

Forum:[Hack Forums](#)

Thread: [Registry Forensics\(Typed URLs, USBs, SAM, and more\)](#)

HFblackhats - December 31, 2014, 8:51 am

Registry Forensics

Tools:

Access Data Registry Viewer

Registry forensics is pretty cool you can find a ton of information if you know where to look. You can find typed urls, list of all usb's plugged into the computer, The computer time zone, last user logged in, and a lot more.

Let me start off by saying that is registry forensics we look at things calld Hives
You typical have 5 hives to look at each containing different information about the computer.

1. Hkey_Local_Machine\system
2. Hkey_Local_Machine\Software
3. Hkey_Local_Machine\Sam
4. Hkey_Local_Machine\Security
5. NTUSER.dat

You can do a google search and find out where to find these hives on your computer or just ask me.

[img]http://s3.postimg.org/6igtfbt1f/image.png[/img]

[img]http://s3.postimg.org/ukxna79oj/image.png[/img]

Open up Access Data Registry Viewer

First let me go over the Sam Hive.

Go to the same Hive > Sam > Domains > Account > Users >Names

[img]http://s3.postimg.org/ckog5thhf/image.png[/img]

we will be working under the Users tab and also the Names tab.

If you click under the names tab and pick one of the user names im going to use Archangle you will see the Type is 0x03EB. This is called a RID and it allows you to locate which User it is under the Users tab.

[img]http://s3.postimg.org/jcev8o6gz/image.png[/img]

Im going to click under the Users tab and click the folder 0000003EB and that will be the Archangle user. Do you under stand that 03EB means archangel user?

This will show us a lot of information about the user like.

The last login- 10/1/2009

Login count – 3

User name Archangle

Last password change – Never

And over to the left you see User title. This is the person picture that you see at the login screen. You can actually extract that and recover the persons image that they set at the login screen. Make sure if you want to extract the bmp file to start with BMX and go copy everything down from there. Then right click hit save selection and save it as a .bmp file. Pretty cool right?

[img]http://s3.postimg.org/9hnq2g2ir/image.png[/img]

Let move on to something else. I can't possibly show you everything thing you can do with all the HIVES because there is so much information that it would take weeks. So I'm just going to show a few things I think is cool. If you want to know more just PM me.

HMMM let's take a look at the users typed URLs

For this we need to move to the users NTUSER.dat folder. Every user account has their own NTUSER.DAT folder so I'm going to pick the user account called String and click on his NTUSER.DAT

To get to the users internet explorer typed URLs we have to navigate to a certain folder. Don't worry I know where to look.

In the NTUSER>.Dat go to Software > Microsoft > Internet Explorer > Typed urls

And bam we can see all of his typed urls. Looks like he likes helicopters lol.

[img]http://s3.postimg.org/hyn8dd77n/image.png[/img]

What else can I show you that might be interesting hmmmmmm. Let's take a look at all the USBs that were plugged into this computer.

Ok First go to the System HIVE

Controlset > Enum > USBTOR

This will list all usb's that were connected to your computer So if you think someone can't link a particular usb thumb drive, external harddrive or anything that uses a usb to you. YOUR WRONG.

If you click one of the folders and expand it you can see the devices serial number. For example the serial number for this sandisk I found on the computer is 00001543A86049CD&0

Haha got em.

And you can also see the name of the usb device under Friendly Name. In my case it's SanDisk u3 cruze micro usb device.

[img]http://s3.postimg.org/qjgk4jhdv/image.png[/img]

There is sooooo much more I can show you if you guys seem to like this TUT I'll make more showing you how to find different things like account passwords for outlook, Things about yahoo messenger, ICQ, AOL Instant messenger, Yahoo messenger, system information, More things on internet explorer, and a lot more.

Hope you enjoyed it took me like an hour to write this up for you guys. I noticed my last tutorial about data carving might have been a little complicated/ advanced for most users on here so I made this because it's a lot easier to understand and comprehend.

Go forensics :)

And no this is not my computer my teacher gave me this practice file for an assignment a few

months ago if you want these hives you can practice as well just let me know i don't mind sharing :)

HFblackhats - *January 1, 2015, 11:21 am*

whats up does no one like like forensics on this site ???? Figured someone would comment .

Sacred Symmetry - *January 1, 2015, 11:23 am*

Well done, very well written and illustrated.

You will have a good life here on HF if you keep this up

powerl105 - *January 2, 2015, 5:01 am*

keep them coming! solid info.....i wonder if there is software out there that will target these reg keys specifically and wipe them. I dont think ccleaner does this.

Michael.G - *January 7, 2015, 8:07 am*

I would be very interested in any other tutorials u may have!!

Wanna do a tutorial on how to recover deleted history from the various browsers e.g chrome safari etc and also iS it possible to recover "incognito" browser history