(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2014 年 7 月 10 日 (10.07.2014)

WIPO | PCT

(10) 国际公布号
WO 2014/106489 A1

(51) 国际专利分类号:
H04L 29/14 (2006.01)

(21) 国际申请号: PCT/CN2014/070185

(22) 国际申请日: 2014 年 1 月 6 日 (06.01.2014)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201310004497X 2013 年 1 月 7 日 (07.01.2013) CN

(71) 申请人: **北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED)** [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室（德胜园区）, Beijing 100088 (CN)。 **奇智软件（北京）有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED)** [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。

(72) 发明人: **范家鹏 (FAN, Jiapeng)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **张鹏翼 (ZHANG, Pengyi)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。 **任寰 (REN, Huan)**; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

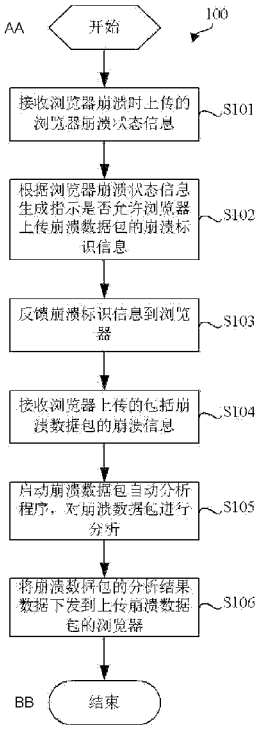
(74) 代理人: **北京智汇东方知识产权代理事务所（普通合伙） (WISEAST INTELLECTUAL PROPERTY LAW FIRM)**; 中国北京市海淀区成府路 28 号优盛大厦 D-1111 室, Beijing 100083 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM,

[见续页]

(54) **Title**: METHOD AND SYSTEM FOR PROCESSING BROWSER CRASH INFORMATION

(54) **发明名称** : 浏览器崩溃信息的处理方法及系统



S101 Receiving browser crash state information uploaded when a browser crashes
S102 According to the browser crash state information, generating crash identification information for indicating whether to allow a browser to upload a crash data packet
S103 Feeding back the crash identification information to the browser
S104 Receiving crash information including the crash data packet uploaded by the browser
S105 Starting an automatic analysis program of the crash data packet so as to analyze the crash data packet
S106 Issuing analysis result data of the crash data packet to the browser uploading the crash data packet
AA Start
BB End

图 1/Fig.1

(57) **Abstract**: Disclosed are a method and system for processing browser crash information. The method comprises: receiving browser crash state information uploaded when a browser crashes; according to the browser crash state information, generating crash identification information for indicating whether to allow a browser to upload a crash data packet; feeding back the crash identification information to the browser; in the case that the crash identification information indicates allowing the browser to upload the crash data packet, receiving crash information including the crash data packet uploaded by the browser; starting an automatic analysis program of the crash data packet so as to analyze the crash data packet; and issuing analysis result data of the crash data packet to the browser uploading the crash data packet. Provided is a cloud system level solution, which is capable of collecting, processing, analyzing and authenticating crash information of a browser in a targeted way.

(57) **摘要**: 本发明公开了一种浏览器崩溃信息的处理方法及系统。其中方法包括：接收浏览器崩溃时上传的浏览器崩溃状态信息；根据所述浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息；反馈所述崩溃标识信息到所述浏览器；在所述崩溃标识信息表明允许浏览器上传崩溃数据包的情况下，接收所述浏览器上传的包括崩溃数据包的崩溃信息；启动崩溃数据包自动分析程序，对所述崩溃数据包进行分析；将所述崩溃数据包的分析结果数据下发到所述上传崩溃数据包的浏览器。本发明提供了一种云系统级的方案，能够有针对性地对浏览器的崩溃信息进行收集、处理、分析以及鉴定。

WO 2014/106489 A1

ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国** (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

浏览器崩溃信息的处理方法及系统

技术领域

本发明涉及计算机网络技术领域，具体涉及一种浏览器崩溃信息的处理方法及系统。

背景技术

云计算（cloud computing）是分布式计算技术的一种，其最基本的概念是通过网络将庞大的计算处理程序自动拆分成无数个较小的子程序，再交由多部服务器所组成的庞大系统经搜寻、计算分析之后将处理结果回传给用户。通过该技术，网络服务提供者可以在数秒之内达成处理数以千万计甚至数以亿计的信息的目的，从而达成和“超级计算机”同样强大效能的网络服务。

在浏览器进行网页加载的过程中，常常由于种种原因使得浏览器反应变得很慢，或者造成浏览器失去响应，甚至会导致机器无法进行其他的操作。这种现象被称之为浏览器崩溃。导致浏览器崩溃的原因主要包括：内存泄露、网页代码复杂和浏览器的故障（Bug）、网页数据过多、网络服务漏洞等。

在 windows 系统中，一般通过 windows 错误报告来上传操作系统出现的各类问题。由于 windows 系统中 IE 浏览器是与操作系统绑定的，所以当 IE 出现崩溃时，操作系统会收集浏览器的状态信息，并将信息封装到一个错误报告中回传给服务器端。而对于浏览器端产生崩溃后，现有技术没有提供一种云系统级的方案，能够有针对性地对浏览器的崩溃信息进行收集、保存、分析以及鉴定。

发明内容

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浏览器崩溃信息的处理系统和相应的浏览器崩溃信息的处理方法。

根据本发明的一个方面，提供了一种浏览器崩溃信息的处理方法，包括：接收浏览器崩溃时上传的浏览器崩溃状态信息；根据所述浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息；反馈所述崩溃标识信息到所述浏览器；在所述崩溃标识信息表明允许浏览器上传崩溃数据包的情况下，接收所述浏览器上传的包括崩溃数据包的崩溃信息；启动崩溃数据包自动分析程序，对所述崩溃数据包进行分析；将所述崩溃数据包的分析结果数据下发到所述上传崩溃数据包的浏览器。

根据本发明的另一方面，提供了一种浏览器崩溃信息的处理系统，包括：第一接口，用于接收浏览器崩溃时上传的浏览器崩溃状态信息；第一云崩溃服务器，用于根据所述浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息，通过所述第一接口反馈所述崩溃标识信息到所述浏览器；第二接口，用于在所述崩溃标识信息表明允许浏览器上传崩溃数据包的情况下，接收所述浏览器上传的包括崩溃数据包的崩

溃信息；分析设备，用于启动崩溃数据包自动分析程序，对所述崩溃数据包进行分析；下发设备，用于通过所述第二接口将所述崩溃数据包的分析结果数据下发到所述上传崩溃数据包的浏览器。

根据本发明提供的方案，在接收到浏览器崩溃时上传的浏览器崩溃状态信息之后，根据该浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息，并反馈给浏览器，以供浏览器根据崩溃标识信息确定是否得到上传崩溃数据包的允许。在得到允许的情况下，浏览器上传崩溃数据包，云端启动自动分析程序对崩溃数据包进行分析，并将分析结果数据下发给浏览器。本发明提供了一种云系统级的方案，能够有针对性地对浏览器的崩溃信息进行收集、处理、分析以及鉴定。

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

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：

图 1 示出了根据本发明一个实施例的浏览器崩溃信息的处理方法的流程图；

图 2 示出了根据本发明另一个实施例的浏览器崩溃信息的处理方法的流程图；

图 3 示出了根据本发明一个实施例的浏览器崩溃信息的处理系统的结构框图；

图 4 示出了根据本发明一个实施例的执行本发明所述方法的服务器的框图；以及

图 5 示出了根据本发明一个实施例的用于保持或者携带实现本发明所述方法的程序代码的存储单元。

具体实施方式

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。

图 1 示出了根据本发明一个实施例的浏览器崩溃信息的处理方法 100 的流程图。如图 1 所示，方法 100 始于步骤 S101，其中接收浏览器崩溃时上传的浏览器崩溃状态信息。在浏览器产生崩溃时，首先向云端上传浏览器崩溃状态信息。可选地，浏览器使用云端提供的 Get 接口向其上传浏览器崩溃状态信息。浏览器崩溃状态信息是浏览器反馈的有关崩溃状态的信息，其至少包括浏览器崩溃公共参数信息（pubkey），可选地还可包括命令行、浏览器产品名称以及第一浏览器侧数据校验信息，其中第一浏览器侧数据校验信息是浏览器根据浏览器崩溃公共参数信息和预设密钥生成的。浏览器崩溃公共参数信

