟机的方法达到对物理磁盘或者磁盘镜像的仿真取证的操作系统虚拟仿真取证的方法。

[0004] 为了实现上述目的，本发明的操作系统虚拟仿真取证的方法具有如下构成：

[0005] 该操作系统虚拟仿真取证的方法，其主要特点是，所述的方法包括以下步骤：

[0006] (1)将虚拟操作环境下虚拟机中待虚拟仿真取证的磁盘文件格式挂载到服务主机上；

[0007] (2)在虚拟机关机的状态下获取虚拟机的静态信息。

[0008] 进一步地，所述的步骤(1)具体包括以下步骤：

[0009] (1.1)挂载待虚拟仿真取证的物理磁盘或磁盘镜像；

[0010] (1.2)获取虚拟机的工作始点；

[0011] (1.3)创建虚拟机vmx配置文件。

[0012] 更进一步地，所述的步骤(1.1)具体为：

[0013] 挂载待虚拟仿真取证的支持以USB接口加载的物理磁盘或挂载待虚拟仿真取证的支持以文件形式加载的磁盘镜像。

[0014] 更进一步地，所述的步骤(1.2)具体包括以下步骤：

[0015] (1.2.1)判断所述的物理磁盘或者所述的磁盘镜像是否为只读模式；

[0016] (1.2.2)如果所述的物理磁盘或者所述的磁盘镜像为只读模式，则判断所述的虚拟机是否存在快照；

[0017] (1.2.3)如果所述的虚拟机存在快照，则根据从上次离开的地方继续工作，然后继续步骤(1.3)；

[0018] (1.2.4)如果所述的虚拟机先前未被启动，则继续步骤(1.3)；

[0019] (1.2.5)如果所述的物理磁盘或者所述的磁盘镜像不为只读模式，则继续步骤(2)。

[0020] 更进一步地，所述的步骤(2)具体包括以下步骤：

[0021] (2.1)判断所述的虚拟机中是否存在mbr文件；

[0022] (2.2)如果所述的虚拟机中存在mbr文件，则读取所述的mbr文件后，启动虚拟机；

[0023] (2.3)如果所述的虚拟机中不存在mbr文件，则采用预先定制的mbr文件修复启动主扇区，然后继续步骤(1.2)。

[0024] 再进一步地，所述的步骤(2.1)具体包括以下步骤：

[0025] (2.1.1)判断所述的虚拟机中是否存在vmware工具集；

[0026] (2.1.2)如果所述的虚拟机中存在vmware工具集，则判断所述的虚拟机是否存在操作密码；

[0027] (2.1.3)如果所述的虚拟机存在操作密码，则所述的虚拟机中是否存在mbr文件；

[0028] (2.1.4)如果所述的虚拟机中存在mbr文件，则返回所述的虚拟机中存在mbr文件的结果；

[0029] (2.1.5)如果所述的虚拟机中不存在mbr文件，则返回所述的虚拟机中不存在mbr文件的结果；

[0030] (2.1.6)如果所述的虚拟机不存在操作密码，则更改注册表破解所述的虚拟机的密码，然后继续步骤(2.1.8)；

[0031] (2.1.7)如果所述的虚拟机中不存在vmware工具集，则继续步骤(2.1.8)；

[0032] (2.1.8)读取所述的mbr文件后，启动虚拟机。

[0033] 采用了该发明中的操作系统虚拟仿真取证的方法，使用物理磁盘或者磁盘镜像，通过在VMware以只读方式仿真启动操作系统，在仿真操作系统中可以查看物理磁盘或者磁盘镜像原始操作系统中的内容，以达到不用损坏物理磁盘或者磁盘镜像来取证的目的，操作简单，应用范围广泛。

附图说明

[0034] 图1为本发明的操作系统虚拟仿真取证的方法的步骤流程图。

具体实施方式

[0035] 为了能够更清楚地描述本发明的技术内容，下面结合具体实施例来进行进一步的描述。

[0036] 本发明详细分析了使用物理磁盘或者磁盘镜像，通过在VMware以只读方式仿真启动操作系统，在仿真操作系统中可以查看物理磁盘或者磁盘镜像原始操作系统中的内容，以达到不用损坏物理磁盘或者磁盘镜像来取证的目的。

