(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 102289485 A
(43)申请公布日 2011.12.21

(21)申请号 201110223064.4

(22)申请日 2011.08.04

(71)申请人 盘石软件(上海)有限公司
地址 200333 上海市普陀区中江路879号19号楼4楼

(72)发明人 陆道宏 汤伟

(74)专利代理机构 上海天翔知识产权代理有限公司 31224
代理人 梁晓霏

(51)Int.Cl.
G06F 17/30(2006.01)

权利要求书 1 页 说明书 5 页

(54)发明名称

一种针对计算机文件进行时间线分析的方法

(57)摘要

本发明公开了一种针对计算机文件和记录数据进行时间线分析的方法，针对系统中所有文件的创建时间、修改时间、最后访问时间，注册表键的创建时间，邮件的发送时间、服务器接收时间、保存到本地时间，上网日志的最后访问时间，系统和应用日志时间，即时通讯记录时间，文件下载项的创建时间、接收时间、完成时间进行排序，通过图表及摘要的方式进行显示。

CN 102289485 A

1. 一种针对计算机文件和记录数据进行时间线分析的方法，其特征在于，所述方法包括如下步骤：

1) 通过解析具体的文件系统得到相应的文件记录数据；

2) 确定每种记录类型所在文件的具体格式，解析出该记录，得到文件相关的时间信息；

3) 解析注册表记录，得到注册表项的时间信息；

4) 解析邮件数据，得到邮件的发送时间、服务器接收时间、保存到本地时间信息；

5) 解析上网日志记录，得到上网日志的访问时间信息；

6) 解析即时通讯日志记录，得到即时通讯记录的时间信息；

7) 解析操作系统和应用日志数据，得到日志的时间信息；

8) 解析各类下载软件的下载项记录，得到下载项创建时间、接收时间信息；

9) 将上述记录的指针，连同时间类型一起组成数据对，加入到一个列表中，按时间值进行排序；

10) 计算列表中数据对的数量，并将记录显示到界面中；

2. 如权利要求所述的一种针对计算机文件和记录数据进行时间线分析的方法，其特征在于，所述方法能指定时间段，对相应的时间段数据和记录进行过滤和显示。

3. 如权利要求所述的一种针对计算机文件和记录数据进行时间线分析的方法，其特征在于，对各种记录用不同的颜色进行分门别类的显示。

4. 如权利要求所述的一种针对计算机文件和记录数据进行时间线分析的方法，其特征在于，在解析一种新的记录或加载一个磁盘时，重新根据统一的数据对，进行时间排序。

5. 如权利要求所述的一种针对计算机文件和记录数据进行时间线分析的方法，其特征在于，所述方法能对数据对按照其数据特性进行过滤。

一种针对计算机文件进行时间线分析的方法

技术领域

[0001] 本发明涉及到计算机取证领域，特别涉及到一种针对文件时间、数据记录时间进行分析的方法。

背景技术

[0002] 计算机取证(Computer Forensics、计算机取证技术、计算机鉴识、计算机法医学)是指运用计算机辨析技术，对计算机犯罪行为进行分析以确认罪犯及计算机证据，并据此提起诉讼。也就是针对计算机入侵与犯罪，进行证据获取、保存、分析和出示。计算机证据指在计算机系统运行过程中产生的以其记录的内容来证明案件事实的电磁记录物。从技术上而言，计算机取证是一个对案件相关的计算机系统进行扫描和分析，以对计算机中现场数据进行重建的过程。可理解为“从计算机上提取证据”即：获取、保存、分析、出示、提供的证据必须可信。计算机取证(Computer Forensics)在打击计算机和网络犯罪中作用十分关键，它的目的是要将犯罪者留在计算机中的“痕迹”作为有效的诉讼证据提供给法庭，以便将犯罪嫌疑人绳之以法。因此，计算机取证是计算机领域和法学领域的一门交叉科学，被用来解决大量的计算机犯罪和事故，包括网络入侵、盗用知识产权和网络欺骗等。

[0003] 文件中的属性保存有创建时间、修改时间，最后访问时间，注册表中的键保存有创建时间、即时通信保存有聊天记录时间等。在某段时间内，可能会发生一个文件的创建、两个人的聊天内容，一个新的键产生，这些变化很可能互有关联性，但目前市场上并没有相关软件能描述这些变化，以及针对这些变化带来的影响。

