(19)中华人民共和国国家知识产权局

(12)实用新型专利

(10)授权公告号 CN 202205195 U
(45)授权公告日 2012.04.25

(21)申请号 201120248200.0

(22)申请日 2011.07.14

(73)专利权人 山东省计算中心
地址 250014 山东省济南市历下区科院路19号

(72)发明人 顾卫东 王连海 张磊 武鲁

(74)专利代理机构 济南泉城专利商标事务所 37218
代理人 李桂存

(51)Int.Cl.
G06F 13/40(2006.01)
G06F 21/00(2006.01)

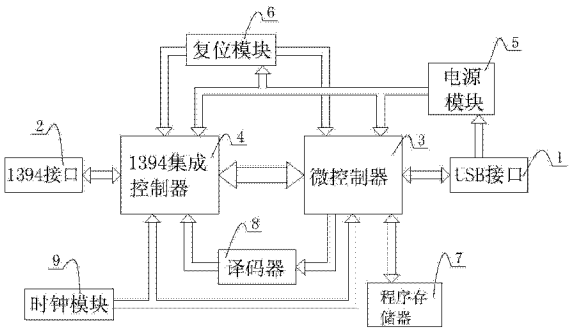
权利要求书 1 页 说明书 3 页 附图 1 页

(54)实用新型名称

一种通过 IEEE 1394 接口读写计算机物理内存的设备

(57)摘要

本实用新型的通过 IEEE 1394 接口读写计算机物理内存的设备，其特征在于：包括执行程序和起控制作用的微控制器、与微控制器相连接的1394 集成控制器、用于提供时钟信号的时钟模块以及提供电能的电源模块；所述微控制器和 1394 集成控制器分别设置有与取证计算机相连接的 USB 接口和与目标计算机相连接的 1394 接口，所述微控制器与 1394 集成控制器之间还设置有起扩展控制端口的译码器；所述微控制器外部扩展有程序存储器。本实用新型通过设置与目标计算机相连接的 1394 接口以及与取证计算机 USB 接口，实现了即插即用功能；并实现了目标计算机在密码保护状态(如屏保、锁定状态)下读写内存信息，提高了在线取证的灵活性和增强了在线取证的可信性，具有很高的使用价值。



CN 202205195 U

1. 一种通过 IEEE 1394 接口读写计算机物理内存的设备，其特征在于：包括执行程序和起控制作用的微控制器（3）、与微控制器相连接的 1394 集成控制器（4）、用于提供时钟信号的时钟模块（9）以及提供电能的电源模块（5）；所述微控制器和 1394 集成控制器分别设置有与取证计算机相连接的 USB 接口（1）和与目标计算机相连接的 1394 接口（2），所述微控制器与 1394 集成控制器之间还设置有起扩展控制端口的译码器（8）；所述微控制器外部扩展有程序存储器（7）。

2. 根据权利要求 1 所述的通过 IEEE 1394 接口读写计算机物理内存的设备，其特征在于：还设置有对微控制器（3）和 1394 集成控制器（4）进行控制的复位模块（6）；所述电源模块（5）的输入端与 USB 接口（1）的电源线相连接，电源模块的输出端与微控制器、1394 集成控制器和复位模块均相连接。

3. 根据权利要求 1 或 2 所述的通过 IEEE 1394 接口读写计算机物理内存的设备，其特征在于：所述时钟模块（9）的输出端与微控制器（3）和 1394 集成控制器（4）均相连接。

4. 根据权利要求 1 或 2 所述的通过 IEEE 1394 接口读写计算机物理内存的设备，其特征在于：所述 1394 集成控制器（4）包括物理层和链路层两部分，其为物理层和链路层集成的单独芯片或者物理层与链路层分别集成的两个芯片。

5. 根据权利要求 4 所述的通过 IEEE 1394 接口读写计算机物理内存的设备，其特征在于：所述 1394 集成控制器（4）的型号为 TSB43AA82A。

6. 根据权利要求 1 或 2 所述的通过 IEEE 1394 接口读写计算机物理内存的设备，其特征在于：所述微控制器（3）为带有 8051 控制器和 USB 接口的 CY7C68013A 芯片。

一种通过 IEEE 1394 接口读写计算机物理内存的设备

技术领域

[0001] 本实用新型涉及一种通过 IEEE 1394 接口读写计算机物理内存的设备，更具体的说，尤其涉及一种即插即用并对计算机内存改动很小的通过 IEEE 1394 接口读写计算机物理内存的设备。