息至少包括如下信息：崩溃模块的相关信息、具体崩溃偏移、崩溃堆栈、浏览器版本号以及操作系统版本号。

随后，方法 100 进入步骤 S102，其中根据浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息（dumpid）。云端主要是根据上述浏览器崩溃公共参数信息生成崩溃标识信息。具体来说，云端从浏览器崩溃状态信息中提取出崩溃模块的相关信息、具体崩溃偏移、崩溃堆栈、浏览器版本号、操作系统版本号等浏览器崩溃公共参数信息，按照预设算法对这些信息进行处理，生成崩溃键值（dumpkey），例如：按照 MD5 算法对上述信息进行处理生成 dumpkey。云端累计对相同的浏览器崩溃状态信息的接收次数，具体做法就是累计相同 dumpkey 的数目，如果相同 dumpkey 的数目大于或等于预设阈值（比如 3），表明云端对相同的浏览器崩溃状态信息的接收次数已大于或等于 3 次，则生成的 dumpid 为 0，即不允许浏览器上传崩溃数据包；如果相同 dumpkey 的数目小于 3，则生成的 dumpid 大于 0，即允许浏览器上传崩溃数据包。

随后，方法 100 进入步骤 S103，其中反馈崩溃标识信息到浏览器。云端将崩溃标识信息反馈给浏览器，可选地云端反馈给浏览器的信息为 JSON 格式的信息。浏览器接收到崩溃标识信息后，如果获知不允许上传崩溃数据包，那么此次交手结束。如果获知允许上传崩溃数据包，则进入步骤 S104。

在步骤 S104 中，接收浏览器上传的包括崩溃数据包的崩溃信息。在崩溃标识信息表明允许浏览器上传崩溃数据包的情况下，云端接收浏览器上传的崩溃数据包。可选地，云端使用 Post 接口接收浏览器上传的崩溃数据包。

在步骤 S104 之后，方法 100 进入步骤 S105，其中启动崩溃数据包自动分析程序，对崩溃数据包进行分析。云端可以通过部署的自动崩溃数据包分析程序，随时监控浏览器上传的崩溃数据包，一旦发现有新的崩溃数据包，立即进行分析，并及时返回分析结果数据，这样达到了实时分析的目的。云端也可以调用自动化分析接口对浏览器上传的崩溃数据包进行分析。

随后，方法 100 进入步骤 S106，将崩溃数据包的分析结果数据下发到上传崩溃数据包的浏览器。云端根据崩溃数据包的分析结果数据所对应的浏览器的 MID 或 QID 将崩溃数据包的分析结果数据下发到对应的浏览器。

图 2 示出了根据本发明另一个实施例的浏览器崩溃信息的处理方法 200 的流程图。如图 2 所示，方法 200 始于步骤 S201，其中使用 Get 接口接收浏览器崩溃时上传的浏览器崩溃状态信息。本方法中，在浏览器产生崩溃时，浏览器使用云端提供的 Get 接口向其上传浏览器崩溃状态信息。表 1 示出了浏览器崩溃状态信息所包含的具体内容。其中，浏览器崩溃公共参数信息（pubkey）、浏览器产品名称（src）和第一浏览器侧数据校验信息（cverify1）是必选内容，命令行（cmd）和自定义信息（custom）是可选内容，这些信息的类型均为 string 类型。

表 1. 浏览器崩溃状态信息的示意表

参数	必选	类型及范围	说明
pubkey	true	string	浏览器公共参数部分，取值参见表 2
custom	false	string	自定义信息，多个值以下划线“_”分隔
cmd	false	string	命令行参数，多个值以下划线“_”分隔
src	true	string	浏览器产品名称
cverify1	true	string	第一浏览器侧数据校验信息，用此字段来检验是否为合法数据

进一步的，表 2 示出了 pubkey 的具体内容。pubkey 除了包括崩溃模块的相关信息、具体崩溃偏移、崩溃堆栈、浏览器版本号以及操作系统版本号等信息以外，还包括很多其它信息。

表 2. 浏览器崩溃公共参数信息的示意表

参数	说明
process_type	进程类型
thread_type	线程类型
process_stage	进程阶段
thread_stage	线程阶段
crash	崩溃还是异常
version	主程序版本号
crash_type	崩溃类型
first_crash_name	第一层崩溃模块名称：包含 unknown
first_crash_version	第一层崩溃模块版本号
first_crash_offset	第一层崩溃偏移
more_crash_name	具体崩溃模块名称：去掉 unknown
more_crash_version	具体崩溃模块版本号
more_crash_offset	具体崩溃偏移
my_crash_name	最近的自己崩溃模块名称
my_crash_version	最近的自己崩溃模块版本号
my_crash_offset	最近的自己崩溃偏移
mid	mid
pid	pid
stack_md5	崩溃堆栈 md5 =MD5（崩溃模块名称 + 顶层崩溃模块偏移）

system_version	操作系统版本号
ie_version	ie 版本号
flash_version	flash 版本号
catch_num	异常次数
m	M 值
ie8_kernel	是否是 IE8 内核
open_death	是否打开防假死
process_model	进程模型

随后，方法 200 进入步骤 S202，其中通过效验浏览器产品名称（src）来对浏览器产品的合法性进行校验。在接收到浏览器上传的浏览器崩溃状态信息之后，提取其中的 src，根据 src 可判断出浏览器产品是否合法，如合法，则进入步骤 S203；如不合法，本方法结束。

在步骤 S203 中，通过验证第一浏览器侧数据校验信息（cverify1）是否正确来对崩溃状态信息的合法性和完整性进行校验。其中 cverify1 是浏览器根据 pubkey 和预设密钥生成的，例如：cverify1=MD5(pubkey+密钥)，即对 pubkey 和预设密钥进行 MD5 算法加密得到 cverify1。在接收到浏览器上传的浏览器崩溃状态信息之后，提取其中的 cverify1，判断 cverify1 是否正确，如正确，表明崩溃状态信息是合法且完整的，则进入步骤 S204；否则，本方法结束。

在步骤 S204 中，对预先定义的时间段内从相同地址的浏览器再次接收的浏览器崩溃状态信息进行丢弃处理。为了防止浏览器在短时间内（比如 2s）连续提交相同的信息，通过进行缓存进行提交限制，在短时间内连续提交的信息视为一次提交，判断规则可基于 cverify1。

随后，方法 200 进入步骤 S205，其中根据浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息（dumpid）。具体来说，云端从 pubkey 中提取出崩溃模块的相关信息、具体崩溃偏移、崩溃堆栈、浏览器版本号、操作系统版本号等信息，根据这些信息生成崩溃键值（dumpkey），例如：dumpkey=MD5(崩溃模块+具体崩溃偏移+崩溃堆栈 md5+IE 版本号+操作系统版本号)，即对这些信息进行 MD5 算法加密得到 dumpkey。云端累计对相同的浏览器崩溃状态信息的接收次数，具体做法就是累计相同 dumpkey 的数目，如果相同 dumpkey 的数目大于或等于预设阈值（比如 3），表明云端对相同的浏览器崩溃状态信息的接收次数已大于或等于 3 次，则生成的 dumpid 为 0，即不允许浏览器上传崩溃数据包；如果相同 dumpkey 的数目小于 3，则生成的 dumpid 大于 0，如 dumpid=dump_id，dump_id 为大于 0 的值，即允许浏览器上传崩溃数据包。

随后，方法 200 进入步骤 S206，其中反馈崩溃标识信息到浏览器。进一步的，在反馈崩溃标识信息的同时，还需反馈第一服务器侧数据校验信息（sverify1），以供浏览器对崩溃标识信息的合法性和完整性进行校验。该第一服务器侧数据校验信息是云端根据

dumpid 和预设密钥生成的，例如：sverify1=MD5(dumpid+密钥)，即对 dumpid 和预设密钥进行 MD5 算法加密得到 sverify1。云端将崩溃标识信息和第一服务器侧数据校验信息封装为回传信息，反馈给浏览器。该回传信息可为 JSON 格式。例如，云端反馈给浏览器的回传信息如下：