[0004] 综上所述，针对现有技术的缺陷，特别需要一种针对计算机中文件和数据记录进行时间线分析的方法，以解决现有技术的不足。

发明内容

[0005] 本发明的目的是提供一种针对计算机中文件和数据记录进行时间线分析的方法，针对系统中所有文件的创建时间、修正时间、最后访问时间，注册表键的创建时间，邮件的发送时间、服务器接收时间、保存到本地时间，上网日志的最后访问时间，操作系统和应用日志时间，即时通讯记录时间，文件下载项的创建时间、接收时间、完成时间进行排序，通过图表及摘要的方式进行显示，从而实现本发明的目的。

[0006] 本发明所解决的技术问题可以采用以下技术方案来实现：

[0007] 一种针对计算机中文件和数据记录进行时间线分析的方法，其特征在于，所述方法包括如下步骤：

[0008] 1) 通过解析具体的文件系统得到相应的文件记录数据；

[0009] 2) 确定每种记录类型所在文件的具体格式，解析出该记录，得到文件相关的时间信息；

[0010] 3) 解析注册表记录，得到注册表项的时间信息；

[0011] 4) 解析邮件数据，得到邮件的发送时间、服务器接收时间、保存到本地时间信息；

[0012] 5) 解析上网日志记录，得到上网日志的访问时间信息；

[0013] 6) 解析即时通讯日志记录，得到即时通讯记录的时间信息；

[0014] 7) 解析操作系统和应用日志数据，得到日志的时间信息；

[0015] 8) 解析各类下载软件的下载项记录，得到下载项创建时间、接收时间信息；

[0016] 9) 将上述记录的指针，连同时间类型一起组成数据对，加入到一个列表中，按时间值进行排序；

[0017] 10) 计算列表中数据对的数量，并将记录显示到界面中；

[0018] 在本发明的一个实施例中，所述方法能指定时间段，对相应的时间段数据和记录进行显示。

[0019] 在本发明的一个实施例中，对各种记录用不同的颜色进行分门别类的显示。

[0020] 在本发明的一个实施例中，在解析一种新的记录或加载一个磁盘时，重新根据统一的数据对，进行时间排序。

[0021] 在本发明的一个实施例中，可以对数据对按照其数据特性进行过滤。

具体实施方式

[0022] 为了使本发明实现的技术手段、创作特征、达成目的与功效易于明白了解，下面结合具体图示，进一步阐述本发明。

[0023] 本发明主要针对在给定的某段时间内，针对系统中所有文件的创建时间、修正时间、最后访问时间，注册表键的创建时间，邮件的发送时间、服务器接收时间、保存到本地时间，上网日志的最后访问时间，操作系统和应用日志时间，即时通讯记录时间，文件下载项的创建时间、接收时间、完成时间进行排序，通过图表及摘要的方式进行显示。

[0024] 针对七种类型的记录（包括文件 / 文件夹、上网日志、邮件记录、即时通讯、注册表、系统日志、下载记录），设置相应的时间类型枚举变量如下：

[0025]

```
enum TimeType
{
  FILE_CREATE     =     0x00000001,
  FILE_MODIFY     =     0x00000002,
  FILE_ACCESS     =     0x00000004,
  REGISTRY_TIME   =     0x00000008,
  EVENTLOG_TM     =     0x00000010,
  MAIL_SENT       =     0x00000020,
  MAIL_RECEIVE    =     0x00000040,
  MAIL_SAVE       =     0x00000080,
  IM_TIME         =     0x00000100,
  DOWN_CREATE     =     0x00000200,
  DOWN_RECEIVE    =     0x00000400,
  DOWN_FINISH     =     0x00000800,
  WEB_FIRST       =     0x00001000,
```

[0026]

```
  WEB_SECOND      =     0x00002000
};
```

[0027] 这些时间类型便于对列表进行过滤，元素时间与时间类型的获取。

[0028] 所有记录本身与其时间组成的数据对存放于列表中。

[0029] 对于多次加载磁盘与多次做应用分析的情形，给出了相应的对策：由于多次操作，可能造成列表中的元素有重复的现象，为此利用 std::set 剔除相同的元素，再将其置入列表中。

