CAL POLY

California Cybersecurity Institute

Computer Forensics CCIC Training

Chapter 8: External Storage Devices

Lauren Pixley, Cassidy Elwell, and James Poirier

May 2019 (Version 2)

8

External Storage Devices

Introduction

When you looked at Craig's link files and jump lists, some of the data was pointing to an E: drive, which was a removable disk. These link files pointed back to potential fraudulent coupons and CP. Now that you are aware of the suspect's external E: drive, you need to know more about it. It is also important for you to learn more about USB devices and what information is stored when they are plugged into a computer.

USB devices are designed under USB Bus specifications, which describe the design and technical details for manufacturing them. From a forensics viewpoint, there are a couple of technical details under the Standard USB Descriptors Definitions that help to identify a specific USB device. Each USB device contains information that is embedded at the time of manufacturing.

You can use a freeware tool, such as Microsoft's Universal Serial Bus Viewer (USBView) to read the information. USBView can list USB host controllers, USB hubs, and attached USB devices. The following information for a SanDisk, U3 Cruzer Micro, 2GB thumb drive was extracted using USBView:

```
===>Device Descriptor<===

bLength:                  0x12
bDescriptorType:          0x01
bcdUSB:                   0x0200
bDeviceClass:             0x00->This is an Interface Class Defined Device
bDeviceSubClass:          0x00
bDeviceProtocol:          0x00
bMaxPacketSize0:          0x40 = (64) Bytes
idVendor:                 0x0781 = SanDisk Corporation
idProduct:                0x5406
bcdDevice:                0x0200
iManufacturer:            0x01
English (United States)   "SanDisk"
iProduct:                 0x02
English (United States)   "U3 Cruzer Micro"
iSerialNumber:       0x03
English (United States)   "43174013F2C14667"
bNumConfigurations:       0x01
```


The key fields of information that can be relevant to a forensic investigation are:

Vendor ID (idVendor)

Product ID (idProduct)

Manufacturer (iManufacturer)

Product (iProduct)

Serial Number (iSerialNumber)

Since I physically possessed the device, I could confirm the accuracy of the information listed by USBView. I could see that the device was in fact a SanDisk U3 Cruzer Micro. However, the serial number was not stamped on the exterior of the device. You should also be aware that while some devices may have a serial number that is visible, it may not match the serial number that is embedded in the USB circuit board.

No matter what serial number is stamped on the exterior, you will always want to check the internal serial number, which is also called the iSerialNumber.

The Vendor ID, which is 2 bytes in length, is assigned by the USB Implementers Forum, Inc. Each vendor is assigned a unique ID.

The Product ID is also 2 bytes in length, but it is randomly assigned by the manufacturer. A good reference for Vendor and Product ID's can be found at the following website:

`http://www.linux-usb.org/usb.ids`

Although the information on this website shouldn't be considered authoritative, since it's submitted by individuals, it is a good starting point to look up information that may match the Product ID.

Another freeware tool that can be used to read a USB device is USBDeview, which can be downloaded from:

`http://www.nirsoft.net`

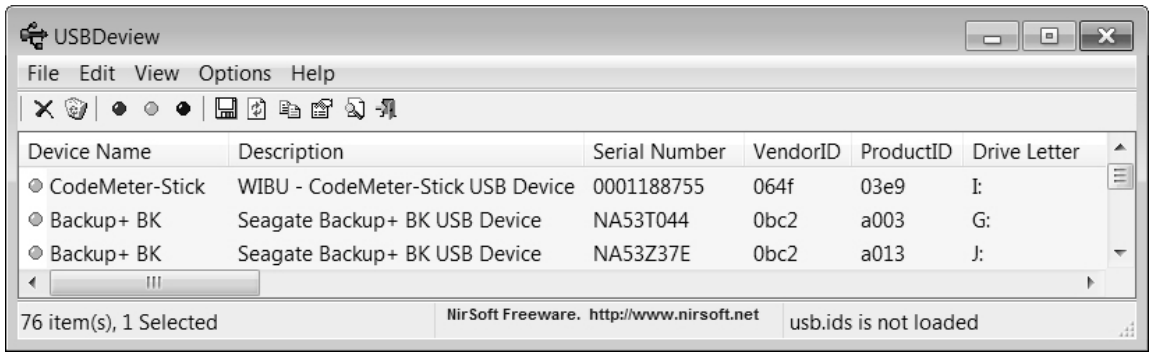

Figure 8-1 – USBDeview

Windows Plug and Play

Now that you know what information is embedded in a USB device, you need to understand what happens when a USB device is plugged into a Windows-based computer.

The plug and play manager extracts information from the USB device when it is first plugged into a Windows computer. As you can see in Figure 8-2, it records that information in several locations.

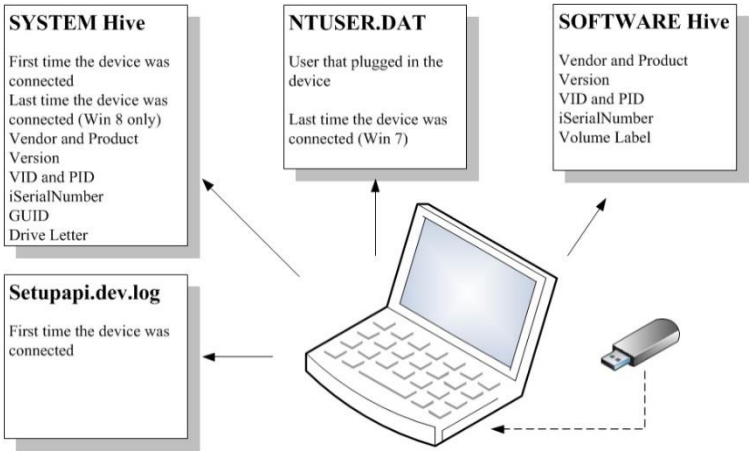

Figure 8-2 - Information Recorded when USB is Connected

Autopsy Devices Attached

When you ran modules earlier on Autopsy, it pulled different information from the registry, including devices connected.