[0037] 请参阅图1所示，图1为本发明的操作系统虚拟仿真取证的方法的步骤流程图。

[0038] 首先将虚拟操作环境下虚拟机中待系统虚拟仿真取证的磁盘文件格式挂载到服务主机上；在一种优选的实施方式中，待系统虚拟仿真取证的磁盘文件可以是物理磁盘或者磁盘镜像；其中，物理磁盘可以是各种类型的物理磁盘，包括SATA、IDE、SSD等各种常见物理硬盘，其支持以USB接口的形式加载物理磁盘；磁盘镜像则是支持常见的img、dd等磁盘镜

像格式，其支持以文件的形式加载磁盘镜像。物理磁盘或者磁盘镜像支持常见的Windows和Linux操作系统类型。

[0039] 然后，在虚拟机关机的状态下获取虚拟机的静态信息；在一种优选的实施方式中，所述的静态信息包含操作系统信息，虚拟机文件系统内容、文件格式、文件结构、分区信息、文件表、残存文件。能将文件系统以图形用户界面的方式展现给取证人员。支持特定目录下的特定文件的搜索，将搜索出来的文件进行加密，可采用MD5摘要算法或其它算法，加密后的文件不可再改动，具有不可抵赖性，最后以电子证据的形式保存到数据库中。

[0040] 在一种优选的实施方式中，选取VMware虚拟机为例，研究在虚拟操作环境中的勘查取证分析。VMware虚拟机的虚拟磁盘格式为VMDK文件，通过对VMDK文件格式的深入分析，将虚拟磁盘模拟为物理设备，实现了对虚拟磁盘的挂载，获取到虚拟磁盘的文件系统。

[0041] 首先，使用vmware-amount工具将物理磁盘或者磁盘镜像挂载到本机操作系统环境下，对于vmware-amount工具以及其他vmware系统的工具集，由于操作系统的不同会导致这些可运行程序所存储的位置不同，通过调用Windows操作系统WMI的方法获取到准确的vmware工具集可运行程序位置。

[0042] 将虚拟磁盘挂载的过程中会判断该虚拟机是否存在快照，如果存在则说明该虚拟机先前被启动过，否则未被启动过。如果这个磁盘镜像已经在之前被启动，可以采用从上次离开的地方继续工作，亦可从头开始工作。将整个物理磁盘或者磁盘镜像以文件的形式读入到内存中后，一般在磁盘文件的二进制字节的头部会发现物理磁盘或者磁盘镜像对应的mbr文件结构。

[0043] mbr指的是主启动扇区，如果物理磁盘或者磁盘镜像受到破损或者其他外部原因无法正常读取mbr文件，我们可采用预先定制的mbr文件结构来重构受损的物理磁盘或者磁盘镜像主启动扇区头，针对不同的操作系统预先定制有不同的主启动扇区头结构。

[0044] 由于vmware虚拟机的启动是从vmx启动生成的，根据物理磁盘或者磁盘镜像的mbr文件中的信息可以生成对应的虚拟机vmx文件。在每个虚拟机文件夹底下都能找到一个.vmx的文件。这个文件记录了该虚拟机的配置情况，可以用文本编辑器打开它，发现其实就是一个properties文件。我们针对要虚拟仿真的物理磁盘或者磁盘镜像，需要编写代码手动的生成一个vmx配置文件，添加以下新增配置内容能让虚拟仿真的物理磁盘或者磁盘镜像在虚拟机中正常的启动。

[0045] mainMem.useNamedFile＝"FALSE"，该配置可以禁止vmem交换文件的生成。如果将该配置参数设为true，虚拟机在启动时会生成与设定内存相同大小的内存交换文件。这就如同操作系统的虚拟内存一样，虚拟机自己管理虚拟机的分页文件，这个设定在需要取证的物理磁盘或者磁盘镜像是适用的，因为物理磁盘或者磁盘镜像上可能会运行不同的虚拟机镜像，各自要相对独立。但是如果只是在个人PC机上运行一个虚拟机测试环境，则该配置会既占硬盘空间又会遇到I/O瓶颈，所以建议关闭此选项，适用操作系统的分页交换机制。