{"dumpid":"0", "sverify1:"sverify1_val"}

或{"dumpid":"dump_id", "sverify1:"sverify1_val"}

其中 sverify1_val 为 sverify1 的具体取值。

浏览器接收到上述回传信息后，提取 dumpid，如果 dumpid 为 0，表明云端不允许浏览器上传崩溃数据包，那么此次交手结束。如果 dumpid 为 dump_id，表明云端允许浏览器上传崩溃数据包，则进入步骤 S207。

在步骤 S207 中，使用 Post 接口接收浏览器上传的包括崩溃数据包的崩溃信息。在崩溃标识信息表明允许浏览器上传崩溃数据包的情况下，云端接收浏览器上传的包括崩溃数据包的崩溃信息。表 3 示出了崩溃信息所包含的具体内容，具体为浏览器产品名称（src），崩溃标识信息（dumpid），崩溃数据包（file）和第二浏览器侧数据校验信息（cverify2）。

表 3. 崩溃信息

参数	必选	类型及范围	说明
src	true	string	浏览器产品名称
dumpid	true	string	云端返回的 dump_id
file	true	string	dump 文件流
cverify2	true	string	第二浏览器侧数据校验信息，用此字段来检验是否为合法数据

随后，方法 200 进入步骤 S208，其中通过效验浏览器产品名称（src）来对浏览器产品的合法性进行校验。在接收到浏览器上传的崩溃信息之后，提取其中的 src，根据 src 可判断出浏览器产品是否合法，如合法，则进入步骤 S209；如不合法，本方法结束。

在步骤 S209 中，通过验证第二浏览器侧数据校验信息（cverify2）是否正确来对崩溃信息的合法性和完整性进行校验。其中 cverify2 是浏览器根据崩溃数据包、崩溃标识信息和预设密钥生成的，例如：cverify2=MD5(file 内容+dump_id+密钥)，即对 file 内容、dump_id 和预设密钥进行 MD5 算法加密得到 cverify2。在接收到浏览器上传的崩溃信息之后，提取其中的 cverify2，判断 cverify2 是否正确，如正确，表明崩溃信息是合法且完整的，则进入步骤 S210；否则，本方法结束。

在步骤 S210 中，将崩溃数据包存入队列中。云端接收的崩溃数据包来自很多客户端的浏览器。一方面，云端的云崩溃服务器将上传的崩溃数据包保存为临时文件，移动到临时目录；另一方面，云崩溃服务器将通过 Post 接口上传的崩溃数据包存入到队列中（每一台服务器都可以有一个队列），然后，给浏览器返回信息，通知浏览器上传数据是否

成功。云端给浏览器返回的信息如下：

{"status":"0", "sverify2:"sverify2_val"}

或{"status":"1", "sverify2:"sverify2_val"}

其中 status 为 0 表示浏览器上传数据失败，status 为 1 表示浏览器上传数据成功。sverify2 为第二服务器侧数据校验信息，它是根据 status，dump_id 和预设密钥生成的，例如：sverify2=MD5(status+dump_id+密钥)，即对 status，dump_id 和预设密钥进行 MD5 算法加密得到 sverify2。sverify2_val 为 sverify2 的取值。

云崩溃服务器可以将崩溃数据包存储到持久化存储器中，如 Cassandra 数据库。

随后，方法 200 进入步骤 S211，其中读取队列，将来自不同浏览器产品的崩溃数据包分送给不同的分析设备。云崩溃服务器读取队列，将来自不同浏览器产品的崩溃数据包同步到多台 Windows 环境下的 Windows 机器目录下。以云崩溃服务器为 Linux 操作系统为例，Linux 系统向 Windows 同步文件可以采用基于 C/S 模式软件的 rsync 实现，rsync 是数据镜像备份工具，可以镜像保存整个目录树和文件系统。在同步到 Windows 机器目录下后，在临时目录下的已被同步的崩溃数据包被删除。

随后，方法 200 进入步骤 S212，其中不同的分析设备启动各自的崩溃数据包自动分析程序，对崩溃数据包进行分析。该分析步骤可以采取以下两种方式：一种是 Windows 机器上部署了自动崩溃数据包分析程序，随时监控当前目录下的文件，一旦发现有新的崩溃数据包，立即进行分析，并及时返回分析结果数据；另一种是 Windows 机器调用另一云崩溃服务器的自动化分析接口对崩溃数据包进行分析。

随后，方法 200 进入步骤 S213，其中将崩溃数据包的分析结果数据下发到上传崩溃数据包的浏览器。

进一步的，本方法还可以包括：按照预设时间间隔，以增量索引的方式将崩溃数据包的分析结果数据存储在数据库中。具体来说，分析结果数据采用 MYSQL（主+从）+SPHINX 的架构，所采用的技术为主从数据库分离、按月分表的技术，其中 MYSQL 为永久存储引擎，MYSQL 的主从之间的数据自动同步。主 MYSQL 专门用于分析结果数据的插入，如上述云崩溃服务器将分析得到的分析结果数据插入到主 MYSQL 中。从 MYSQL 用于后台管理员管理，也可作为 SPHINX 服务器的索引源头，使得 SPHINX 索引服务器可以对于不断更新的崩溃数据包的分析结果数据进行增量索引，实现管理员的实时数据的检索。具体来说，SPHINX 索引服务器每隔 5 分钟利用增量索引、合并索引方式达到数据实时更新。当数据库中已有数据量很大，又不断有新数据加入到数据库时，如果全部重新建立索引很消耗资源，事实上，在原有数据上需要更新的数据相比较而言很少，例如原来的数据有几百万条，而新增的只是几千条，这样就可以使用“主索引+增量索引”的模式来实现近乎实时更新的功能。

本方法还可以包括：将接收到的崩溃状态信息放入队列，启动进程将队列中的崩溃状态信息存入到主 MYSQL 中。

一方面，管理员借助 SPHINX 索引服务器对于从 MySQL 中收集的崩溃状态信息进

行检索以获取例如哪个 IE 版本的崩溃最多、哪个主程序（浏览器）的崩溃最多、哪种类型的崩溃最多等信息，其直接在崩溃状态信息中依据上述列举消息的请求量给出崩溃的预警信息。将这些检索得到的数据发送到提交崩溃数据包的浏览器进行显示，对用户进行预警哪些浏览器中的崩溃最多。例如可以显示浏览器的各种版本单独监控结果或版本间的对比结果，可以显示每个浏览器版本的各种问题的数据量统计，或者问题数据量超过预期阀值也可以直接通过短信方式报警以提醒用户。

另一方面，存储在 MySQL 的崩溃数据包的分析结果数据可以包含以下信息：已经分析出来的崩溃模块或函数名称（也可以是关键模块的崩溃情况，即依据收集的崩溃信息中分析、统计出来的关键崩溃模块的信息）；调用上述崩溃模块或函数之前的行为、动作（例如变量名冲突、内存崩溃等）；待依据需求再定的内容（后续扩展的内容）。这样管理者可以进一步检索 MySQL 中的分析结果记录，通过 SPHINX 索引服务器获取指定机器标识（MID）的分析结果，然后依据 MID 显示在客户端的浏览器，对客户端的浏览器进行提示和预警。可选地，除了上述 MID，还可以进一步在云崩溃服务器侧获取分析结果的浏览器用户的标识（QID），该 QID 为浏览器用户的唯一标识，在用户登录时就使用该 QID 进行唯一标识，这样可以实现对于特定用户（对应着 QID）的崩溃分析，从而实现特定用户的预警提示。

综上，根据浏览器的登录用户和非登录用户上报的崩溃数据包或崩溃状态信息，能够及时的获取到基于崩溃状态信息和/或该次崩溃分析结果的预警告示，实现实时化、个性化的预警。

根据上述实施例提供的方法，在接收到浏览器崩溃时上传的浏览器崩溃状态信息之后，根据该浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息，并反馈给浏览器，以供浏览器根据崩溃标识信息确定是否得到上传崩溃数据包的允许。在得到允许的情况下，浏览器上传崩溃数据包，云端启动自动分析程序对崩溃数据包进行分析，并将分析结果数据下发给浏览器。该方法提供了一种云系统级的方案，能够有针对性地对浏览器的崩溃信息进行收集、处理、分析以及鉴定。

