

Forum:[Hack Forums](#)

Thread: [How to Trace USB History and Modify or delete them...??](#)

andrew3008 - April 26, 2011, 7:13 am

Well!! nowadays we use our USB port to plug in many devices like mp3 players, i pods, pen drives etc, it is also very true that these devices are also vector of many viruses, Trojans and backdoor etc which can be lethal sometimes.

Today I am going to discuss how we can keep a track of all the USB devices that were connected to our computer (WIN XP / 7/ Vista). This trick can be very helpful in case you find that some data has been stolen from your PC.

The USB history in a PC can be tracked by two methods:

- a) By looking directly into the registry files.
- b) by using Tool.

Lets first start with Registry file method.

- 1) First open up Run and type "regedit" and hit enter.

Note: USB history can be found at two places in registry

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

- 2) A registry editor window open up ,in that window follow the steps as shown in the image below. (Here we will look into the second registry path mentioned above but you can also try with the first one)

[img]http://i51.[censored].com/2j43mrs.png[/img]

In the above image you can see that after i connected a pen drive and its information is present there in the registry.

So lets see how we can do this with a tool. The tool that we will be using for this is Nirsoft's USBVIEW. [DOWNLOAD](#)

- 1) Download the Tool and just run ,it will show all the devices that were connected to your PC.

[img]http://i54.[censored].com/mx1zqw.jpg[/img]

Note: Serial numbers are unique for external devices but internal devices as you can see have same serial number.

- 2) Now select anyone of the external device and right click on it and select Properties. It will show you all details about the external device as shown in the image below.

[img]http://i52.[censored].com/vpawp2.jpg[/img]

Now we have retrieved the history of the USB devices so,lets see how we can delete these history informations.

1) Open up the registry editor window as shown in the above steps then follow the on screen steps as shown in the image below.

[img]http://i51.[censored].com/b4ds8g.png[/img]

2)After completing all the steps in the above image you will be able to delete the registry key or subkey.

By doing this the traces are removed ...!!

Foosmeels - April 26, 2011, 3:27 pm

Is this a Tutorial or a Question? I don't understand? If this is a tutorial, why not post it in the tutorial section?

andrew3008 - April 26, 2011, 11:12 pm

Sorry mistakly i posted here :((i thought its correct to share Miscellaneous Computer Talk)

Terence McKenna - April 27, 2011, 6:50 am

This is a tutorial, and a rather HQ one at that, nice tutorial OP.