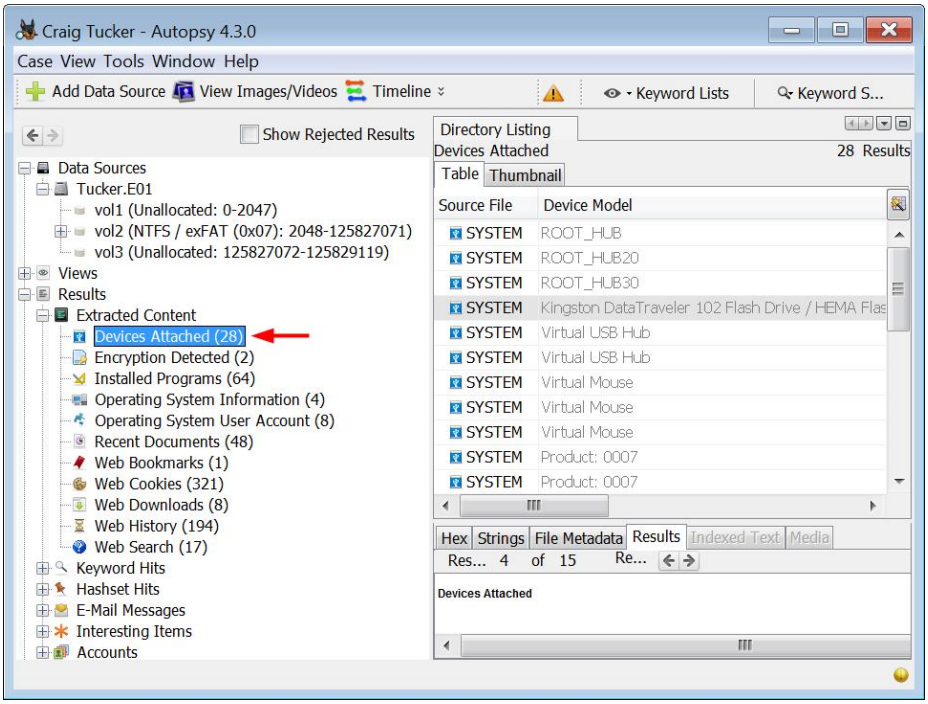

Figure 8-3 – Devices Attached Information Autopsy Retrieved After Running Module

While this information can be useful at face value, it does not really give much detail on the devices actually connected. There are also entries that are not related to external drives that were physically connected, which is not useful to the investigation at the moment. You are going to extract the four key files that store USB information (SYSTEM, SOFTWARE, NTUSER.DAT, and setupapi.dev.log) and then use another tool to find more detailed information.

SYSTEM Hive

Throughout these next sections, you can use the Windows 8 USB Worksheet in the Appendix to follow along with the useful information you want to find for connected USBs.

When a USB device is first connected, it stores the following information in the SYSTEM hive:

Vendor

Product

Version

VID and PID

iSerialNumber

GUID

Drive letter of the USB

Open the SYSTEM hive in Registry Explorer and navigate to the following subkey:

`[CurrentControlSet]\Enum\USBSTOR`

Note: As you may remember from earlier, the Select subkey showed you that the current control set was 1. In this case, it is also the only control set in this SYSTEM hive.

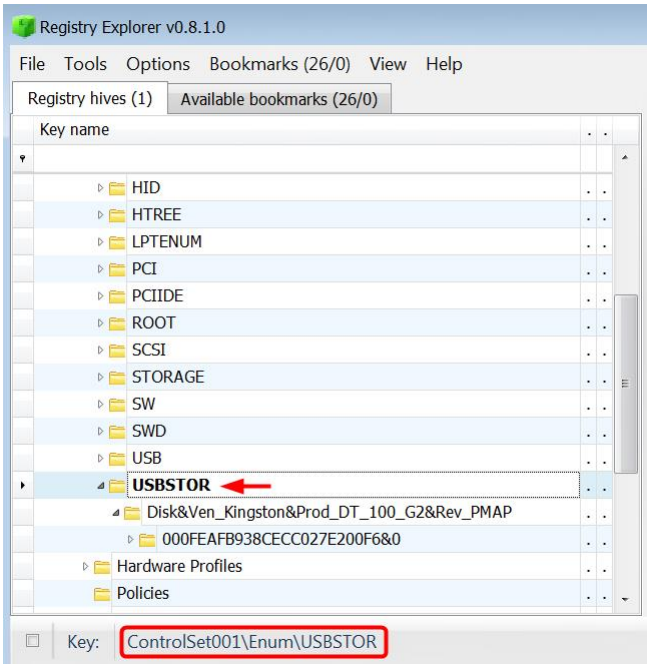

Figure 8-4 - USBSTOR Subkey in SYSTEM Hive

You will see a subkey under USBSTOR which has a name with the following information:

Vendor (Ven):	Kingston
Product (Prod):	DT_100_G2
Version (Rev):	PMAP

✔**Checkpoint:** Write Vendor, Product, and Version in Section 1 on your USB worksheet.