图 3 示出了根据本发明一个实施例的浏览器崩溃信息的处理系统的结构框图。如图 3 所示，该系统包括第一接口 310、第一云崩溃服务器 320、第二接口 330、分析设备 340 和下发设备 350。

其中第一接口 310 用于接收浏览器崩溃时上传的浏览器崩溃状态信息。可选地，第一接口 310 为 Get 接口。浏览器崩溃状态信息至少包括如下信息中的一种或多种：浏览器崩溃公共参数信息、命令行、浏览器产品名称以及第一浏览器侧数据校验信息，其中第一浏览器侧数据校验信息是浏览器根据浏览器崩溃公共参数信息和预设密钥生成的。浏览器崩溃公共参数信息至少包括如下信息：崩溃模块的相关信息、具体崩溃偏移、崩溃堆栈、浏览器版本号以及操作系统版本号。浏览器崩溃状态信息的具体内容可以参见上述方法实施例的描述。

进一步的，该系统还可包括：第一校验模块 311 和/或第一验证模块 312。在图 3 中，

第一校验模块 311 和第一验证模块 312 集成在第一接口 310 中，但本发明不仅限于此。其中，第一校验模块 311 用于通过验证第一浏览器侧数据校验信息是否正确来对崩溃状态信息的合法性和完整性进行校验。第一验证模块 312 用于通过效验浏览器产品名称来对浏览器产品的合法性进行校验。

该系统还可包括：第二缓存服务器 360，用于丢弃在预先定义的时间段内从相同地址的浏览器再次接收到的浏览器崩溃状态信息。为了防止浏览器在短时间内（比如 2s）连续提交相同的信息，通过进行缓存进行提交限制，在短时间内连续提交的信息视为一次提交，判断规则可基于第一浏览器侧数据校验信息。

第一云崩溃服务器 320 用于根据浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息，通过第一接口 310 反馈崩溃标识信息到浏览器。可选的，该系统还包括：第一缓存服务器 370，用于按照预设算法对浏览器崩溃公共参数信息进行处理，生成崩溃键值；第一云崩溃服务器 320 具体用于根据崩溃键值，得到指示是否允许浏览器上传崩溃数据包的崩溃标识信息。具体来说，第一缓存服务器 370 从浏览器崩溃公共参数信息中提取出崩溃模块的相关信息、具体崩溃偏移、崩溃堆栈、浏览器版本号、操作系统版本号等信息，根据这些信息生成崩溃键值（dumpkey），例如对这些信息进行 MD5 算法加密得到 dumpkey。第一云崩溃服务器 320 累计对相同的浏览器崩溃状态信息的接收次数，具体做法就是累计相同 dumpkey 的数目，如果相同 dumpkey 的数目大于或等于预设阈值（比如 3），表明云端对相同的浏览器崩溃状态信息的接收次数已大于或等于 3 次，则生成的 dumpid 为 0，即不允许浏览器上传崩溃数据包；如果相同 dumpkey 的数目小于 3，则生成的 dumpid 大于 0，如 dumpid=dump_id，dump_id 为大于 0 的值，即允许浏览器上传崩溃数据包。

可选的，第一云崩溃服务器 320 还用于根据崩溃标识信息和预设密钥生成第一服务器侧数据校验信息，并在反馈崩溃标识信息到浏览器的同时，反馈第一服务器侧数据校验信息到浏览器，以供浏览器通过验证第一服务器侧数据校验信息来对崩溃标识信息的合法性和完整性进行校验。

浏览器接收到上述回传信息后，提取 dumpid，如果 dumpid 为 0，表明云端不允许浏览器上传崩溃数据包，那么此次交手结束。如果 dumpid 为 dump_id，表明云端允许浏览器上传崩溃数据包。

该系统还包括：数据库 380 和数据队列服务器 390。数据队列服务器 390 用于将崩溃状态信息放入队列，启动进程将队列中的崩溃状态信息存入到数据库 380 中。

第二接口 330 用于在崩溃标识信息表明允许浏览器上传崩溃数据包的情况下，接收浏览器上传的包括崩溃数据包的崩溃信息。可选地，第二接口 330 为 Post 接口。崩溃信息可以包含浏览器产品名称，崩溃标识信息，崩溃数据包和第二浏览器侧数据校验信息，其中第二浏览器侧数据校验码是根据崩溃数据包、崩溃标识信息和预设密钥而生成的。崩溃信息的具体内容可以参见上述方法实施例的描述。

进一步的，该系统还可包括：第二校验模块 331 和/或第二验证模块 332。在图 3 中，

第二校验模块 331 和第二验证模块 332 集成在第二接口 330 中，但本发明不仅限于此。第二校验模块 331 用于通过验证第二浏览器侧数据校验信息是否正确来对崩溃信息的合法性和完整性进行校验。第二验证模块 332 用于通过效验浏览器产品名称来对浏览器产品的合法性进行校验。

该系统还可以包括：第二云崩溃服务器 410 和持久化存储器 420。其中第二云崩溃服务器 410 用于从崩溃信息中提取出崩溃数据包，将崩溃数据包存入队列中；以及，读取队列，将来自不同浏览器产品的崩溃数据包分送给不同的分析设备；持久化存储器 420 用于存储崩溃数据包。第二云崩溃服务器 410 接收的崩溃数据包来自很多客户端的浏览器。一方面，第二云崩溃服务器 410 将上传的崩溃数据包保存为临时文件，移动到临时目录；另一方面，第二云崩溃服务器 410 将通过 Post 接口上传的崩溃数据包存入到队列中（每一台服务器都可以有一个队列），然后，给浏览器返回信息，通知浏览器上传数据是否成功。第二云崩溃服务器 410 还将崩溃数据包存储到持久化存储器 420 中，持久化存储器 420 可以为 Cassandra 数据库。

分析设备 340 用于启动崩溃数据包自动分析程序，对崩溃数据包进行分析。在本系统中，分析设备 340 可以为多台 Windows 环境下的 Windows 机器，以第二云崩溃服务器 410 为 Linux 操作系统为例，Linux 系统向 Windows 同步文件可以采用基于 C/S 模式软件的 rsync 实现，rsync 是数据镜像备份工具，可以镜像保存整个目录树和文件系统。在同步到 Windows 机器目录下后，在临时目录下的已被同步的崩溃数据包被删除。分析设备 340 进一步用于：通过部署的自动崩溃数据包分析程序，随时监控浏览器上传的崩溃数据包，一旦发现有新的崩溃数据包，立即进行分析，并及时返回分析结果数据；或者，调用自动化分析接口对浏览器上传的崩溃数据包进行分析。

下发设备 350 用于通过第二接口 330 将崩溃数据包的分析结果数据下发到上传崩溃数据包的浏览器。下发设备 350 进一步用于根据崩溃数据包的分析结果数据所对应的浏览器的机器标识或浏览器用户的标识，将崩溃数据包的分析结果数据下发到对应的浏览器。

本系统还可以包括：第三云崩溃服务器 430 和索引服务器 440。第三云崩溃服务器 430 用于将分析设备 340 分析得到的数据传输给索引服务器 440。索引服务器 440 用于按照预设时间间隔，以增量索引的方式将崩溃数据包的分析结果数据存储在数据库 380 中。具体来说，本系统采用 MYSQL（主+从）+SPHINX 的架构，即数据库 380 包括主 MYSQL 和从 MYSQL，索引服务器 440 为 SPHINX 索引服务器。数据库 380 所采用的技术为主从数据库分离、按月分表的技术，MYSQL 为永久存储引擎，MYSQL 的主从之间的数据自动同步。主 MYSQL 专门用于分析结果数据的插入，如上述第三云崩溃服务器 430 向分析设备 340 提供自动化分析接口，将分析得到的分析结果数据插入到主 MYSQL 中。从 MYSQL 用于后台管理员管理，也可作为 SPHINX 服务器的索引源头，使得 SPHINX 索引服务器可以对于不断更新的崩溃数据包的分析结果数据进行增量索引，实现管理员的实时数据的检索。