[0030] 对于文件/目录类型的记录，从所给的根结点处往下遍历，将所有的结点（包括文件夹）与其对应的时间类型置入列表中。

[0031] 对于应用分析类型的记录，也是从所给根结点处往下遍历，插入的结点应满足如下条件：

[0032]

记录类型	节点条件
即时通讯：	非 folder
下载：	非 folder

操作系统和应用日志	非 folder
上网日志：	非 folder
邮件记录：	非 folder
注册表	所有结点

[0033] 具体对每一结点的插入操作又有以下分类：

[0034]

记录类型	插入操作
文件/目录	每一结点对应的时间有三种:创建时间(C)、修改时间(M)、访问时间(A).若这三种时间中有相同的则进行全并,最后组成的集合{(时间类型,条目)}置入列表中
即时通讯	只插入消息结点
下载	每一结点对应的时间有三种:创建时间(C)、接收时间(R)、完成时间(F).若这三种时间中有相同的则进行全并,最后组成的集合{(时间类型,条目)}置入列表中
系统日志	对每一节点都进行插入.
上网日志	每一结点对应的时间有三种:第一时间(F)、第二时间(S).若这两种时间中有相同的则进行全并,最后组成的集合{(时间类型,条目)}置入列表中
邮件记录	每一结点对应的时间有三种:发送时间(S)、接收时间(R)、保存时间(SA).若这三种时间中有相同的则进行全并,最后组成的集合{(时间类型,条目)}置入列表中
注册表	对每一节点都进行插入.

[0035]

[0036] 按时间过滤:过滤出最小时间 (minT) 与最大时间 (maxT) 间的所有记录。返回处于列表中的开始迭代器与结束迭代器。

[0037] 按类型过滤:从给定的开始、结束迭代器中获取给定时间类型的记录。

[0038] 本发明的有益效果在于：

[0039] 1) 通过调整时间控件或调整左侧进度条的长度,可实现过滤出任意时间段内记

录；

[0040] 2) 通过选择相应类型记录及其时间类型，可以控制所需要的记录；

[0041] 3) 通过过滤器，可过滤出名称、摘要、是否删除等信息；

[0042] 4) 可以查看每种类型的具体数目；

[0043] 5) 可设置每种类型的颜色；

[0044] 6) 每设置一定时间内显示的粒度；

[0045] 7) 可跳转到系统安装时间及最后一次关机时间；

[0046] 8) 可针对有用的信息进行打勾选择；

[0047] 9) 可导出有意义的列表；

[0048] 10) 可跳转到源记录，以便查看更为详细的信息；

[0049] 这里以如何分析注册表时间为例，来说明时间线分析的方法：

[0050] 1、通过研究注册表，确认注册表有几个主要的文件，其中 Windows/System32/Config 下的 system 表示 HKEY_LOCAL_MACHINE 下的 SYTEM 键，software 表示 HKEY_LOCAL_MACHINE 下的 SOFTWARE 键，等等。

[0051] 2、解析注册表文件的格式，得到相应的注册表键值的树状表示；

[0052] 3、通过研究其格式，确认只有注册表键有创建时间，注册表值是没有时间项的，故只能是注册表键参与时间线分析；

[0053] 4、将每一个注册表键的指针同其相关的枚举值 (REGISTRY_TIME) 组建成一个数据对；

[0054] 5、将所有的数据对，全部导入到一个全局的列表中，其中可以保存各种类型的记录及相关的时间类型；

[0055] 6、针对这个列表进行排序，排序比较的准则是，依据相关的时间，这里是注册表键，则取其键的创建时间；

[0056] 7、计算列表中元素（即数据对）的数量，将记录显示到界面中；

[0057] 以上显示和描述了本发明的基本原理和主要特征和本发明的优点。本行业的技术人员应该了解，本发明不受上述实施例的限制，上述实施例和说明书中描述的只是说明本发明的原理，在不脱离本发明精神和范围的前提下，本发明还会有各种变化和改进，这些变化和改进都在要求保护的本发明范围内，本发明要求保护范围由所附的权利要求书及其等效物界定。