Digital Forensics for the Aspiring Hacker, Part 9 (Finding Storage Device Artifacts in the Registry)

- By **occupytheweb**
- Forensics

Welcome back, my fledgling hackers!

In this series, I am trying to develop your knowledge of digital forensics, which is valuable whether you're choosing a career in it *or* just want to know how your hacker activity can be traced. Few professional digital forensic investigators have a hacking background, but the best ones do.

The occupation of digital forensic investigation is a rapidly growing one. Nearly every crime has a digital component these days. This might include things as innocuous as a text message, a Google search, or an email, and law enforcement and civil litigators need trained professionals to find the necessary information and preserve it in a forensically sound manner.

Finding Storage Device Artifacts in a Windows Registry

As I have mentioned in a previous article in this series, the registry in Windows is how Microsoft manages the operating system. As such, it contains volumes of information on who, what, where, and how activity took place on this system. If we know where and how to look in the registry, we can build a strong case of what actually took place there.

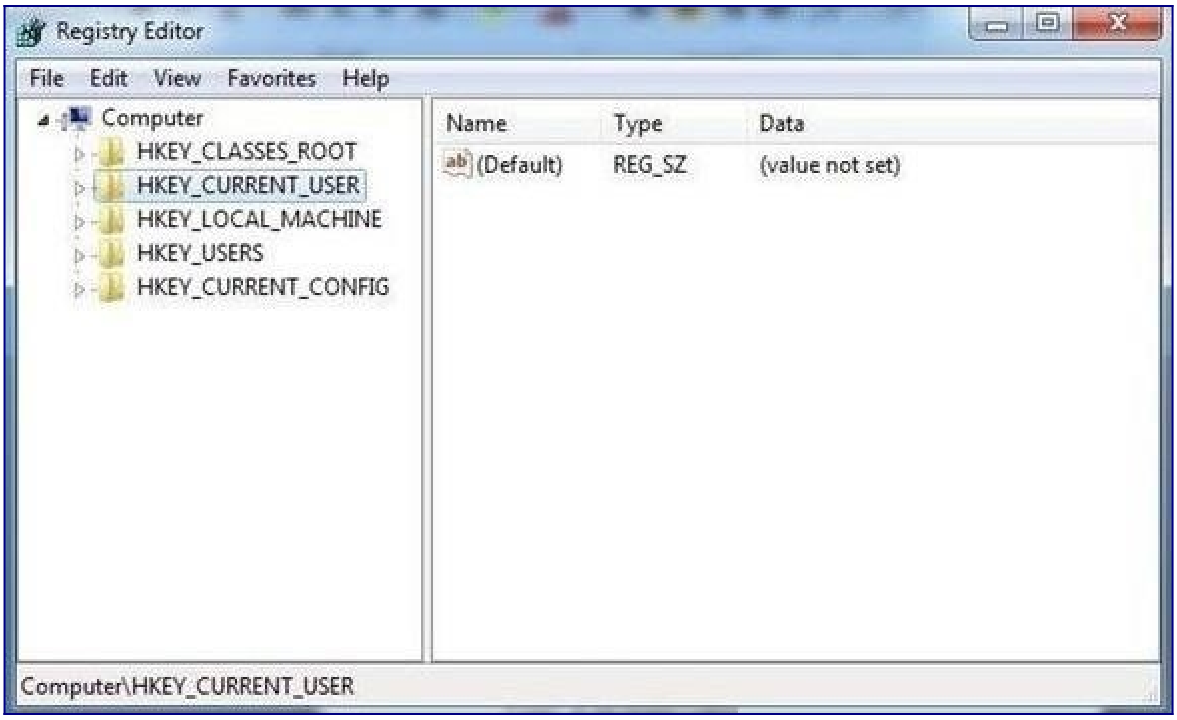
In this tutorial, we will focus on finding evidence of storage devices within the registry. Often, the suspect will use a Flash drive or hard drive for their malicious activities and then remove them so as not to leave any evidence. The skilled forensic investigator, though, can still find traces of evidence of those storage devices within the registry, if they know where to look.

The registry on a Windows system varies a bit from version to version. A skilled, professional digital forensic investigator needs to be able to work with nearly all versions of Windows and other operating systems. Since Windows 7 is still the most widely used operating system, by far, I will be demonstrating on it. Keep in mind, though, that this will vary slightly between versions.