背景技术

[0002] 随着计算机技术、计算机网络技术和互联网的飞速发展，计算机正在极大地促进人类社会的进步，计算机和电子数据已经深入到人们生活的各个方面。计算机技术在带给我们巨大的益处的同时也带来了计算机犯罪问题。各类黑客入侵、网络诈骗、网络色情等案件不断涌现。网络犯罪已涉及到绝大部分社会犯罪现象，已经影响了正常的经济秩序。而打击网络犯罪主要依靠的科技手段是计算机取证技术。

[0003] 作为计算机运行过程中程序和中间数据的存放地，计算机内存中含有大量的有用信息，包括程序进程运行状态、网络连接、开放端口、口令密码、加密文件的明文甚至密钥，这些信息往往在案件调查中起到关键作用。然而如何准确、完整地获取系统的内存，并尽量减少对目标系统的内存改变成为一个难题。在目标计算机上运行内存获取软件会造成内存大量改变，破坏了数字证据的完整性；而且由于 Windows 的 C2 安全等级，内存获取软件必须在开机状态才能运行，在屏保待机状态则无法运行。通过硬件接口获取内存的设备必须实现在目标计算机中安装，无法实现即插即用，显然，将此用于对犯罪嫌疑人的调查取证是不现实的。

发明内容

[0004] 本实用新型为了克服上述技术问题的缺点，提供了一种即插即用并对计算机内存改动很小的通过 IEEE 1394 接口读写计算机物理内存的设备。

[0005] 本实用新型的通过 IEEE 1394 接口读写计算机物理内存的设备，其特别之处在于：包括执行程序和起控制作用的微控制器、与微控制器相连接的 1394 集成控制器、用于提供时钟信号的时钟模块以及提供电能的电源模块；所述微控制器和 1394 集成控制器分别设置有与取证计算机相连接的 USB 接口和与目标计算机相连接的 1394 接口，所述微控制器与 1394 集成控制器之间还设置有起扩展控制端口的译码器；所述微控制器外部扩展有程序存储器。微控制器作为设备主控芯片，可对 1394 集成控制器的工作状态进行控制；1394 集成控制器为 1394 接口的控制芯片，1394 接口实现与目标计算机的连接。USB 接口实现与取证计算机的连接，并在微控制器的控制下，把 1394 接口传来的目标计算机的内存数据传送至取证计算机。时钟模块给微控制器和 1394 集成控制器提供工作脉冲；电源模块给整个设备提供电能。

[0006] 本实用新型的通过 IEEE 1394 接口读写计算机物理内存的设备，还设置有对微控制器和 1394 集成控制器进行控制的复位模块；所述电源模块的输入端与 USB 接口的电源线相连接，电源模块的输出端与微控制器、1394 集成控制器和复位模块均相连接。复位模块

为微控制器和1394集成控制器的复位电路，电源模块的输入端与USB接口中的电源线相连接，用于把5V电压转换为微控制器和1394集成控制器的工作电压进行输出。

[0007] 本实用新型的通过IEEE 1394接口读写计算机物理内存的设备，所述时钟模块的输出端与微控制器和1394集成控制器均相连接。

[0008] 本实用新型的通过IEEE 1394接口读写计算机物理内存的设备，所述1394集成控制器包括物理层和链路层两部分，其为物理层和链路层集成的单独芯片或者物理层与链路层分别集成的两个芯片。

[0009] 本实用新型的通过IEEE 1394接口读写计算机物理内存的设备，所述1394集成控制器的型号为TSB43AA82A。TSB43AA82A为TI公司的1394协议芯片。

[0010] 本实用新型的通过IEEE 1394接口读写计算机物理内存的设备，所述微控制器为带有8051控制器和USB接口的CY7C68013A芯片。CY7C68013A芯片不仅含有8051微控制器，而且还设置有USB接口，即实现了对整个设备的控制，还实现了与取证计算机的端口连接。

[0011] 本实用新型的有益效果是：本实用新型通过设置与目标计算机相连接的1394接口以及与取证计算机USB接口，具有即插即用功能；通过IEEE 1394接口直接读取计算机内存中的数据，并实现了目标计算机在密码保护状态(如屏保、锁定状态)下读写内存信息，不需要在计算机上运行软件，对目标计算机运行状态改动很小，提高了在线取证的灵活性和增强了在线取证的可信性，具有很高的使用价值。

附图说明

[0012] 图1为本实用新型的电路原理图；

[0013] 图2为本实用新型的样品图。

[0014] 图中：1 USB接口，2 1394接口，3 微控制器，4 1394集成控制器，5电源模块，6复位模块，7程序存储器，8译码器，9时钟模块，10壳体，11工作指示灯。

