

C# 系统应用之通过注册表获取USB使用记录(一)

原创 Eastmount 最后发布于2014-04-08 01:04:05 阅读数 8037 ☆ 收藏

展开



Python+TensorFlow人工智能

该专栏为人工智能入门专栏,采用Python3和TensorFlow实现人工智能相关算法。前期介绍安装流程、基础语法...



Eastmount

¥9.90

去订阅

该文章是“个人电脑历史记录清除软件”项目的系统应用系列文章。

前面已经讲述了如何清除IE浏览器的历史记录、获取Windows最近访问文件记录、清除回收站等功能.现在我需要完成的是删除USB设备上的U盘、手机、移动硬盘等记录,真心觉得这方面资料特别少.这篇文章首先主要讲述了通过注册表获取USB使用记录,希望对大家有所帮助.

一.注册表基本知识

注册表(registry)是Windows系统中一个重要的数据库,它用于存储有关应用程序、用户和系统信息.注册表的结构就像一颗树.树的顶级节点(hive)不能添加、修改和删除.如下图所示是Windows注册表的顶级节点:



- (1).HKEY_CURRENT_USER:包含当前登录到Windows的用户配置信息
- (2).HKEY_USERS:包含计算机所有用户的配置信息
- (3).HKEY_LOCAL_MACHINE:包含与计算机相关的配置信息,不论用户是否登录
- (4).HKEY_CLASSES_ROOT:包含将文件类型同程序关联起来的信息及COM组件配置数据
- (5).HKEY_CURRENT_CONFIG:包含本地计算机启动时所使用的硬件描述文件.

详见[百度百科](#)

二.C#中注册表简单使用

在前面“[C# 系统应用之IE浏览器记录和地址栏输入网址](#)”文章中我已经简单的使用了通过注册表获取地址栏的信息并显示.这里想讲讲注册表常使用的获取内容方法.主要代码如下:

```
// 定义注册表顶级节点 其命名空间是using Microsoft.Win32;
RegistryKey historykey;;
// 检索当前用户CurrentUser子项Software\Microsoft\Internet Explorer\typedURLs
historykey = Registry.CurrentUser.OpenSubKey("Software\Microsoft\Internet Explorer\typedURLs", true);
if (historykey != null)
{
    // 获取检索的所有值
    String[] names = historykey.GetValueNames();
    foreach (String str in names)
    {
        listBox1.Items.Add(historykey.GetValue(str).ToString());
    }
}
```

```
}  
}
```

其中,RegistryKey类(MSDN)表示注册表中的顶级结点,此类是注册表封装.Registry类(MSDN)提供表示Windows注册表中的根项的RegistryKey对象,并提供访问项/值.常用值如下对应的是注册表顶级节点内容.

	名称	说明
	ClassesRoot	定义文档的类型 (或类) 以及与那些类型关联的属性。该字段读取 Windows 注册表基项 HKEY_CLASSES_ROOT。
	CurrentConfig	包含有关非用户特定的硬件的配置信息。该字段读取 Windows 注册表基项 HKEY_CURRENT_CONFIG。
	CurrentUser	包含有关当前用户首选项的信息。该字段读取 Windows 注册表基项 HKEY_CURRENT_USER。
	DynData	已过时。包含动态注册表数据。该字段读取 Windows 注册表基项 HKEY_DYN_DATA。
	LocalMachine	包含本地计算机的配置数据。该字段读取 Windows 注册表基项 HKEY_LOCAL_MACHINE。
	PerformanceData	包含软件组件的性能信息。该字段读取 Windows 注册表基项 HKEY_PERFORMANCE_DATA。
	Users	包含有关默认用户配置的信息。该字段读取 Windows 注册表基项 HKEY_USERS。

上面代码获取IE浏览器地址栏最近输入URL对应的注册表树形路径为:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs

通过Registry.CurrentUser(HKEY_CURRENT_USER)中的OpenSubKey函数检索指定的子项,并指定是否将写访问权限应用于该项.最后通过GetValueNames()获取检索的所有值.函数原型:

```
public RegistryKey OpenSubKey(  
    string name,      //要打开的子项名称或路径  
    bool writable     //如果需要项的写访问权限=true  
)
```

三.注册表如何存储USB信息

此处查阅多处资料并主要引用《计算机信息获取系统的研究与实现》论文部分:

<http://cdmd.cnki.com.cn/Article/CDMD-10431-2010236667.htm>

在Windows系统中,当一个USB移动存储设备插入时,就会在注册表中留下痕迹.当移动设备插入计算机时,即插即用管理器PnP(Plug and Play)接受该事件,并且在USB设备的固件(Firewire information)中查询有关该设备的描述信息(厂商、型号、序列号等).当设备被识别后,在注册表中创建一个新的键值:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

在这个键值下,会看到类似下面的结构子键:(该子键代表设备类标示符,用来标识设备的一个特定类)

Disk&Ven_####&Prod_####&Rev_###

其中子键中"####"代表区域由PnP管理器依据在USB设备描述符中获取的数据填写.如下图所示



Disk&Ven_aigo&Prod_Miniking&Rev_8.07是Device class ID

Q0UKCH37&0是Unique instance ID(UID)

如果使用UVCView工具可以看见USB设备描述内容,其中的信息都是相互对应的.设备类ID一旦建立,就需要建立一个特定唯一的UID.它可以把具有同一设备

类标识的多个存储设备区分.

四.程序实现获取USB使用信息

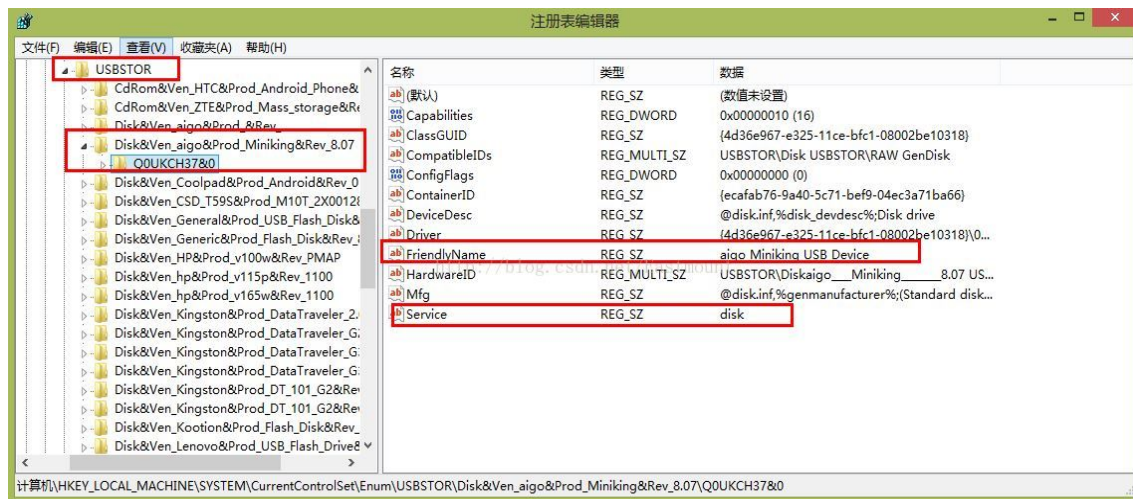
具体代码如下所示,同时希望大家去下载wnt08的代码,很有帮助<http://download.csdn.net/detail/lwnt08/3083499>

```
// 获取USB使用信息
private void button1_Click(object sender, EventArgs e)
{
    // 定义注册表顶级节点 其命名空间是using Microsoft.Win32;
    RegistryKey USBKey;
    // 检索子项
    USBKey = Registry.LocalMachine.OpenSubKey(@"SYSTEM\CurrentControlSet\Enum\USBSTOR", false);
    // 检索所有子项USBSTOR下的字符串数组
    foreach (string sub1 in USBKey.GetSubKeyNames())
    {
        RegistryKey sub1key = USBKey.OpenSubKey(sub1, false);
        foreach (string sub2 in sub1key.GetSubKeyNames())
        {
            try
            {
                // 打开sub1key的子项
                RegistryKey sub2key = sub1key.OpenSubKey(sub2, false);
                // 检索Service=disk(磁盘)值的子项 cdrom(光盘)
                if (sub2key.GetValue("Service", "").Equals("disk"))
                {
                    String Path = "USBSTOR" + "\\" + sub1 + "\\" + sub2;
                    String Name = (string)sub2key.GetValue("FriendlyName", "");
                    richTextBox1.AppendText("USB名称 " + Name + "\r\n");
                    richTextBox1.AppendText("UID标记 " + sub2 + "\r\n");
                    richTextBox1.AppendText("路径信息 " + Path + "\r\n\r\n");
                }
            }
            catch (Exception msg) // 异常处理
            {
                MessageBox.Show(msg.Message);
            }
        }
    }
}
```