Step 1Open Regedit

Although a forensic investigator will usually be working on an image file and using a forensic suite, we can clearly demonstrate the principals and locations by using regedit on a live system. In some forensic investigations, you might actually have the need or luxury of working on a live system, but it is rare. Usually, you will be using an image, but the registry remains the same whether live or image.

To open the Registry Editor, type "regedit" at the command prompt. When you do so, it will open the Registry Editor as seen below.



Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG

Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_CURRENT_USER

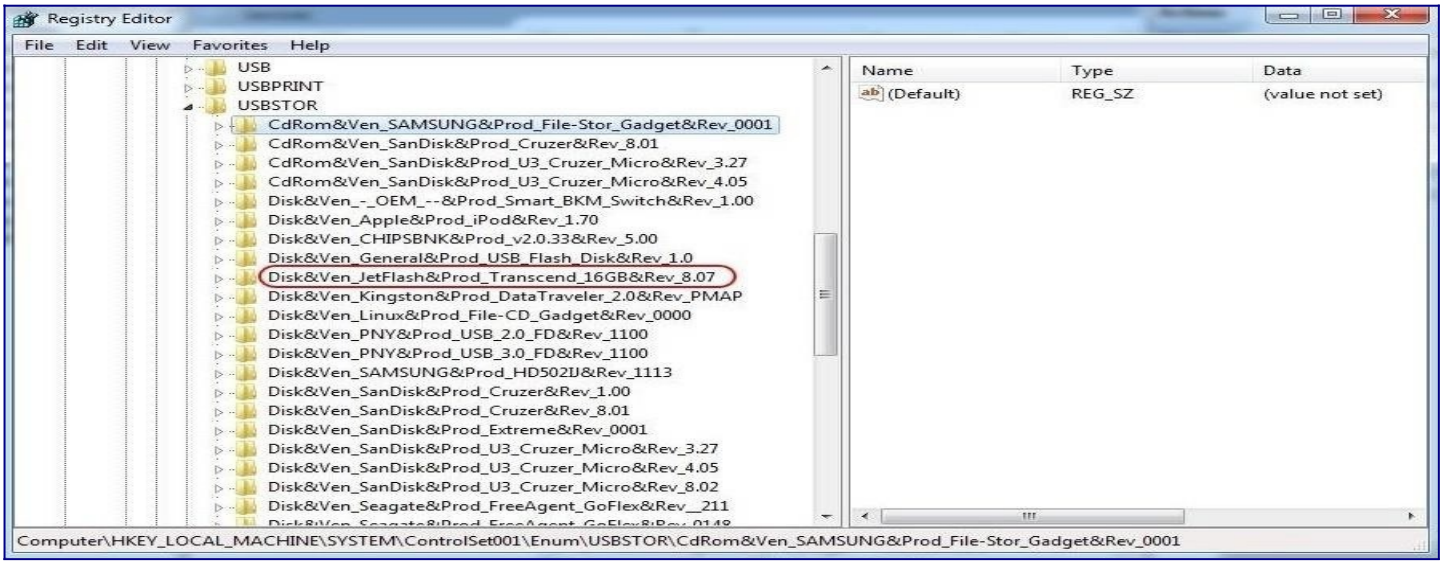
As you remember from a previous tutorial, the registry has five hives.

Step 2USB Storage Devices

Imagine a case where we suspect that someone installed a keylogger or removed confidential information with a USB drive. How would we find evidence that a USB storage device was inserted and used? To find evidence of USB storage devices, we want to look at the following key.

HK_Local_Machine\System\ControlSet00x\Enum\USBSTOR

In this key, we will find evidence of *any* USB storage device that has *ever* been connected to this system. Expand USBSTOR to see a listing of every USB storage device ever connected to this system.