本系统还可以包括：预警设备 450，用于对数据库中存储的数据进行统计，如果统计结果超出预设阀值则进行报警。一方面，管理员借助 SPHINX 索引服务器对于从 MySQL 中收集的崩溃状态信息进行检索以获取例如哪个 IE 版本的崩溃最多、哪个主程序（浏览器）的崩溃最多、哪种类型的崩溃最多等信息，其直接在崩溃状态信息中依据上述列举消息的请求量给出崩溃的预警信息。将这些检索得到的数据发送到提交崩溃数据包的浏览器进行显示，对用户进行预警哪些浏览器中的崩溃最多。例如可以显示浏览器的各种版本单独监控结果或版本间的对比结果，可以显示每个浏览器版本的各种问题的数据量统计，或者问题数据量超过预期阀值也可以直接通过短信方式报警以提醒用户。另一方面，存储在 MySQL 的崩溃数据包的分析结果数据可以包含以下信息：已经分析出来的崩溃模块或函数名称（也可以是关键模块的崩溃情况，即依据收集的崩溃信息中分析、统计出来的关键崩溃模块的信息）；调用上述崩溃模块或函数之前的行为、动作（例如变量名冲突、内存崩溃等）；待依据需求再定的内容（后续扩展的内容）。这样管理者可以进一步检索 MySQL 中的分析结果记录，通过 SPHINX 索引服务器获取指定机器标识（MID）的分析结果，然后依据 MID 显示在客户端的浏览器，对客户端的浏览器进行提示和预警。可选地，除了上述 MID，还可以进一步在云崩溃服务器侧获取分析结果的浏览器用户的标识（QID），该 QID 为浏览器用户的唯一标识，在用户登录时就使用该 QID 进行唯一标识，这样可以实现对于特定用户（对应着 QID）的崩溃分析，从而实现特定用户的预警提示。综上，根据浏览器的登录用户和非登录用户上报的崩溃数据包或崩溃状态信息，能够及时的获取到基于崩溃状态信息和/或该次崩溃分析结果的预警告示，实现实时化、个性化的预警。

根据上述实施例提供的系统，在第一接口接收到浏览器崩溃时上传的浏览器崩溃状态信息之后，第一云崩溃服务器根据该浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息，并通过第一接口反馈给浏览器，以供浏览器根据崩溃标识信息确定是否得到上传崩溃数据包的允许。在得到允许的情况下，浏览器上传崩溃数据包，云端通过第二接口接收该崩溃数据包，分析设备启动自动分析程序对崩溃数据包进行分析，并由下发设备将分析结果数据下发给浏览器。该系统提供了一种云系统级的方案，能够有针对性地对浏览器的崩溃信息进行收集、处理、分析以及鉴定。

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。

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。

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。

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。

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。

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浏览器崩溃信息的处理系统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。

例如，图 4 示出了可以实现根据本发明的一个实施例的执行本发明所述方法的服务器，例如应用服务器。该服务器传统上包括处理器 410 和以存储器 420 形式的计算机程序产品或者计算机可读介质。存储器 420 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 420 具有用于执行上述方法中的任何方法步骤的程序代码 431 的存储空间 430。例如，用于程序代码的存储空间 430 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 431。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图 5 所述的便携式或者固定存储单元。该存储单元可以具有与图 4 的服务器中的存储器 420 类似布置的存储段、存储空间等。

程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 431'，即可以由例如诸如 410 之类的处理器读取的代码，这些代码当由服务器运行时，导致该服务器执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

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。

此外，还应当注意，本说明书中使用的语言主要是为了可读性和教导的目的而选择的，而不是为了解释或者限定本发明的主题而选择的。因此，在不偏离所附权利要求书的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。对于本发明的范围，对本发明所做的公开是说明性的，而非限制性的，本发明的范围由所附权利要求书限定。

权 利 要 求

1、一种浏览器崩溃信息的处理方法，包括：

接收浏览器崩溃时上传的浏览器崩溃状态信息；

根据所述浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息；

反馈所述崩溃标识信息到所述浏览器；

在所述崩溃标识信息表明允许浏览器上传崩溃数据包的情况下，接收所述浏览器上传的包括崩溃数据包的崩溃信息；

启动崩溃数据包自动分析程序，对所述崩溃数据包进行分析；

将所述崩溃数据包的分析结果数据下发到所述上传崩溃数据包的浏览器。

2、根据权利要求 1 所述的方法，所述接收浏览器崩溃时上传的浏览器崩溃状态信息的步骤进一步为：使用 Get 接口接收浏览器崩溃时上传的浏览器崩溃状态信息。

3、根据权利要求 1 所述的方法，所述接收所述浏览器上传的包括崩溃数据包的崩溃信息的步骤进一步为：使用 Post 接口接收所述浏览器上传的包括崩溃数据包的崩溃信息。

4、根据权利要求 1 至 3 任一项所述的方法，所述浏览器崩溃状态信息至少包括如下信息中的一种或多种：浏览器崩溃公共参数信息、命令行、浏览器产品名称以及第一浏览器侧数据校验信息，其中所述第一浏览器侧数据校验信息是所述浏览器根据所述浏览器崩溃公共参数信息和预设密钥生成的。

5、根据权利要求 4 所述的方法，所述浏览器崩溃公共参数信息至少包括如下信息：崩溃模块的相关信息、具体崩溃偏移、崩溃堆栈、浏览器版本号以及操作系统版本号。

6、根据权利要求 4 或 5 所述的方法，所述根据所述浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息进一步包括：

按照预设算法对所述浏览器崩溃公共参数信息进行处理，生成崩溃键值；

根据所述崩溃键值，得到所述指示是否允许浏览器上传崩溃数据包的崩溃标识信息。

7、根据权利要求 6 所述的方法，在所述按照预设算法对所述浏览器崩溃公共参数信息进行处理，生成崩溃键值的步骤之前还包括：通过验证所述第一浏览器侧数据校验信息是否正确来对所述崩溃状态信息的合法性和完整性进行校验。

8、根据权利要求 6 所述的方法，在所述按照预设算法对所述浏览器崩溃公共参数信息进行处理，生成崩溃键值的步骤之前还包括：通过效验浏览器产品名称来对浏览器产品的合法性进行校验。

9、根据权利要求 1 所述的方法，所述接收浏览器崩溃时上传的浏览器崩溃状态信息的步骤之后还包括：丢弃在预先定义的时间段内从相同地址的浏览器再次接收到的浏览器崩溃状态信息。

10、根据权利要求 1 所述的方法，在所述反馈崩溃标识信息到浏览器的同时，反馈第一服务器侧数据校验信息到所述浏览器，以供所述浏览器通过验证所述第一服务器侧

数据校验信息来对崩溃标识信息的合法性和完整性进行校验；所述第一服务器侧数据校验信息是根据所述崩溃标识信息和预设密钥而生成的。

11、根据权利要求 1 所述的方法，在所述接收浏览器上传的包括崩溃数据包的崩溃信息的步骤之后还包括：将所述崩溃数据包存入队列中；读取所述队列，将来自不同浏览器产品的崩溃数据包分送给不同的分析设备；

所述启动崩溃数据包自动分析程序，对所述崩溃数据包进行分析具体为：不同的分析设备启动各自的崩溃数据包自动分析程序，对所述崩溃数据包进行分析。

12、根据权利要求 11 所述的方法，所述崩溃信息还包括第二浏览器侧数据校验信息；所述第二浏览器侧数据校验码是根据所述崩溃数据包、崩溃标识信息和预设密钥而生成的；

在所述将崩溃数据包存入队列中的步骤之前还包括：通过验证所述第二浏览器侧数据校验信息是否正确来对所述崩溃信息的合法性和完整性进行校验。

13、根据权利要求 11 所述的方法，所述崩溃信息还包括：浏览器产品名称；在所述将崩溃数据包存入队列中的步骤之前还包括：通过效验浏览器产品名称来对浏览器产品的合法性进行校验。