Below this subkey is another subkey named after the iSerialNumber "000FEAFB938CECC027E200F6&0", which Microsoft calls the Instance ID. By omitting the suffix (&#), you can see the iSerialNumber.

Note: The (&#) suffix shows what port the USB device was connected to.

✔**Checkpoint:** Write the iSerialNumber in Section 2 on your USB worksheet.

Open up the iSerialNumber subkey and go to the following location:

```
Properties\{83da6326-97a6-4088-9453-a1923f573b29}
```

As you can see in Figure 8-5, this subkey contains six subkeys. Four of the subkeys, 0064, 0065, 0066, and 0067, have important time stamps. The subkey 0064 shows the date and time when the device's driver was first installed. The subkey 0065 shows when the device's driver was installed. 0064 and 0065 will typically be the same date and time.

The subkeys 0066 and 0067 are new to Windows 8. 0066 shows when the device was last connected and 0067 shows when the device was last removed.

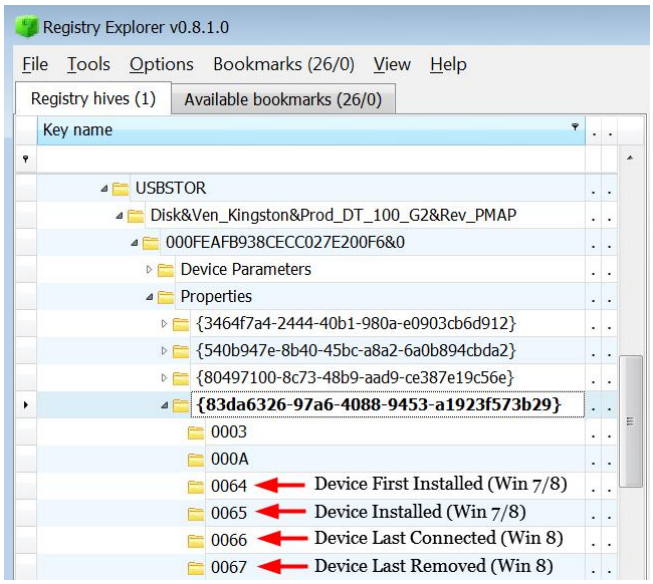

Figure 8-5 - Date and Time Stamps for USB Device

✔**Checkpoint:** Write the first time connected, last time connected, and last time removed in Sections 3, 4, and 5 on your USB worksheet.

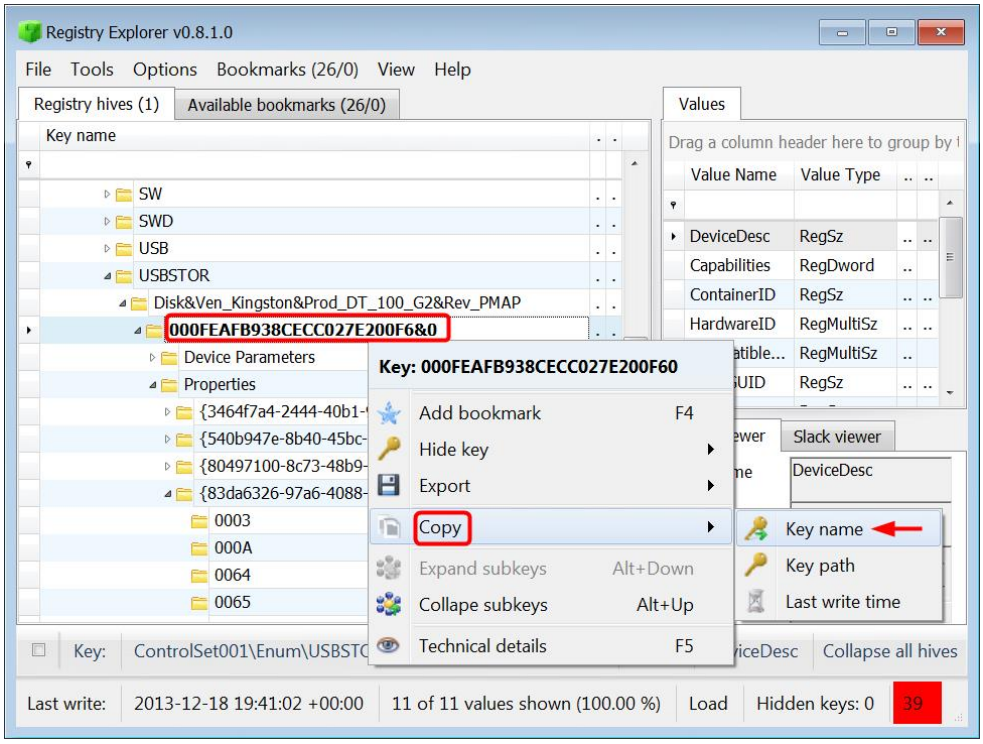

Figure 8-6 – Right-Click iSerialNumber Subkey and Select Copy Key Name

Press Control+F or click on Tools►Find to conduct a search. When the Find window opens, paste the iSerialNumber into the Search For field. Delete the &0 at the end of the iSerialNumber. Check Key Name, Value Data, and Value Name. Leave Value Slack unchecked and then click Search.

