**Lab 7-2: Registry Forensics with RegRipper Plug-ins**

**Registry:**

The window registry is a hierarchical database that houses the OS, apps, users, and device setup settings.

Information on the system, installed and running programs, user activity, and connected devices can all be found there.

The registry is a composed of binary data files also called “hive”.

• The main registry hives are SAM, Security, Software, and system.

• They are located under the C:\windows\system32\config

• There are also specific user’s hives NTUSER.DAT, and URSCLASS.DAT

These are located under the user’s profile

Keys and values are the registry's two fundamental building blocks.

Containers for other keys and/or values include keys.

Names, types, and the corresponding data value serve to define values.

The HKLY\_LOCAL\_MACHINE root key, where the primary registry hives are mapped as subkeys, is the most significant one.

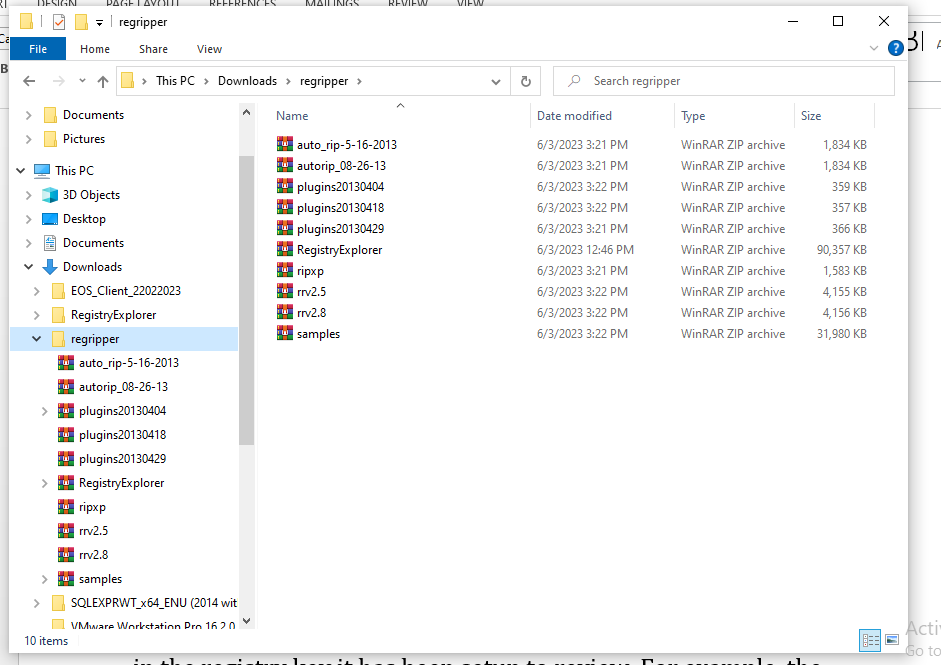
**RegRipper:**

RegRipper uses plugins to extract information out of the registry files. Each plugin has been created to handle the data that is stored in the registry key it has been setup to review. For example, the plugins will decode the ROT-13 encrypted data and translate binary data to ASCII.