14、根据权利要求 1 所述的方法，所述启动崩溃数据包自动分析程序，对所述崩溃数据包进行分析的步骤进一步包括：

通过部署的自动崩溃数据包分析程序，随时监控浏览器上传的崩溃数据包，一旦发现有新的崩溃数据包，立即进行分析，并及时返回分析结果数据；

或者，调用自动化分析接口对浏览器上传的崩溃数据包进行分析。

15、根据权利要求 1 所述的方法，还包括：按照预设时间间隔，以增量索引的方式将所述崩溃数据包的分析结果数据存储在数据库中。

16、根据权利要求 15 所述的方法，还包括：对所述数据库中存储的数据进行统计，如果统计结果超出预设阀值则进行报警。

17、根据权利要求 1 所述的方法，所述将崩溃数据包的分析结果数据下发到所述上传崩溃数据包的浏览器的步骤进一步包括：根据所述崩溃数据包的分析结果数据所对应的浏览器的机器标识或浏览器用户的标识，将所述崩溃数据包的分析结果数据下发到对应的浏览器。

18、一种浏览器崩溃信息的处理系统，包括：

第一接口，用于接收浏览器崩溃时上传的浏览器崩溃状态信息；

第一云崩溃服务器，用于根据所述浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息，通过所述第一接口反馈所述崩溃标识信息到所述浏览器；

第二接口，用于在所述崩溃标识信息表明允许浏览器上传崩溃数据包的情况下，接收所述浏览器上传的包括崩溃数据包的崩溃信息；

分析设备，用于启动崩溃数据包自动分析程序，对所述崩溃数据包进行分析；

下发设备，用于通过所述第二接口将所述崩溃数据包的分析结果数据下发到所述上

传崩溃数据包的浏览器。

19、根据权利要求 18 所述的系统，所述第一接口为 Get 接口。

20、根据权利要求 18 所述的系统，所述第二接口为 Post 接口。

21、根据权利要求 18 至 20 任一项所述的系统，所述浏览器崩溃状态信息至少包括如下信息中的一种或多种：浏览器崩溃公共参数信息、命令行、浏览器产品名称以及第一浏览器侧数据校验信息，其中所述第一浏览器侧数据校验信息是所述浏览器根据所述浏览器崩溃公共参数信息和预设密钥生成的。

22、根据权利要求 21 所述的系统，所述浏览器崩溃公共参数信息至少包括如下信息：崩溃模块的相关信息、具体崩溃偏移、崩溃堆栈、浏览器版本号以及操作系统版本号。

23、根据权利要求 21 或 22 所述的系统，还包括：第一缓存服务器，用于按照预设算法对所述浏览器崩溃公共参数信息进行处理，生成崩溃键值；

所述第一云崩溃服务器具体用于根据所述崩溃键值，得到所述指示是否允许浏览器上传崩溃数据包的崩溃标识信息。

24、根据权利要求 23 所述的系统，还包括：第一校验模块，用于通过验证所述第一浏览器侧数据校验信息是否正确来对所述崩溃状态信息的合法性和完整性进行校验。

25、根据权利要求 23 所述的系统，还包括：第一验证模块，用于通过效验浏览器产品名称来对浏览器产品的合法性进行校验。

26、根据权利要求 18 所述的系统，还包括：第二缓存服务器，用于丢弃在预先定义的时间段内从相同地址的浏览器再次接收到的浏览器崩溃状态信息。

27、根据权利要求 18 所述的系统，所述第一云崩溃服务器还用于根据所述崩溃标识信息和预设密钥生成第一服务器侧数据校验信息，并在反馈崩溃标识信息到浏览器的同时，反馈第一服务器侧数据校验信息到所述浏览器，以供所述浏览器通过验证所述第一服务器侧数据校验信息来对崩溃标识信息的合法性和完整性进行校验。

28、根据权利要求 18 所述的系统，还包括：

数据库；

数据队列服务器，用于将崩溃状态信息放入队列，启动进程将队列中的崩溃状态信息存入到所述数据库中。

29、根据权利要求 18 所述的系统，还包括：

第二云崩溃服务器，用于从崩溃信息中提取出崩溃数据包，将所述崩溃数据包存入队列中；以及，读取所述队列，将来自不同浏览器产品的崩溃数据包分送给不同的所述分析设备；

持久化存储器，用于存储所述崩溃数据包。

30、根据权利要求 29 所述的系统，所述崩溃信息还包括第二浏览器侧数据校验信息；所述第二浏览器侧数据校验码是根据所述崩溃数据包、崩溃标识信息和预设密钥而生成的；

所述系统还包括：第二校验模块，用于通过验证所述第二浏览器侧数据校验信息是

否正确来对所述崩溃信息的合法性和完整性进行校验。

31、根据权利要求 29 所述的系统，所述崩溃信息还包括浏览器产品名称；

所述系统还包括：第二验证模块，用于通过效验浏览器产品名称来对浏览器产品的合法性进行校验。

32、根据权利要求 18 所述的系统，所述分析设备进一步用于：

通过部署的自动崩溃数据包分析程序，随时监控浏览器上传的崩溃数据包，一旦发现有新的崩溃数据包，立即进行分析，并及时返回分析结果数据；

或者，调用自动化分析接口对浏览器上传的崩溃数据包进行分析。

33、根据权利要求 18 所述的系统，还包括：

数据库；

第三云崩溃服务器，用于将分析设备分析得到的数据传输给索引服务器；

索引服务器，用于按照预设时间间隔，以增量索引的方式将所述崩溃数据包的分析结果数据存储在数据库中。

34、根据权利要求 33 所述的系统，还包括：预警设备，用于对所述数据库中存储的数据进行统计，如果统计结果超出预设阀值则进行报警。

35、根据权利要求 18 所述的系统，所述下发设备进一步用于根据所述崩溃数据包的分析结果数据所对应的浏览器的机器标识或浏览器用户的标识，将所述崩溃数据包的分析结果数据下发到对应的浏览器。

36、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在服务器上运行时，导致所述服务器执行根据权利要求 1-17 中的任一个所述的浏览器崩溃信息的处理方法。

37、一种计算机可读介质，其中存储了如权利要求 36 所述的计算机程序。

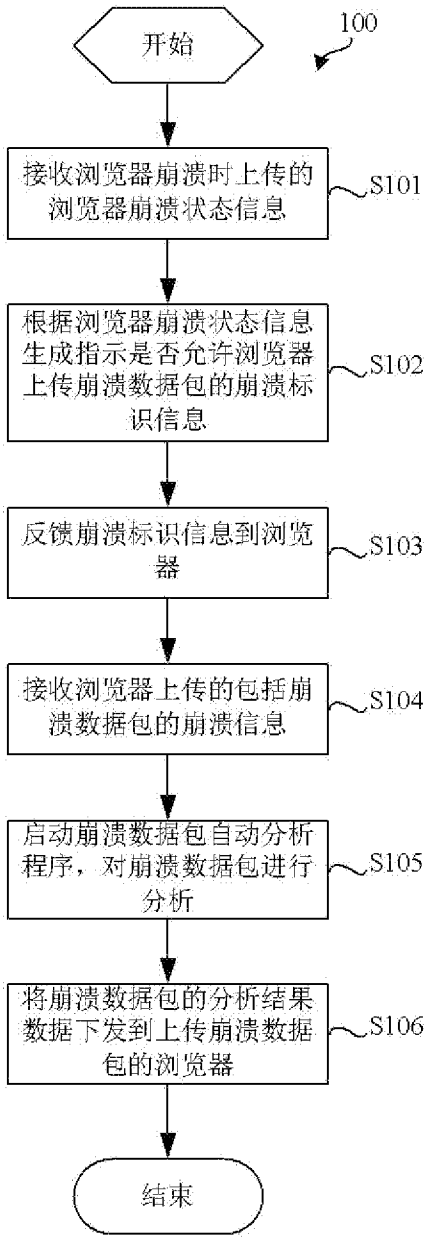

开始
100
接收浏览器崩溃时上传的浏览器崩溃状态信息
S101
根据浏览器崩溃状态信息生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息
S102
反馈崩溃标识信息到浏览器
S103
接收浏览器上传的包括崩溃数据包的崩溃信息
S104
启动崩溃数据包自动分析程序，对崩溃数据包进行分析
S105
将崩溃数据包的分析结果数据下发到上传崩溃数据包的浏览器
S106
结束