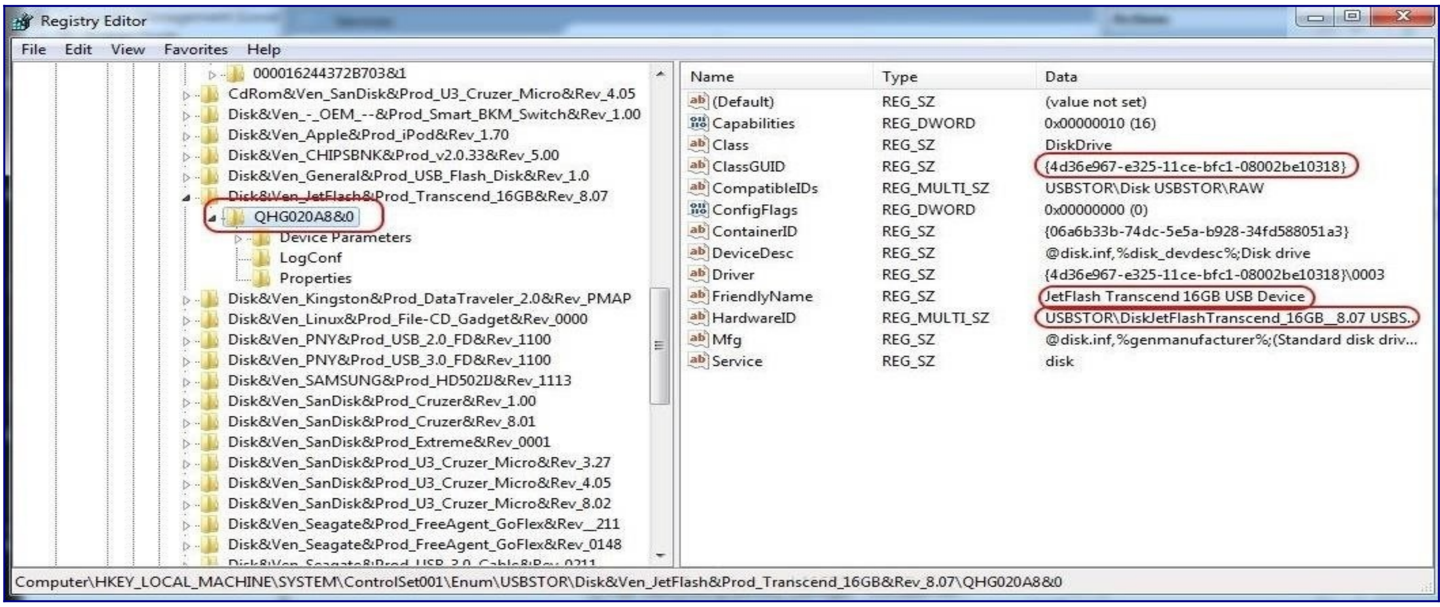


USB
USBPRINT
USBSTOR
CdRom&Ven_SAMSUNG&Prod_File-Stor_Gadget&Rev_0001
CdRom&Ven_SanDisk&Prod_Cruzer&Rev_8.01
CdRom&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_3.27
CdRom&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_4.05
Disk&Ven_-_OEM_--&Prod_Smart_BKM_Switch&Rev_1.00
Disk&Ven_Apple&Prod_iPod&Rev_1.70
Disk&Ven_CHIPSBNK&Prod_v2.0.33&Rev_5.00
Disk&Ven_General&Prod_USB_Flash_Disk&Rev_1.0
Disk&Ven_JetFlash&Prod_Transcend_16GB&Rev_8.07
Disk&Ven_Kingston&Prod_DataTraveler_2.0&Rev_PMAP
Disk&Ven_Linux&Prod_File-CD_Gadget&Rev_0000
Disk&Ven_PNY&Prod_USB_2.0_FD&Rev_1100
Disk&Ven_PNY&Prod_USB_3.0_FD&Rev_1100
Disk&Ven_SAMSUNG&Prod_HD502IJ&Rev_1113
Disk&Ven_SanDisk&Prod_Cruzer&Rev_1.00
Disk&Ven_SanDisk&Prod_Cruzer&Rev_8.01
Disk&Ven_SanDisk&Prod_Extreme&Rev_0001
Disk&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_3.27
Disk&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_4.05
Disk&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_8.02
Disk&Ven_Seagate&Prod_FreeAgent_GoFlex&Rev__211
Disk&Ven_Seagate&Prod_FreeAgent_GoFlex&Rev_0148

Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\CdRom&Ven_SAMSUNG&Prod_File-Stor_Gadget&Rev_0001