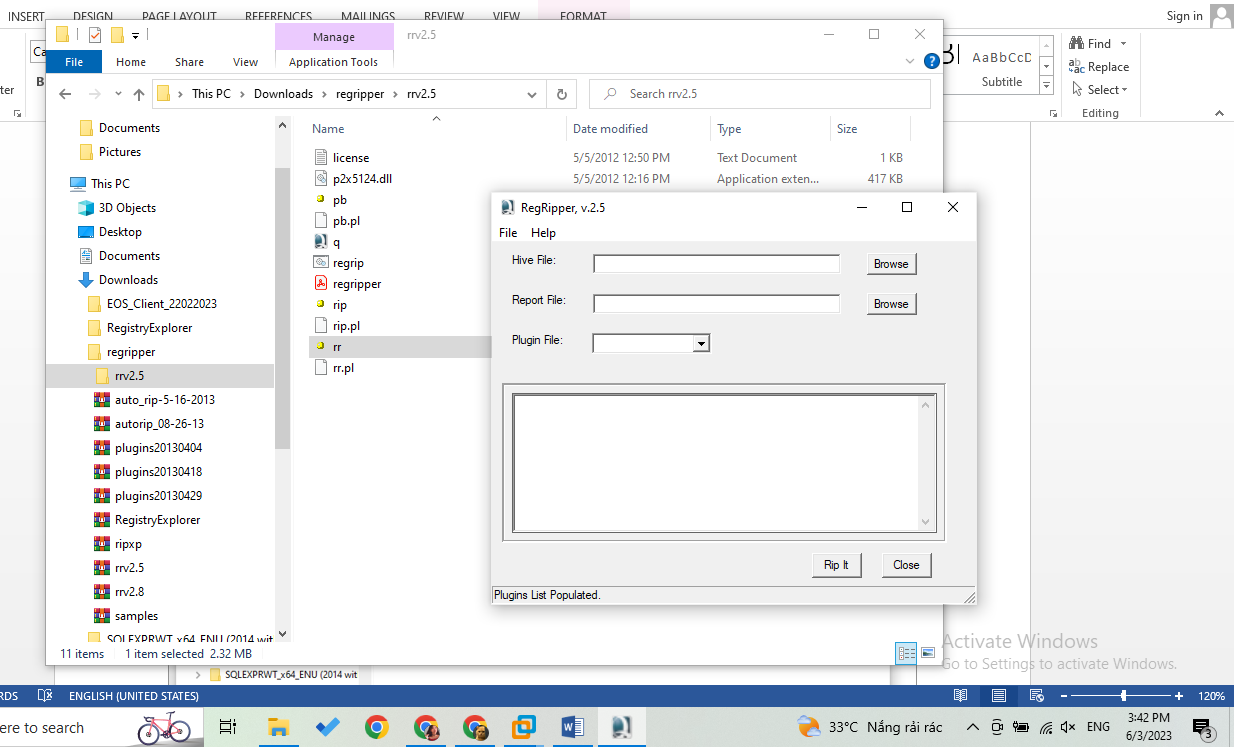
The forensics community contributes Perl scripts as the plugins. It regularly extracts data from a certain area of the registry during your forensics case investigations.

We use available plugins

I have just downloaded all the files and put them into a folder named **regripper**