运行结果如下图所示:



其中对应的注册表信息如下图所示:



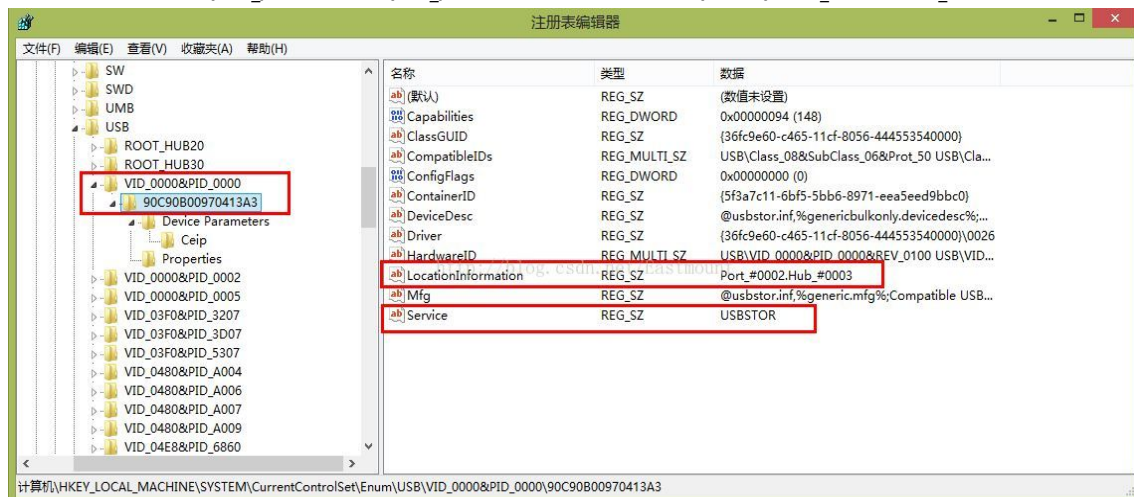
其中对应的FriendlyName即是输出的“USB名称 aigo Miniking USB Device”，UID序号为“Q0UKCH37”。搜索的Service(服务)为disk(磁盘)的选项。

五.总结与展望

首先个人感触,这方面的资料真心很少,文章博客也少,所以看起来操作似乎很简单,但真正实现起来还是令人深思的.然后就是其实存储USB记录的还有很多键值.如

1.HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB

该键值中能看到厂商号(VID_)、厂商产品号(PID_)还有LocationInformation(端口号) Port_#0001.Hub_#0005等.



2.HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses

该键值下有两个设备类: {53F56307-B6BF-11D0-94F2-00A0C91EFB8B}{53F5630d-B6BF-11D0-94F2-00A0C91EFB8B},可以通过他们获取USB最后接入系统时间.

接下来我想要完成的就是如何把这些键值联系起来,似乎要通过Dictionary<string, UInt>,同时怎样获取时间,怎样正确删除这些信息.最后希望文章对大家有所帮助,如果有错误或不足之处,还请海涵!最后感谢下面参考资料的一些文章博客和作者.这类资料真心不好找,都是相关的内容而且不错的,有的引用,有的没有,但都不错,也希望这些链接大家能用到.

(By:Eastmount 2014-4-8 夜1点半 原创CSDN <http://blog.csdn.net/eastmount/>)

参考资料及相似文章(值得一看):

1.《计算机信息获取系统的研究与实现》论文讲述了计算机取证学及USB原理

<http://cdmd.cnki.com.cn/Article/CDMD-10431-2010236667.htm>

2.Tracking USB storage: Analysis of windows artifacts generated by USB storage devices

英文文章,如何获取USB使用记录的时间及信息

<http://www.sciencedirect.com/science/article/pii/S1742287605000320>


3.用C# 编写USB存储设备使用痕迹检测和删除工具 讲述了如何删除获取章节讲解

<http://blog.csdn.net/metaphysis/article/details/18504315>

4.C# 读取注册表获取U盘使用记录
<http://download.csdn.net/detail/lwnt08/3083499>

👍 点赞 4 ☆ 收藏 ➦ 分享 ...



Eastmount  博客专家
发布了450 篇原创文章 · 获赞 6227 · 访问量 496万+

他的留言板

关注