图 1

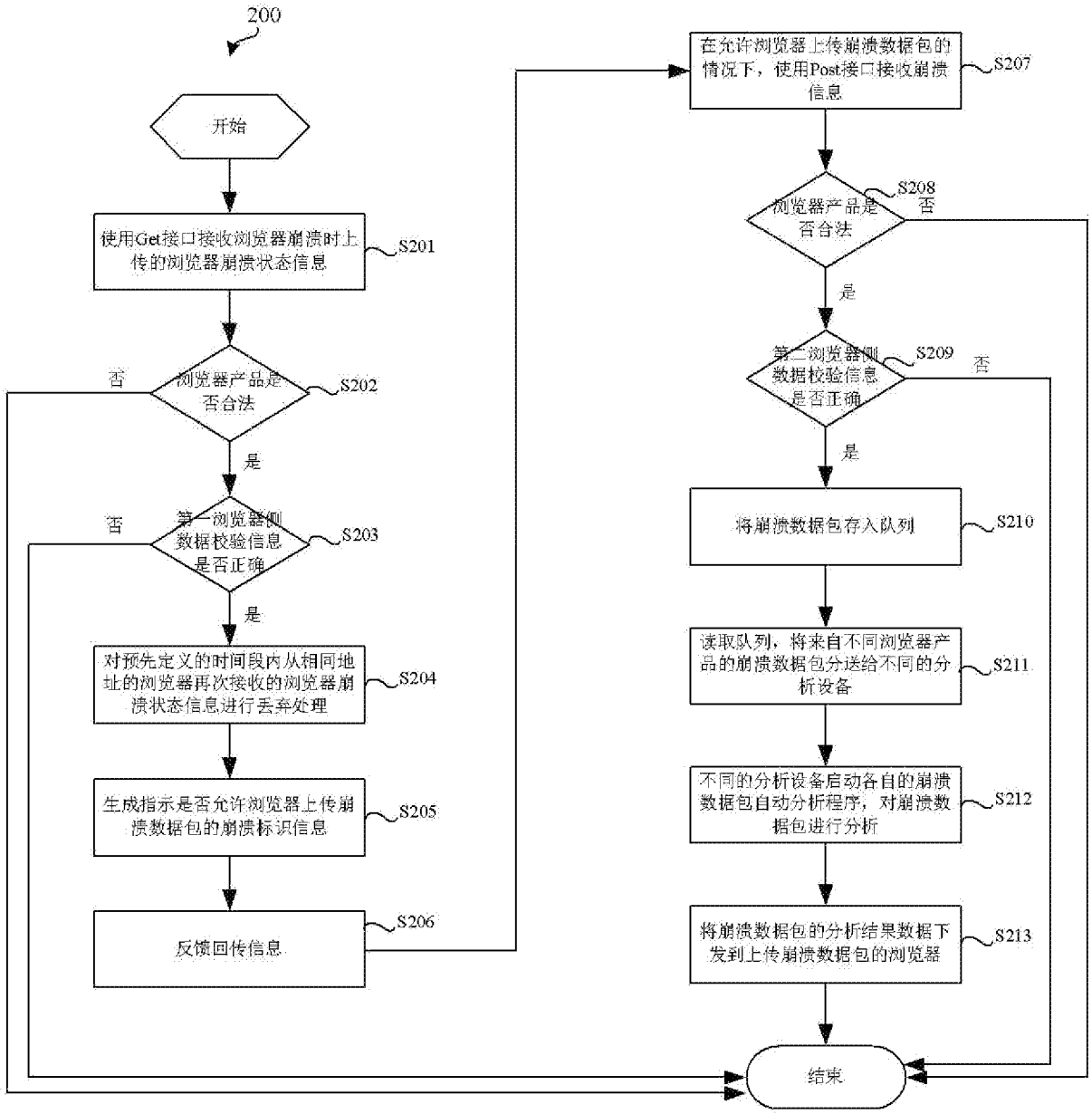

200
开始
使用Get接口接收浏览器崩溃时上传的浏览器崩溃状态信息
S201
浏览器产品是否合法
S202
否
是
第一浏览器侧数据校验信息是否正确
S203
否
是
对预先定义的时间段内从相同地址的浏览器再次接收的浏览器崩溃状态信息进行丢弃处理
S204
生成指示是否允许浏览器上传崩溃数据包的崩溃标识信息
S205
反馈回传信息
S206
在允许浏览器上传崩溃数据包的情况下，使用Post接口接收崩溃信息
S207
浏览器产品是否合法
S208
否
是
第二浏览器侧数据校验信息是否正确
S209
否
是
将崩溃数据包存入队列
S210
读取队列，将来自不同浏览器产品的崩溃数据包分送给不同的分析设备
S211
不同的分析设备启动各自的崩溃数据包自动分析程序，对崩溃数据包进行分析
S212
将崩溃数据包的分析结果数据下发到上传崩溃数据包的浏览器
S213
结束

图 2

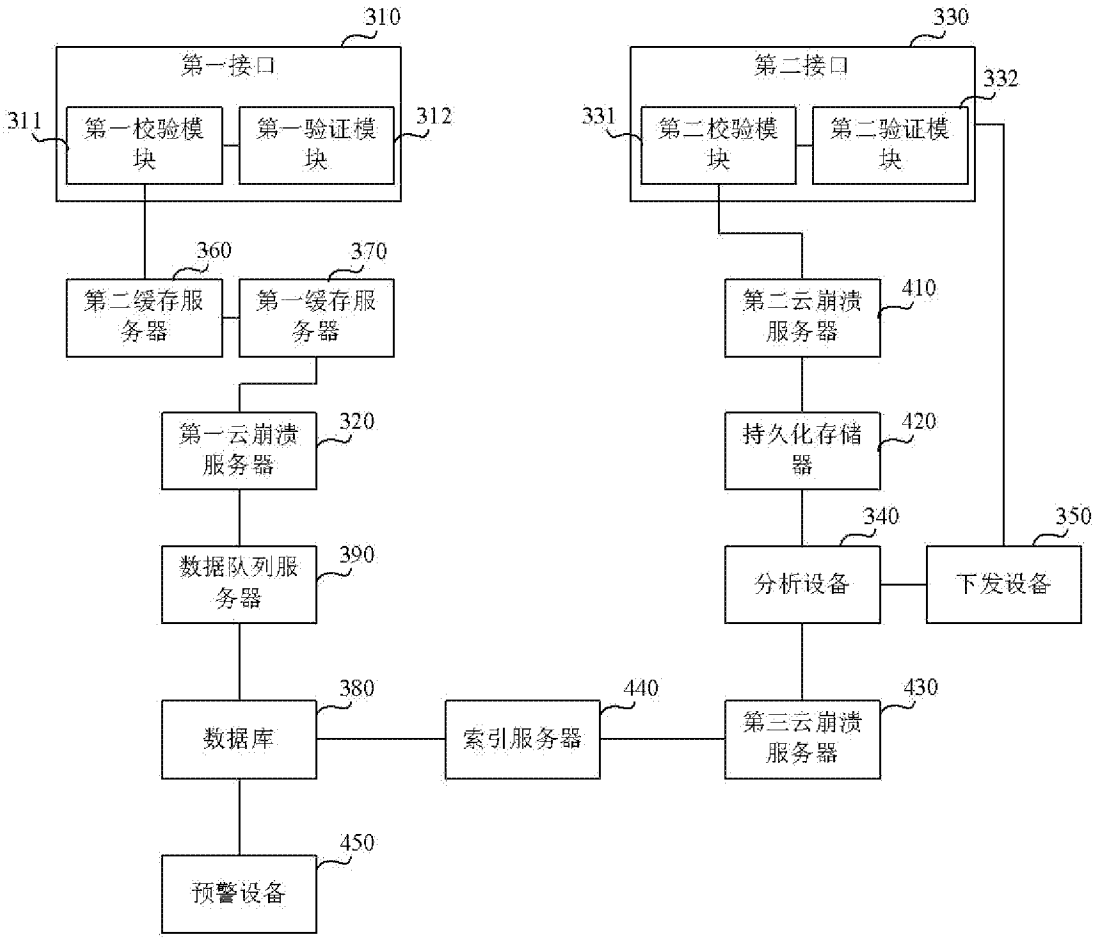

310
第一接口
311
第一校验模块
第一验证模块
312
330
第二接口
332
331
第二校验模块
第二验证模块
360
第二缓存服务器
370
第一缓存服务器
410
第二云崩溃服务器
320
第一云崩溃服务器
420
持久化存储器
340
350
分析设备
下发设备
390
数据队列服务器
380
数据库
440
索引服务器
430
第三云崩溃服务器
450
预警设备