In the screenshot above, I have circled one suspicious looking USB device. When we expand it, it reveals a unique identifier for that device. By clicking on this identifier, we can find much more information about the device.



```
  000016244372B703&1
CdRom&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_4.05
Disk&Ven_-_OEM_--&Prod_Smart_BKM_Switch&Rev_1.00
Disk&Ven_Apple&Prod_iPod&Rev_1.70
Disk&Ven_CHIPSBNK&Prod_v2.0.33&Rev_5.00
Disk&Ven_General&Prod_USB_Flash_Disk&Rev_1.0
Disk&Ven_JetFlash&Prod_Transcend_16GB&Rev_8.07
  QHG020A8&0
    Device Parameters
    LogConf
    Properties
Disk&Ven_Kingston&Prod_DataTraveler_2.0&Rev_PMAP
Disk&Ven_Linux&Prod_File-CD_Gadget&Rev_0000
Disk&Ven_PNY&Prod_USB_2.0_FD&Rev_1100
Disk&Ven_PNY&Prod_USB_3.0_FD&Rev_1100
Disk&Ven_SAMSUNG&Prod_HD502IJ&Rev_1113
Disk&Ven_SanDisk&Prod_Cruzer&Rev_1.00
Disk&Ven_SanDisk&Prod_Cruzer&Rev_8.01
Disk&Ven_SanDisk&Prod_Extreme&Rev_0001
Disk&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_3.27
Disk&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_4.05
Disk&Ven_SanDisk&Prod_U3_Cruzer_Micro&Rev_8.02
Disk&Ven_Seagate&Prod_FreeAgent_GoFlex&Rev__211
Disk&Ven_Seagate&Prod_FreeAgent_GoFlex&Rev_0148
Disk&Ven_Seagate&Prod_USB_3.0_Cable&Rev_0211
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
Capabilities	REG_DWORD	0x00000010 (16)
Class	REG_SZ	DiskDrive
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ConfigFlags	REG_DWORD	0x00000000 (0)
ContainerID	REG_SZ	{06a6b33b-74dc-5e5a-b928-34fd588051a3}
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0003
FriendlyName	REG_SZ	JetFlash Transcend 16GB USB Device
HardwareID	REG_MULTI_SZ	USBSTOR\DiskJetFlashTranscend_16GB__8.07 USBS...
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk driv...
Service	REG_SZ	disk

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_JetFlash&Prod_Transcend_16GB&Rev_8.07\QHG020A8&0

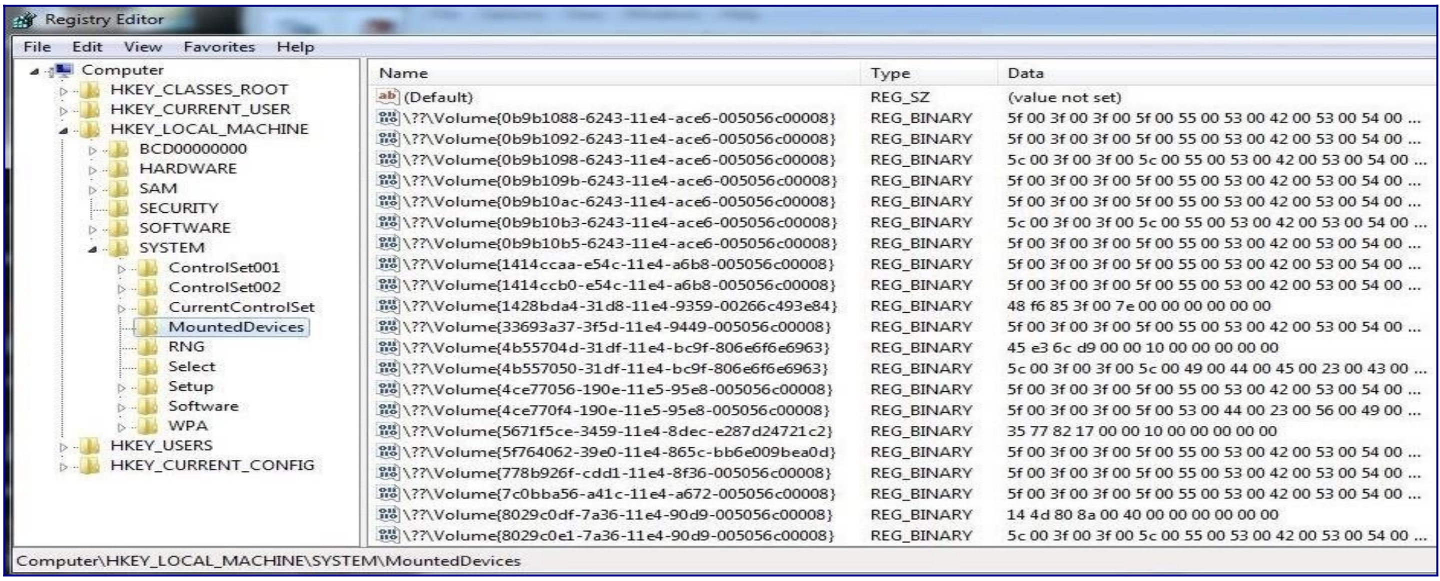
As you can see in the screenshot above, when we click on the USB storage identifier, it reveals in the right-hand window the Global Unique Identifier (GUID), the friendly name, and the hardware ID, among other things. This may be exactly the evidence we need to tie the suspect to their activity on this system!

Step 3Mounted Devices

If the suspect used any hardware device that must be mounted to either read or write data (CD-ROM, DVD, hard drive, flash drive, etc.), the registry will record the mounted device. This information is stored at:

HKEY_LOCAL_MACHINE\System\MountedDevices