[0046] MemTrimRate＝0，关闭该选项会禁止待仿真的物理磁盘或者磁盘镜像在虚拟机中启动时不会用到内存释放给主机，能使虚拟机的内存分配更快。

[0047] sched.mem.pshare.enable＝"FALSE"，关闭该选项会使得待仿真的物理磁盘或者磁盘镜像在虚拟机中启动时共享普通内存块。

[0048] 一个正常的vmx文件主要由Static Values、Drive Info和User Specified这三部

分组成。

[0049] 其中Static Values通常包含以下内容：

[0050] #Static Values

[0051] config.version

[0052] virtualHW.version

[0053] floppy0.present

[0054] displayName

[0055] Drive Info通常包含以下内容：

[0056] #Drive Info

[0057] ide0:0.present

[0058] ide0:0.fileName

[0059] ide0:0.deviceType＝disk

[0060] ide0:0.mode＝persistent

[0061] ide1:0.present＝TRUE

[0062] ide1:0.fileName＝auto detect

[0063] ide1:0.deviceType＝cdrom-raw

[0064] User Specified通常包含以下内容

[0065] #User Specified

[0066] memsize

[0067] rtc.starttime

[0068] tools.syncTime＝FALSE

[0069] time.syncronized.continue＝FALSE

[0070] time.syncronized.restore＝FALSE

[0071] time.syncronized.resume.disk＝FALSE

[0072] time.syncronized.resume.memory

[0073] time.syncronized.shrink＝FALSE

[0074] guestOS

[0075] snapshot.disabled

[0076] 在程序中可以针对这些不同的参数含义配置不同的参数值，以便在待仿真的物理磁盘或者磁盘镜像中设置相应的虚拟机参数。VMWare虚拟操作环境下的vmx文件生成后，下一步即可以生成可以由VMWare Workstation或者VMWare Player该类虚拟机工具启动运行的vmdk虚拟磁盘文件。vmdk虚拟磁盘文件通常由Disk Descriptor File和Disk Data Base两部分组成。

[0077] 其中Disk Descriptor File通常包含以下内容：

[0078] #Disk Descriptor File

[0079] version＝1

[0080] CID＝fffffffe

[0081] parentCID＝ffffffff

[0082] createType＝monolithicFlat

[0083] 如果当挂载的是物理磁盘时，createType的类型为fullDevice。

[0084] 其中Disk Data Base通常包含以下内容：

[0085] "#DDB-Disk Data Base

[0086] ddb.adapterType＝ide

[0087] ddb.geometry.sectors＝mbr.BootablePartition.EndSector

[0088] ddb.geometry.heads＝mbr.BootablePartition.EndHead

[0089] ddb.geometry.cylinders＝mbr.largestCylinderValOnDisk()

[0090] ddb.virtualHWVersion＝3

[0091] 根据挂载的虚拟磁盘的mbr文件生成了包含上述配置属性的虚拟机启动配置文件.vmx文件，在最后的生成阶段，可以选择只生成vmx文件，通过手动启动vmx文件来达到虚拟仿真物理磁盘或者磁盘镜像的功能。也可以直接调用操作系统注册表查询接口自动获取到VMware Workstation在系统中安装的位置、路径等其他配置，然后直接调用WMI接口启动已生成好的vmx虚拟机文件，以达到对物理磁盘或者磁盘镜像仿真取证的目的。

[0092] 最后根据输入的系统仿真参数，通常包括仿真操作系统类型、仿真系统启动时间、仿真系统内存大小和选择是从物理磁盘或者磁盘镜像中启动仿真系统等参数生成对应该的vmdk文件，根据原始物理磁盘或者磁盘镜像中的mbr文件中指定的二进制字段会生成对应的仿真操作系统注册表文件，根据对应的注册表文件和vmdk文件从VMWare Workstation中启动虚拟操作环境下的仿真系统，以达到对待取证物理磁盘或者磁盘镜像的系统仿真取证。

[0093] 采用了该发明中的操作系统虚拟仿真取证的方法，使用物理磁盘或者磁盘镜像，通过在VMware以只读方式仿真启动操作系统，在仿真操作系统中可以查看物理磁盘或者磁盘镜像原始操作系统中的内容，以达到不用损坏物理磁盘或者磁盘镜像来取证的目的，操作简单，应用范围广泛。

[0094] 在此说明书中，本发明已参照其特定的实施例作了描述。但是，很显然仍可以作出各种修改和变换而不背离本发明的精神和范围。因此，说明书和附图应被认为是说明性的而非限制性的。