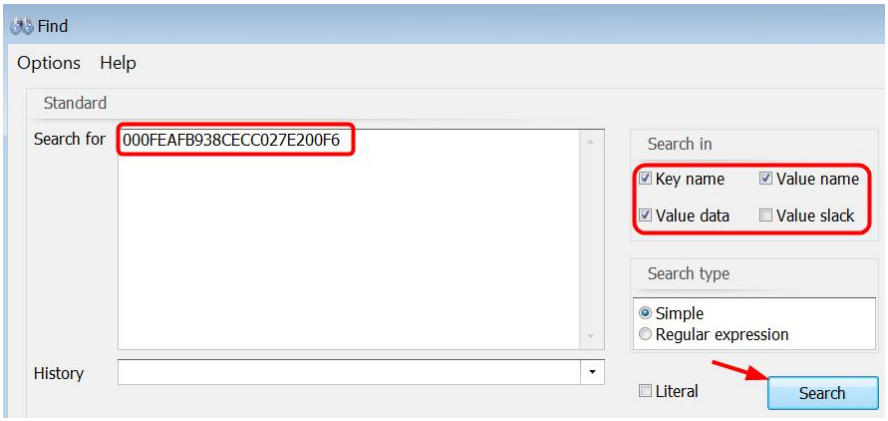

Figure 8-7 – Paste iSerialNumber, Check Key Name/Value Name/Value Data, Click Search

Down in the results pane, you want to look in the Key Path column for a hit under the USB subkey and the Mounted Devices subkey.

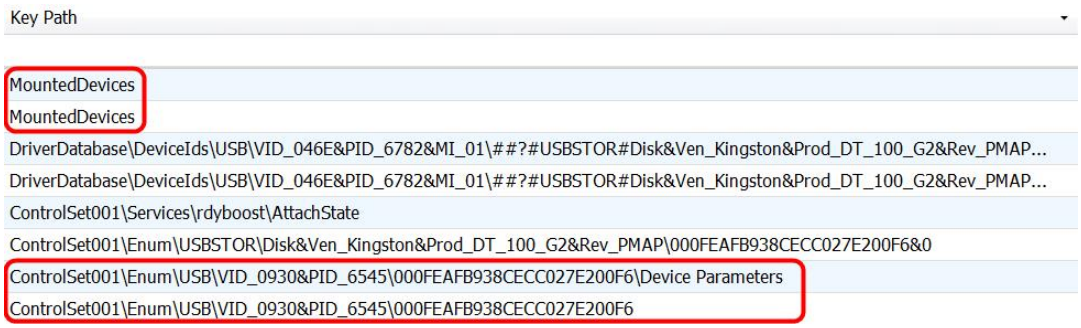

Figure 8-8 – Search Result in MountedDevices and USB Subkeys

First, the iSerialNumber for the connected Kingston device is under the USB subkey. The iSerialNumber has a parent subkey named with the Vendor ID (VID) and the Product ID (PID), which in this case is "VID_0930&PID_6545".

✔**Checkpoint:** Write the VID and PID in Section 6 on your USB worksheet.

Close out of the Find window and navigate to the MountedDevices subkey. Take a look at the different values in the MountedDevices subkey. There are two types of values here. There are some values with names of GUIDs and some values with drive letter names. The value named "Volume{16d5eeec-681c-11e3-824f-000c29d6ef92}" contains information on the Kingston USB. A GUID is a 16-byte value that is randomly generated. Since the value consists of 128 bits, it is unlikely that a randomly generated GUID will match another GUID.

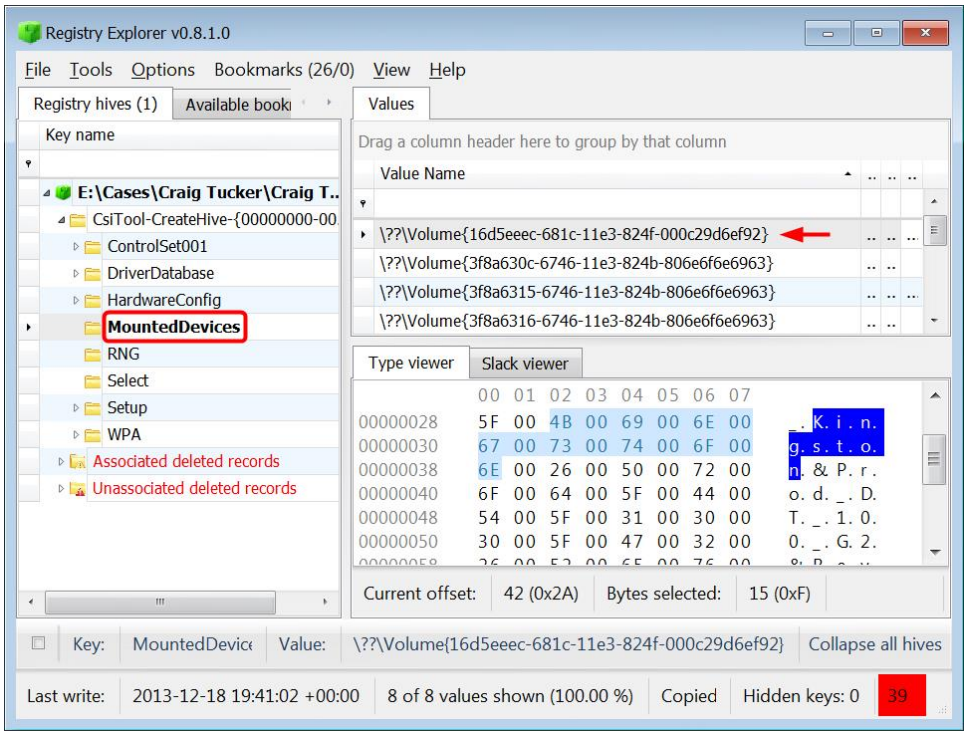

Figure 8-9 – Kingston UBS Information in GUID Value

✔**Checkpoint:** Write the GUID in Sections 7 on your USB worksheet.