图 3

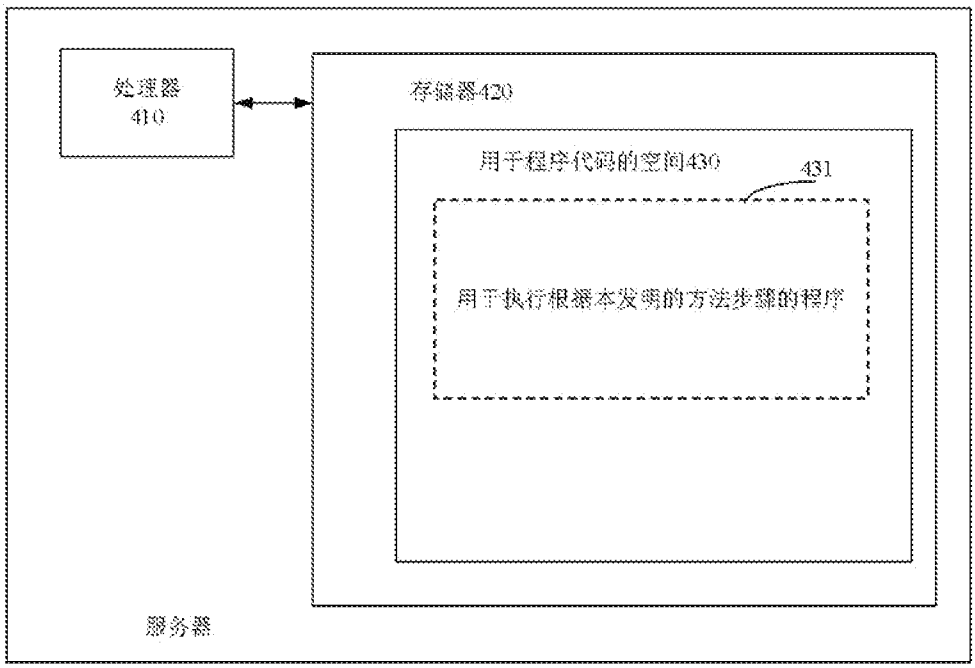

处理器
410
存储器420
用于程序代码的空间430
431
用于执行根据本发明的方法步骤的程序
服务器

图 4

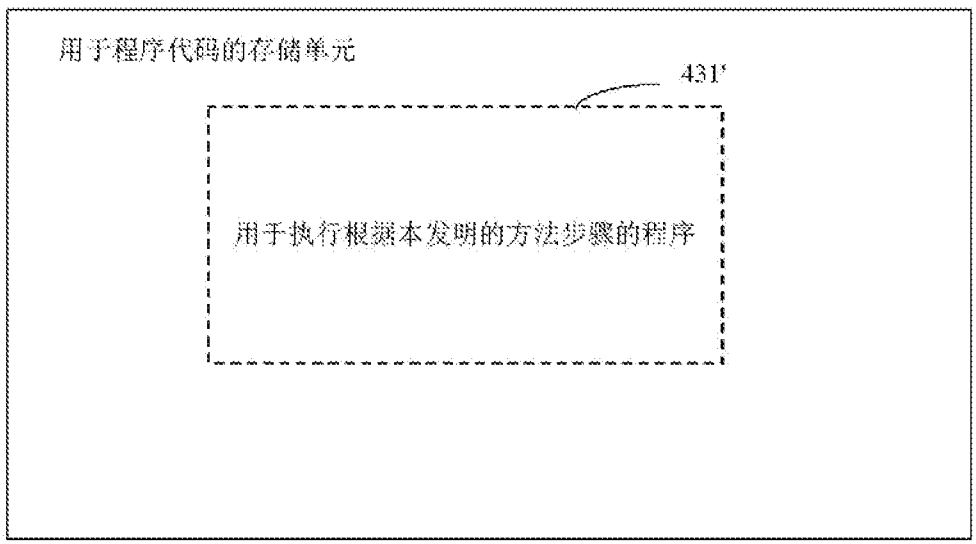

用于程序代码的存储单元
431'
用于执行根据本发明的方法步骤的程序

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/070185

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/14 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 17/-, H04L 29/-

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS, SIPOABS, DWPI: state, parameter, analyse, feedback, send, allow, notification, browser, crash, corrupt+, upload, response, no responding, web page, website, exception, abnormity

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103019879 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 03 April 2013 (03.04.2013), claims 1-35	1-37
PX	CN 103078945 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 01 May 2013 (01.05.2013), description, pages 2-13	1-37
PX	CN 103152381 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 12 June 2013 (12.06.2013), description, pages 5-26	1-37
PX	CN 103167016 A (BEIJING QIHOO TECHNOLOGY CO., LTD. et al.), 19 June 2013 (19.06.2013), description, pages 5-17	1-37
A	WU, Fang; Strategy of Microsoft. NET: the browser - from different perspectives, ELECTRONIC COMPUTER AND EXTERNAL EQUIPMENT, 30 June 2001 (30.06.2001), 2001, no. 6, pages 108-111	1-37
A	CN 102510538 A (SHENZHEN SKYWORTH RGB ELECTRONICS CO., LTD.), 20 June 2012 (20.06.2012), the whole document	1-37

☒ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 March 2014 (27.03.2014)	**22 April 2014 (22.04.2014)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **YI, Jian** Telephone No.: (86-10) **62411692**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/070185

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2012060065 A1(EICKMEYER, K. et al.), 08 March 2012 (08.03.2012), the whole document	1-37

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2014/070185

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103019879 A	03.04.2013	None	
CN 103078945 A	01.05.2013	None	
CN 103152381 A	12.06.2013	None	
CN 103167016 A	19.06.2013	None	
CN 102510538 A	20.06.2012	None	
US 2012060065 A1	08.03.2012	None	

国际检索报告

国际申请号 PCT/CN2014/070185

A. 主题的分类

H04L 29/14(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F17/-, H04L 29/-

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CPRSABS, SIPOABS, DWPI: 浏览器，网页，网站，崩溃，失去响应，无响应，异常，状态，参数，分析，解析，上传，反馈，发送，允许，通知，browser, crash, corrupt+, upload, response, no responding, web page, web site, exception, abnormity

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 103019879 A (北京奇虎科技有限公司等) 2013年 4月 03日 (2013-04-03) 权利要求1-35	1-37
PX	CN 103078945 A (北京奇虎科技有限公司等) 2013年 5月 01日 (2013-05-01) 说明书第2-13页	1-37
PX	CN 103152381 A (北京奇虎科技有限公司等) 2013年 6月 12日 (2013-06-12) 说明书第5-26页	1-37
PX	CN 103167016 A (北京奇虎科技有限公司等) 2013年 6月 19日 (2013-06-19) 说明书第5-17页	1-37
A	吴放. "Microsoft.NET战略之浏览器篇——横看成岭侧成峰" 电子计算机与外部设备, 2001年 6月 30日 (2001-06-30), 2001年第6期, 第108-111页	1-37
A	CN 102510538 A (深圳创维-RGB电子有限公司) 2012年 6月 20日 (2012-06-20) 全文	1-37

☑ 其余文件在C栏的续页中列出。 ☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2014年 3月 27日	2014年 4月 22日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 中国	伊健
传真号 (86-10)62019451	电话号码 (86-10)62411692

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
A	US 2012060065 A1 ((EICKMEYER KELLIE 等)) 2012年 3月 08日 (2012-03-08) 全文	1-37

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2014/070185

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 103019879 A	2013年 4月 03日	无	
CN 103078945 A	2013年 5月 01日	无	
CN 103152381 A	2013年 6月 12日	无	
CN 103167016 A	2013年 6月 19日	无	
CN 102510538 A	2012年 6月 20日	无	
US 2012060065 A1	2012年 3月 08日	无	