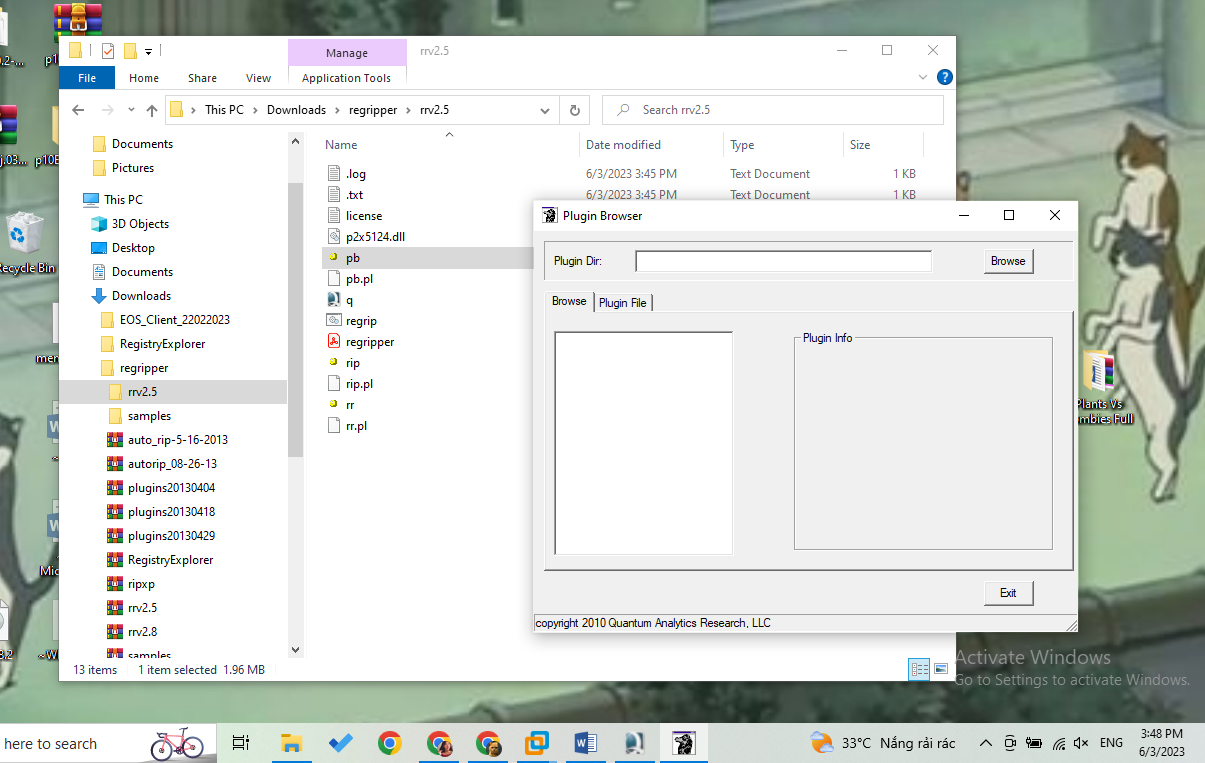


After that we extract the file **rrv2.5** then double-click into **rr:**



* Here is the display that we are going to execute

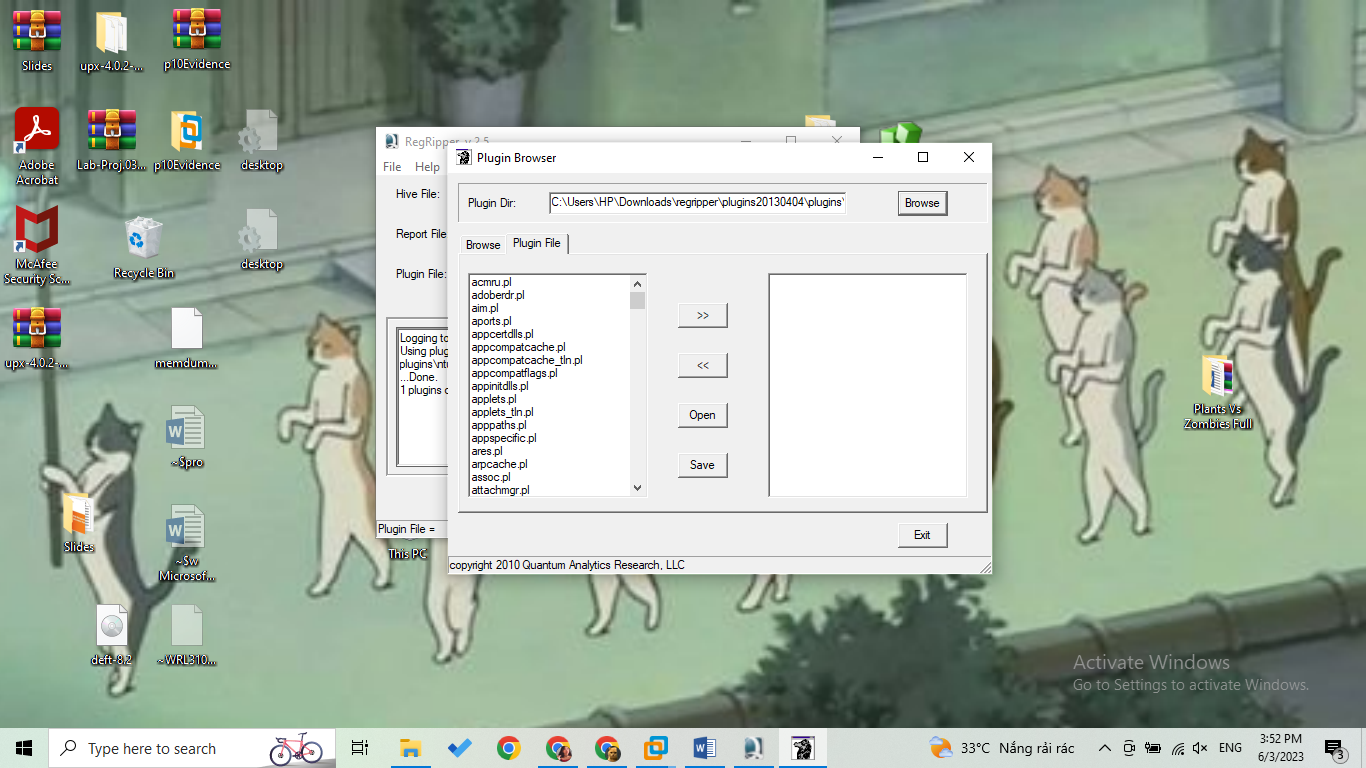