Next take a look at the drive letter values. If you look at the value “DosDevices\E:”, you will see Kingston USB information in it. This device’s drive letter is E. If the drive letter had been assigned to another drive that was attached at a later date, the drive letter information would be overwritten with the new device’s serial number.

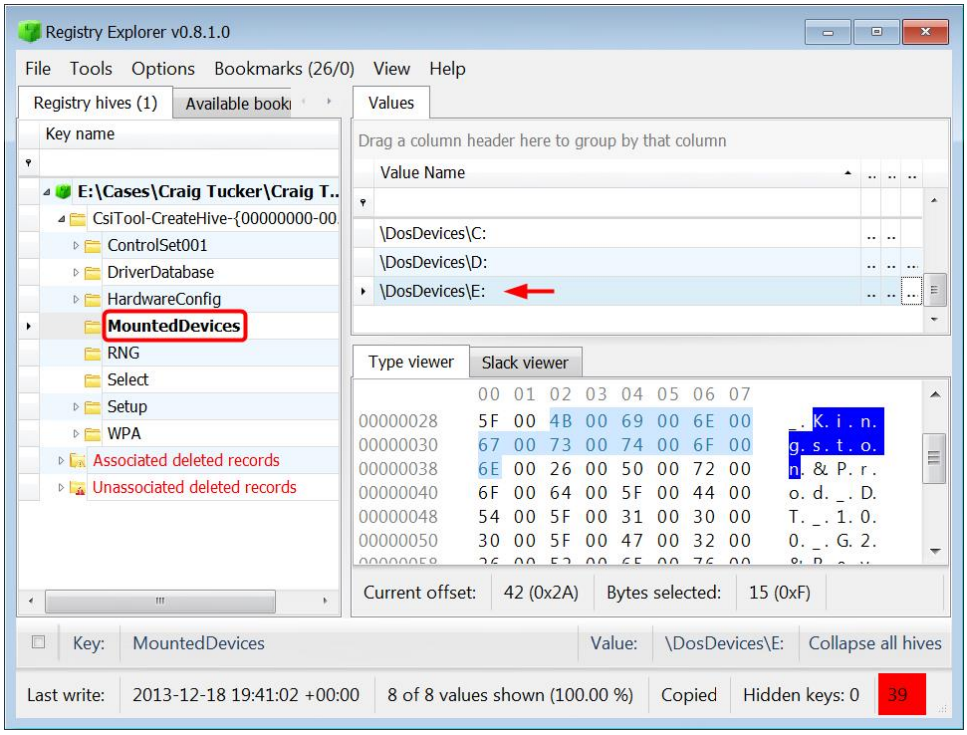

Figure 8-10 – Kingston USB Information in E: Drive Letter Value

✓**Checkpoint:** Write the Drive Letter in Section 8 on your USB worksheet.

SOFTWARE Hive

When a USB device is connected, it stores similar information in the SOFTWARE hive. However, one important piece of information that is only in the SOFTWARE hive is the Volume Label. Open the SOFTWARE hive with Registry Explorer and navigate to the following subkey:

```
Microsoft\Windows Portable Devices\Devices
```

There is only one subkey below Devices, since only one device was connected. The subkey name will contain the same information you found in the SYSTEM hive, except it doesn't have the GUID and drive letter. The subkey will also have a value name called "FriendlyName". The value data of FriendlyName contains the Volume Label, which is "Stuff".