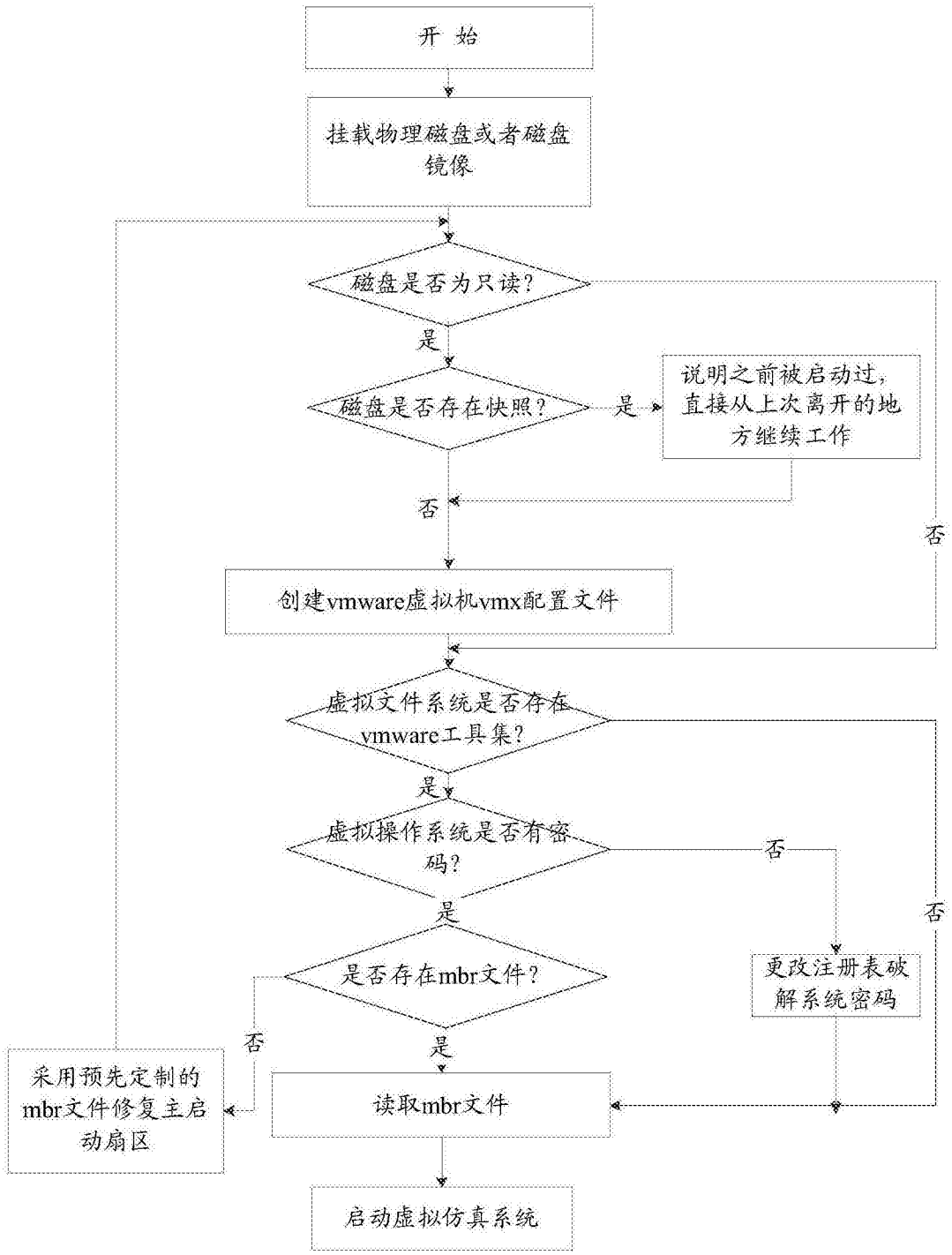

开 始
挂载物理磁盘或者磁盘镜像
磁盘是否为只读?
是
磁盘是否存在快照?
是
说明之前被启动过，直接从上次离开的地方继续工作
否
否
创建vmware虚拟机vmx配置文件
虚拟文件系统是否存在vmware工具集?
是
虚拟操作系统是否有密码?
否
是
是否存在mbr文件?
否
是
更改注册表破解系统密码
否
采用预先定制的mbr文件修复主启动扇区
读取mbr文件
启动虚拟仿真系统

图1