具体实施方式

[0015] 下面结合附图与实施例对本实用新型作进一步说明。

[0016] 如图1所示，给出了本实用新型的电路原理图，其包括USB接口1、1394接口2、微控制器3、1394集成控制器4、电源模块5、复位模块6、程序存储器7、译码器8、时钟模块9；微控制器3采用型号为CY7C68013A的芯片，该芯片中不仅设置有8051控制器，而且还设置有USB接口1；1394集成控制器4采用型号为TSB43AA82A的芯片，以便形成1394接口2。微控制器3不仅通过数据端口与1394集成控制器4相连接，而且还通过译码器8与其相连接，译码器为串行3线-8线译码器，由微控制器3中的8051单片机地址总线为1394控制器芯片提供片选信号。1394接口2和USB接口1分别实现与目标计算机和取证计算机的连接，分别用于接收目标计算机传输的内存数据和向取证计算机发送内存数据。电源模块5的输入端从USB接口的电源线上获取电压，电源模块5使用线性调压器完成电压调节，将USB总线上的5伏电压转化成3.3伏特的电压后输入到微控制器3和1394集成控制器4的电源输入端。复位模块6是微控制器3和1394集成控制器的复位电路，实现设备运行过程中的复位作用。时钟模块9实现微控制器3和1394集成控制器4所需的时钟信号。程序

存储器 7 采用串行 EEPROM 芯片，用于存放本设备的固件程序，通过 I2C 总线与 USB 控制器芯片 3 相连接。

[0017] 微控制器 3 负责整个系统的运行控制，包括参数接收、1394 集成控制器 4 的配置和控制、控制内存数据在 1394 集成控制器 4 和微控制器 3 之间的传输以及将获取的内存数据送至取证计算机。1394 控制器 4 包括物理层和链路层两部分，可选择两个单独的芯片或两层集成的芯片，负责 1394 数据包的发送和接收。利用 CY7C68013A 芯片携带的 8051 控制器作为微控制器 3 对 TSB43AA82A 的 CSR 描述和 ConfigROM 描述进行配置，将此设备配置成 Windows 本身已自带驱动并允许物理请求的 1394 Mass Storage 设备类，实现设备即插即用的功能，使目标计算机操作系统向本设备开放 DMA 功能。CY7C68013A 芯片协调控制 TSB43AA82A 对内存数据的读取。

[0018] 在图 2 中，给出了本实用新型的样品图，三个工作指示灯 11 指示目前设备运行的状态。红灯为电源灯，表示设备通电；黄灯为空闲灯，表示设备正常加载，但没有进行数据读写操作；绿灯为运行灯，表示目前设备正在进行读写操作。

[0019] 实用新型专利基于 1394 总线技术和操作系统在特定情况下可开放 DMA 的特点，借助于 I/O 设备的 DMA 数据传输方式、各种操作系统的基本配置和即插即用功能。本实用新型的设备在使用的过程中，USB 接口 1 与取证计算机相连接，1394 接口 2 与目标计算机相连接，通过 DMA 的方式实现对目标计算机物理内存的访问，将所读取的物理内存数据包通过通用 USB 接口 2 发送至取证计算机，在对目标计算机内存改动很小的情况下实现内存数据的获取。