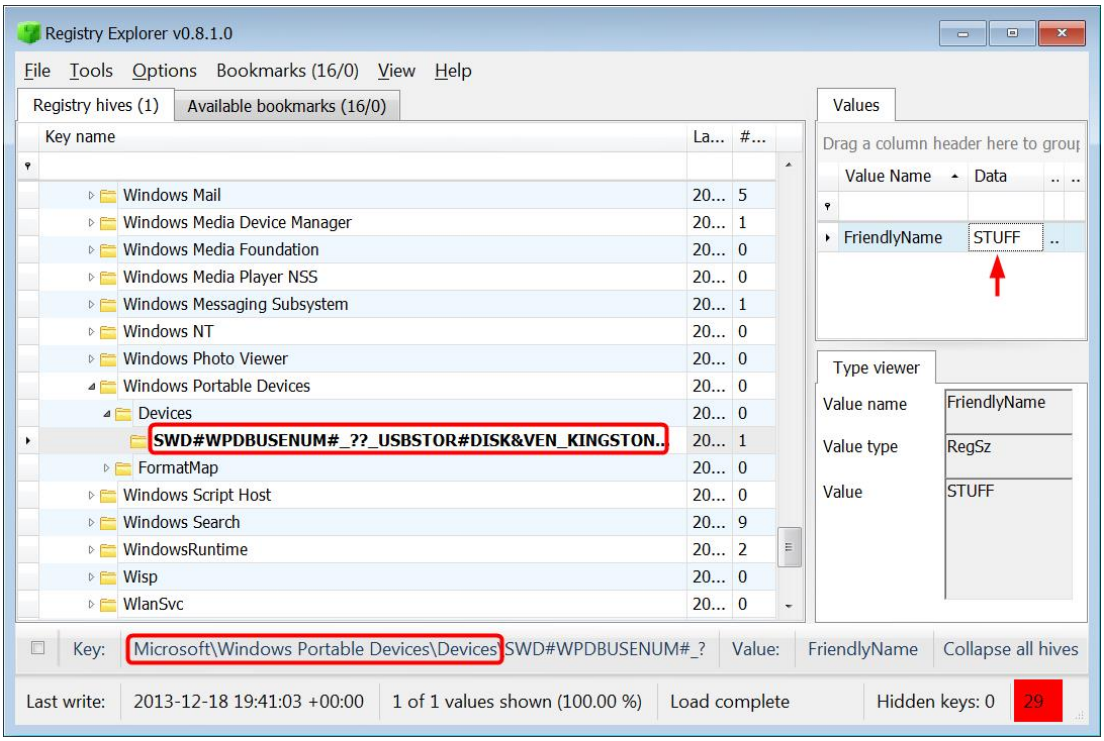

Figure 8-11 - Volume Label in SOFTWARE Hive

✔**Checkpoint:** Write the Volume Label in Section 9 on your USB worksheet.

If you remember from the Recent Files section, a link file stores the volume label and volume serial number where the file was located.

The volume serial number is created when the device is formatted. The way it is calculated is based on the date and time of when the device was formatted, which means that the chance of two devices having the same volume serial number is very unlikely.

A device's volume label can be changed at any time, but the volume serial number can only be changed if the device is reformatted.

NTUSER.DAT

If the computer contained multiple user accounts, you would want to know which user plugged in the device. The user profile hive (NTUSER.DAT) will show you if that user account was specifically associated with that USB device. It will also show you the last time the device was plugged in by that user.

Open Craig's NTUSER.DAT file in Registry Explorer and conduct a search in the NTUSER.DAT file for the first part of the device's GUID (16d5eeec) that you obtained earlier. Only have Key Name checked and then click Search.

Note: Make sure you remove other hives from Registry Explorer before conducting a search so your results will only come from the NTUSER.DAT file.

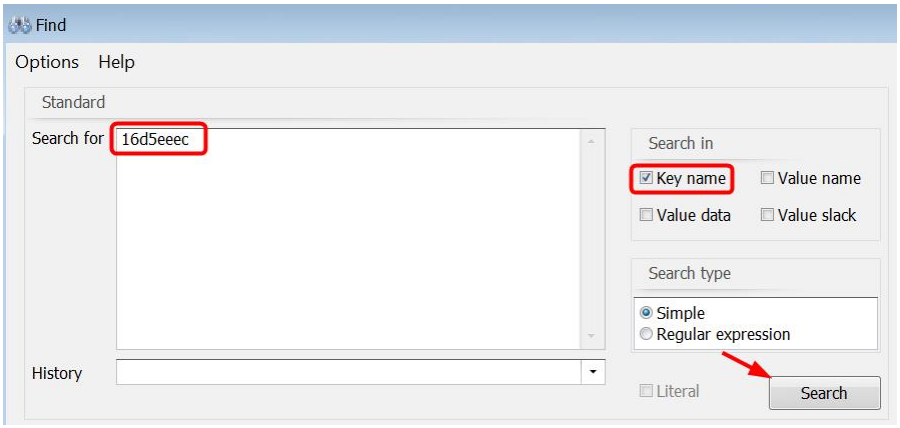

Figure 8-12 – Search for First Part of GUID in Craig's NTUSER.DAT File and Click Search

You should see a result in the following subkey:

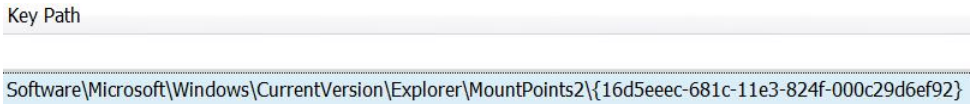

Figure 8-13 – Search Result of Kingston USB GUID

Since the device's GUID is located in Craig's NTUSER.DAT under the MountPoints2 subkey, you know that he was the user that plugged in the device.

✔**Checkpoint:** Write the user that connected the device in Section 10 on your USB worksheet.

Note: Since you do not have the subkeys 0066 and 0067 in the SYSTEM hive for Windows 7 machines, you could look at these Key Properties to determine the last time the device was connected. However, you would not know the last time the device was removed.

Setupapi.dev.log

When a USB device is first connected, it also stores information in the "setupapi.dev.log" file. You already know the first time the device was connected from the SYSTEM hive, but this is another file that will show you the first time the USB device was connected. It is located in:

```
C:\Windows\inf
```