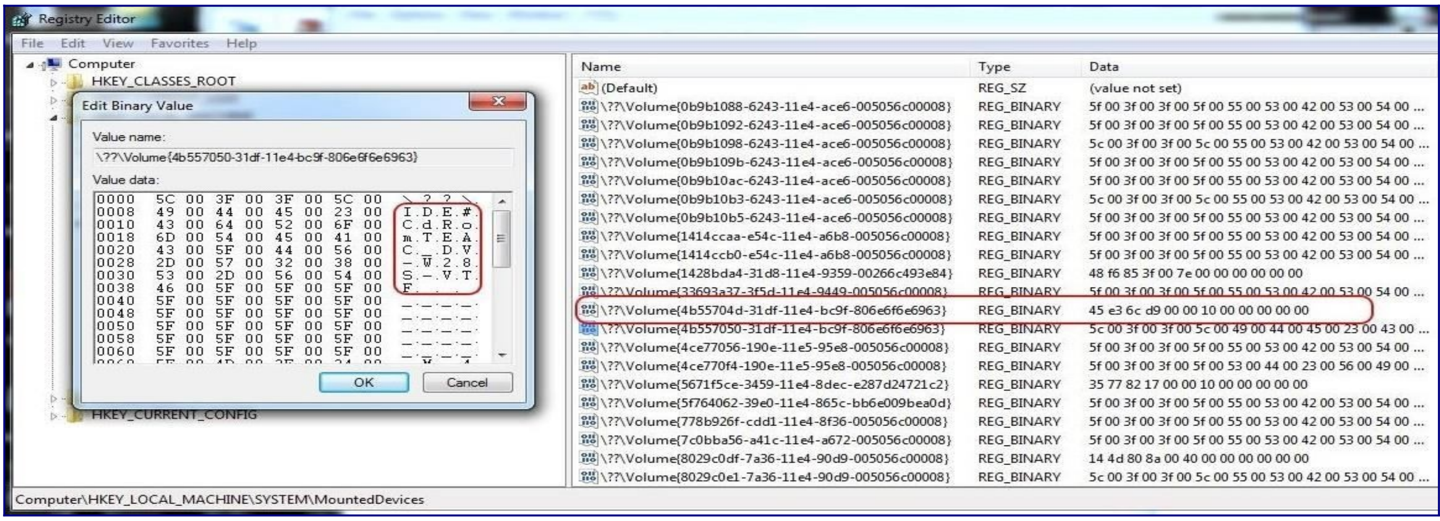
As you can see below, when we click on this key, it provides us a long list of every device ever mounted on that machine.



Name	Type	Data
(Default)	REG_SZ	(value not set)
\??\Volume{0b9b1088-6243-11e4-ace6-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{0b9b1092-6243-11e4-ace6-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{0b9b1098-6243-11e4-ace6-005056c00008}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{0b9b109b-6243-11e4-ace6-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{0b9b10ac-6243-11e4-ace6-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{0b9b10b3-6243-11e4-ace6-005056c00008}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{0b9b10b5-6243-11e4-ace6-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{1414ccaa-e54c-11e4-a6b8-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{1414ccb0-e54c-11e4-a6b8-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{1428bda4-31d8-11e4-9359-00266c493e84}	REG_BINARY	48 f6 85 3f 00 7e 00 00 00 00 00 00
\??\Volume{33693a37-3f5d-11e4-9449-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{4b55704d-31df-11e4-bc9f-806e6f6e6963}	REG_BINARY	45 e3 6c d9 00 00 10 00 00 00 00 00
\??\Volume{4b557050-31df-11e4-bc9f-806e6f6e6963}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 ...
\??\Volume{4ce77056-190e-11e5-95e8-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{4ce770f4-190e-11e5-95e8-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 53 00 44 00 23 00 56 00 49 00 ...
\??\Volume{5671f5ce-3459-11e4-8dec-e287d24721c2}	REG_BINARY	35 77 82 17 00 00 10 00 00 00 00 00
\??\Volume{5f764062-39e0-11e4-865c-bb6e009bea0d}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{778b926f-cdd1-11e4-8f36-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{7c0bba56-a41c-11e4-a672-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{8029c0df-7a36-11e4-90d9-005056c00008}	REG_BINARY	14 4d 80 8a 00 40 00 00 00 00 00 00
\??\Volume{8029c0e1-7a36-11e4-90d9-005056c00008}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 55 00 53 00 42 00 53 00 54 00 ...

Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

If we need further information on any of those mounted devices, we can simply click on it, and it will open a small app that will enable us to read the data in ASCII. As you can see, this device was an IDE CD-ROM manufactured by Teac.



Value name:

\??\Volume{4b557050-31df-11e4-bc9f-806e6f6e6963}

Value data:

```
0000   5C  00  3F  00  3F  00  5C  00   \.?.?.\.
0008   49  00  44  00  45  00  23  00   I.D.E.#.
0010   43  00  64  00  52  00  6F  00   C.d.R.o.
0018   6D  00  54  00  45  00  41  00   m.T.E.A.
0020   43  00  5F  00  44  00  56  00   C._.D.V.
0028   2D  00  57  00  32  00  38  00   -.W.2.8.
0030   53  00  2D  00  56  00  54  00   S.-.V.T.
0038   46  00  5F  00  5F  00  5F  00   F._._._.
0040   5F  00  5F  00  5F  00  5F  00   _._._._.
0048   5F  00  5F  00  5F  00  5F  00   _._._._.
0050   5F  00  5F  00  5F  00  5F  00   _._._._.
0058   5F  00  5F  00  5F  00  5F  00   _._._._.
0060   5F  00  5F  00  5F  00  5F  00   _._._._.
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
\??\Volume{0b9b1088-6243-11e4-ace6-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{0b9b1092-6243-11e4-ace6-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{0b9b1098-6243-11e4-ace6-005056c00008}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{0b9b109b-6243-11e4-ace6-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{0b9b10ac-6243-11e4-ace6-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{0b9b10b3-6243-11e4-ace6-005056c00008}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{0b9b10b5-6243-11e4-ace6-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{1414ccaa-e54c-11e4-a6b8-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{1414ccb0-e54c-11e4-a6b8-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{1428bda4-31d8-11e4-9359-00266c493e84}	REG_BINARY	48 f6 85 3f 00 7e 00 00 00 00 00 00
\??\Volume{33693a37-3f5d-11e4-9449-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{4b55704d-31df-11e4-bc9f-806e6f6e6963}	REG_BINARY	45 e3 6c d9 00 00 10 00 00 00 00 00
\??\Volume{4b557050-31df-11e4-bc9f-806e6f6e6963}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 49 00 44 00 45 00 23 00 43 00 ...
\??\Volume{4ce77056-190e-11e5-95e8-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{4ce770f4-190e-11e5-95e8-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 53 00 44 00 23 00 56 00 49 00 ...
\??\Volume{5671f5ce-3459-11e4-8dec-e287d24721c2}	REG_BINARY	35 77 82 17 00 00 10 00 00 00 00 00
\??\Volume{5f764062-39e0-11e4-865c-bb6e009bea0d}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{778b926f-cdd1-11e4-8f36-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{7c0bba56-a41c-11e4-a672-005056c00008}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{8029c0df-7a36-11e4-90d9-005056c00008}	REG_BINARY	14 4d 80 8a 00 40 00 00 00 00 00 00
\??\Volume{8029c0e1-7a36-11e4-90d9-005056c00008}	REG_BINARY	5c 00 3f 00 3f 00 5c 00 55 00 53 00 42 00 53 00 54 00 ...

Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

If there is not a TEAC CD_ROM on the system, the forensic investigator now knows that they need to find this piece of hardware to find further evidence of the crime.

The registry is a depository of volumes of information on what happened on a Windows system, and by learning our way around it, we can reconstruct the elements of a crime that it was used for.

Keep coming back, my aspiring forensic investigators, as we explore more ways to find evidence of criminal or malicious activity.