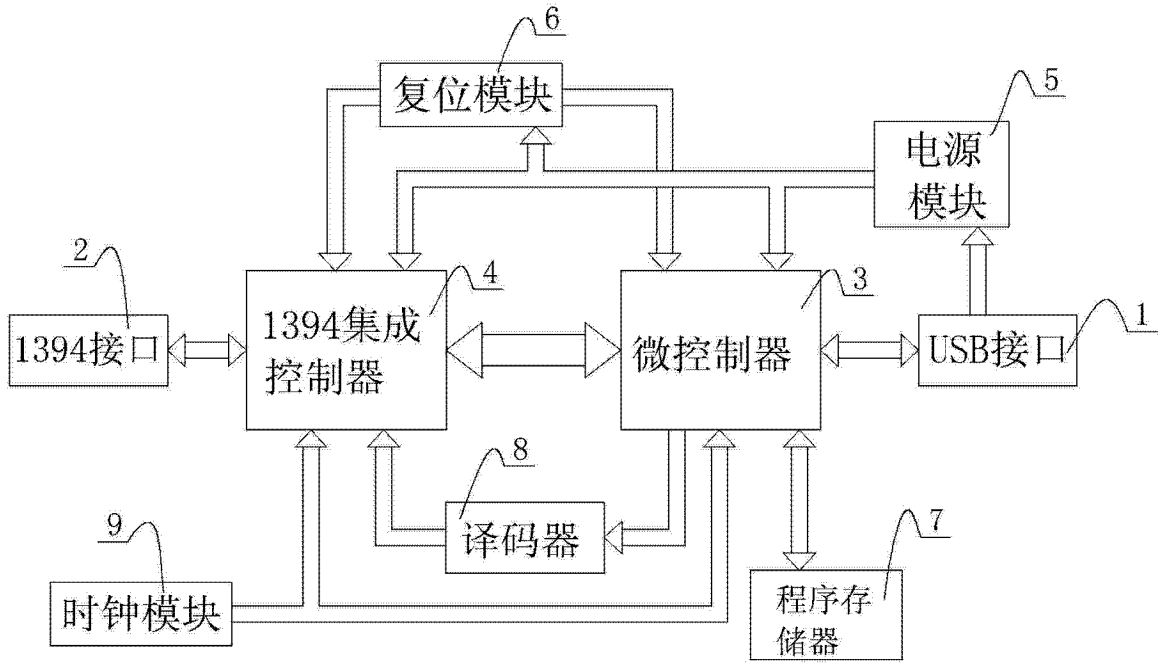

6
复位模块
5
电源
模块
2
1394接口
4
1394集成
控制器
3
微控制器
1
USB接口
8
译码器
9
时钟模块
7
程序存
储器

图 1

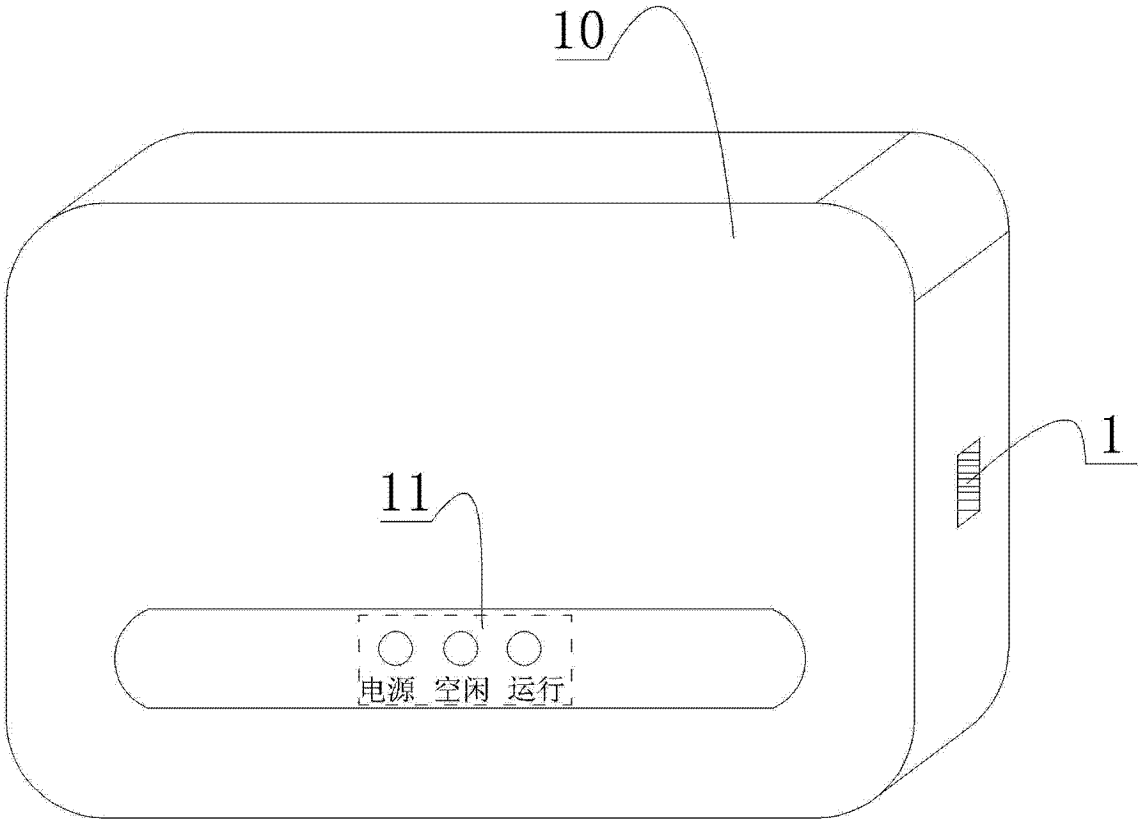

10
1
11
电源 空闲 运行

图 2