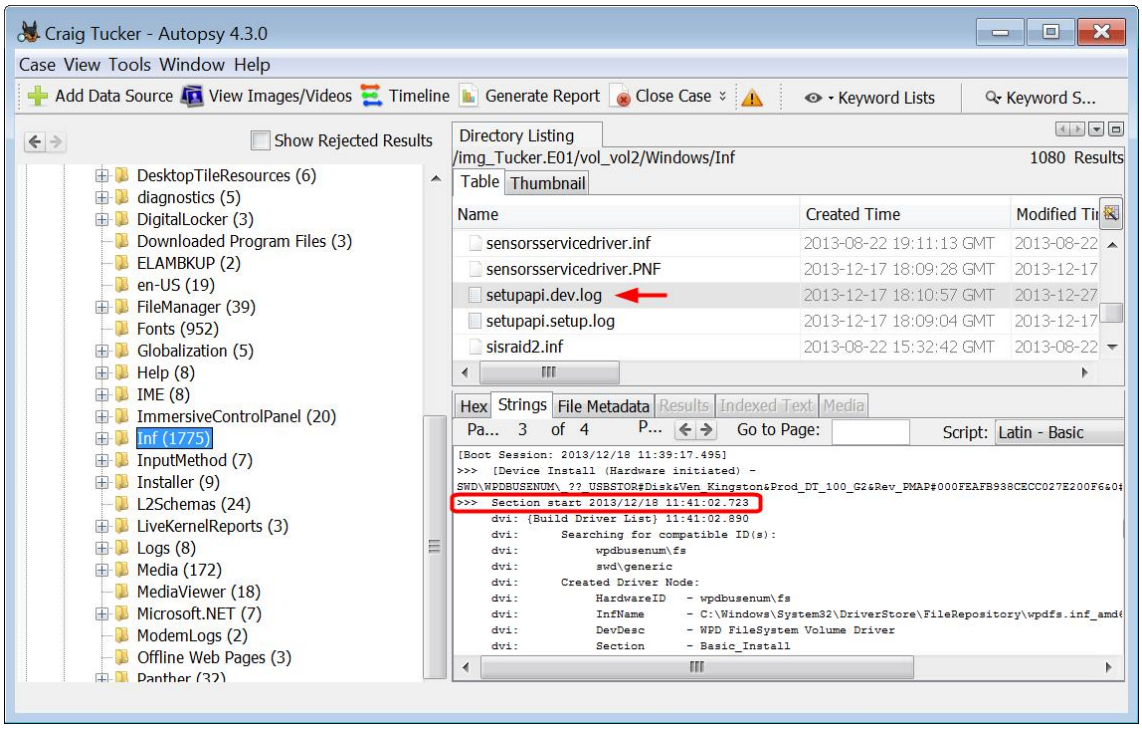

Figure 8-14 – Setupapi.dev.log File

If you click through the pages of the setupapi.dev.log file, you will find an entry for the Kingston USB with the following text:

```
>>>  [Device Install (Hardware initiated) -
SWD\WPDBUSENUM\_??_USBSTOR#Disk&Ven_Kingston&Prod_DT_100_G2&Rev_PMAP#000FE
AFB938CECC027E200F6&0#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}]
>>>  Section start 2013/12/18 11:41:02.723
```

The last line that starts with "> > > Section start" contains the date and time when the device was first connected. This log records information in local time. That means that the first time the device was plugged in was December 18, 2013 at 11:41 AM (PST).

You are going to need this file for the USB tool, so go ahead and extract the setupapi.dev.log file by right-clicking it and selecting Extract File(s) (see Figure 8-15).

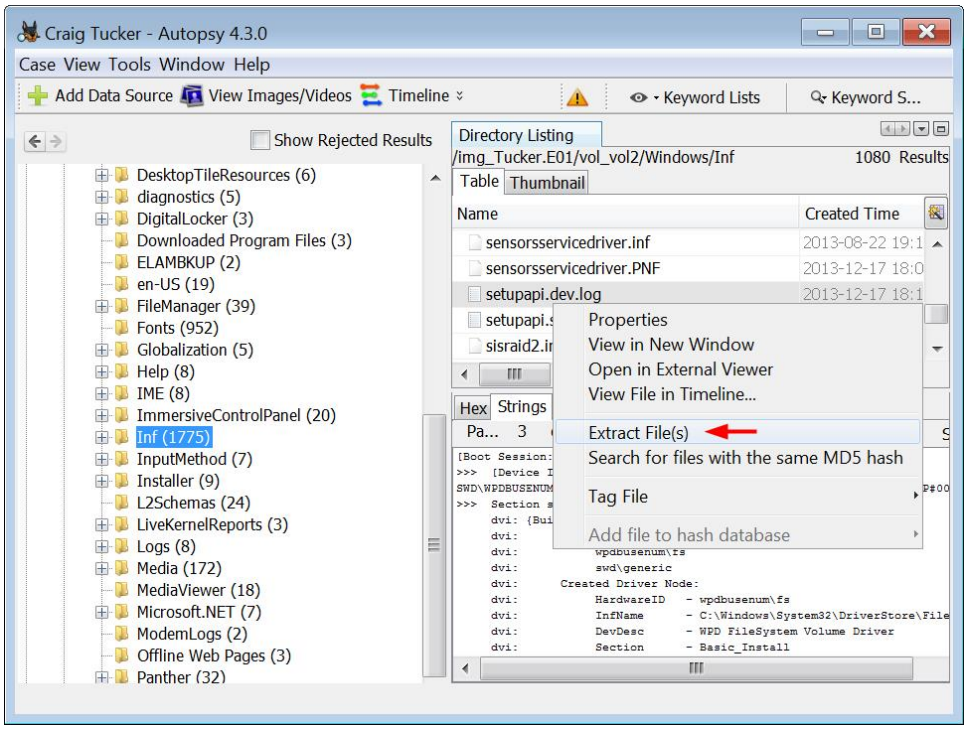

Figure 8-15 – Extract setupapi.dev.log to Export Folder

Navigate to the setupapi.dev.log file to the case Export folder and click Save.

USB Historian

Now that you know what information is stored when a USB device is connected, and where it is stored, you can use tools to quickly create a USB report. You are going to use a tool called USB Historian from 4Discovery, which you can download for free from their website:

```
https://4discovery.com/usb-historian/
```

Open the USB Historian tool, and in the top left corner you need to click the button Open File(s). A Wizard window will open, and you need to choose Select Individual Hives/Files. Click Next.

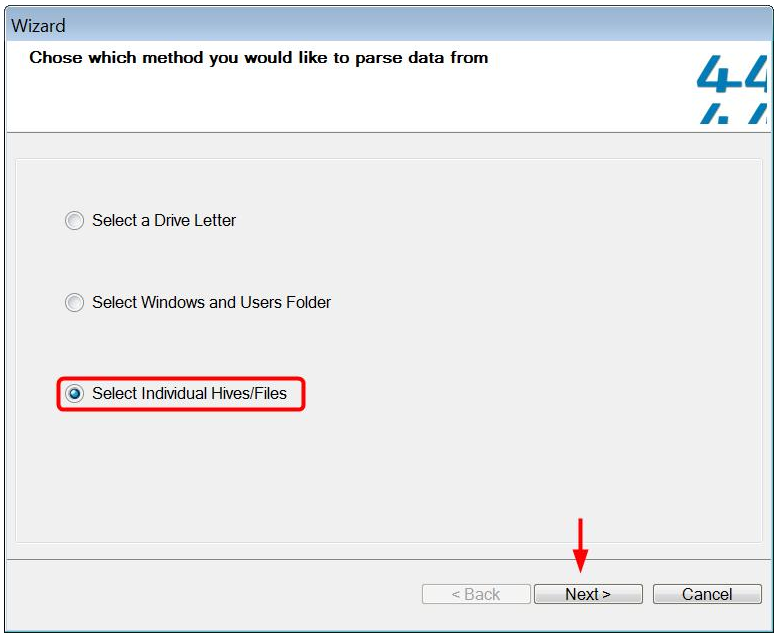

Figure 8-16 – Choose Select Individual Hives/Files and Click Next

When the next window opens, you need to add the SYSTEM hive, the SOFTWARE hive, the NTUSER.DAT registry hive, and the setupapi.dev.log file you exported. Navigate to your case's Export folder and add each corresponding hive or file and then click Finish (see Figure 8-17).

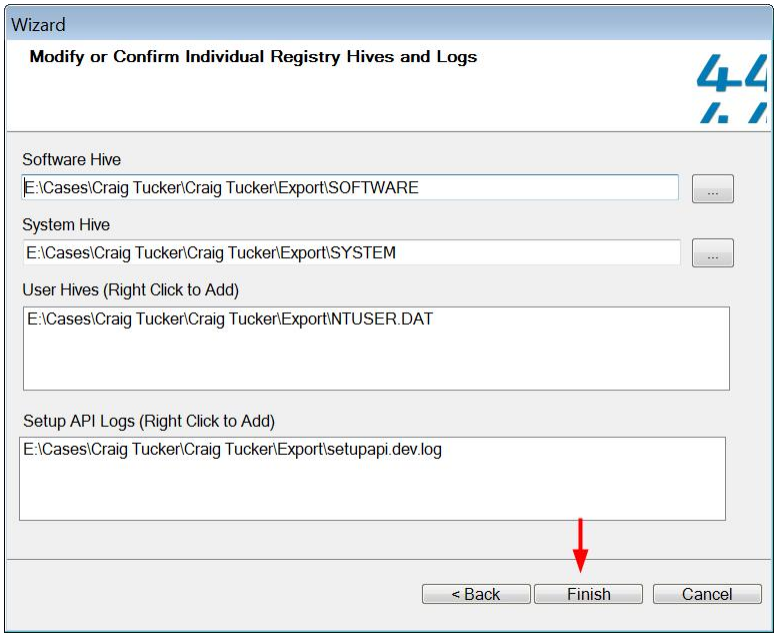

Figure 8-17 – Add Exported SOFTWARE, SYSTEM, NTUSER.DAT, setupapi.dev.log and Click Finish

Friendly Name	Serial No	S..	Mount Point 2	Drive Letter	Volume Name	Ready Boost Volume Name
Kingston DT 100 G2 USB Device	000FEAFB938CECC027E200F6		[Craig:12/21/2013 9:23:15 PM]	E:		STUFF

Friendly Name: The name of the device. (Found in SYSTEM hive)

Serial No: The iSerialNumber of the device. (Found in SYSTEM hive)

Mount Point 2: The user that plugged in the device and the last time (UTC) that the device was plugged in by that user. (Found in NTUSER.DAT)

Vol: The device's drive letter. (Found in SYSTEM hive)

Ready Boost Volume Name: Volume label of the device. (Found in SOFTWARE hive)

Usb Stor DateTime	Usb Stor DateTime64	Usb Stor DateTime65	Vendor	Product	Version	Vid	Pid
12/18/2013 7:41:02 PM			Ven_Kingston	Prod_DT_100_	Rev_PMAP	VID_0930	PID_6545

Usb Stor DateTime The date/time that the device driver was installed (Found in SYSTEM hive)

Vendor, Product, Version: The vendor, product, and version. (Found in SYSTEM hive)

Vid and Pid: The Vender ID and Product ID. (Found in SYSTEM hive)

Guid
16d5eeec-681c-11e3-824f-000c29d6ef92

Guid: The device's GUID. (Found in SYSTEM hive)