Open **pb** to browse the needed files



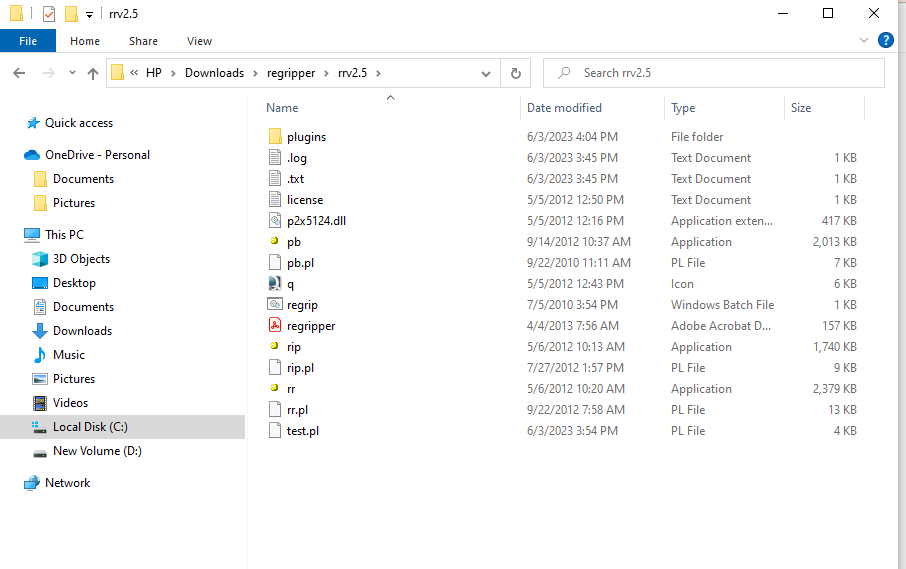
Browse any files then check the plugins

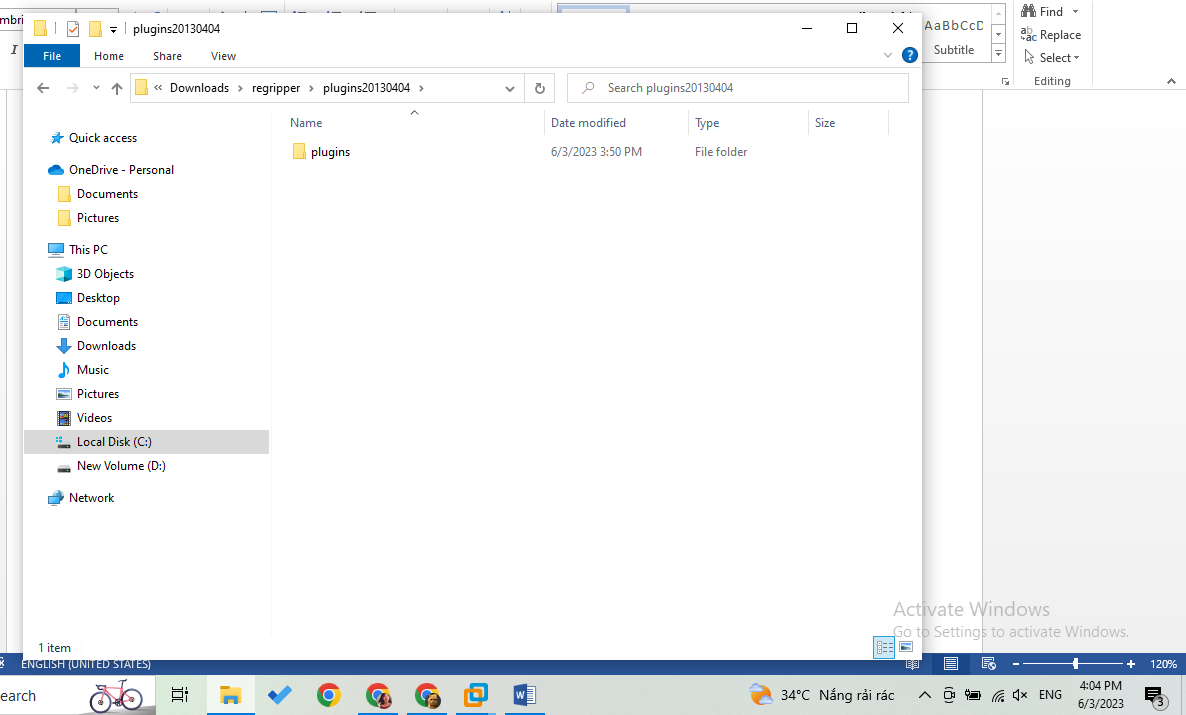
Use << >> for copy the between 2 displays

Open or save when we need

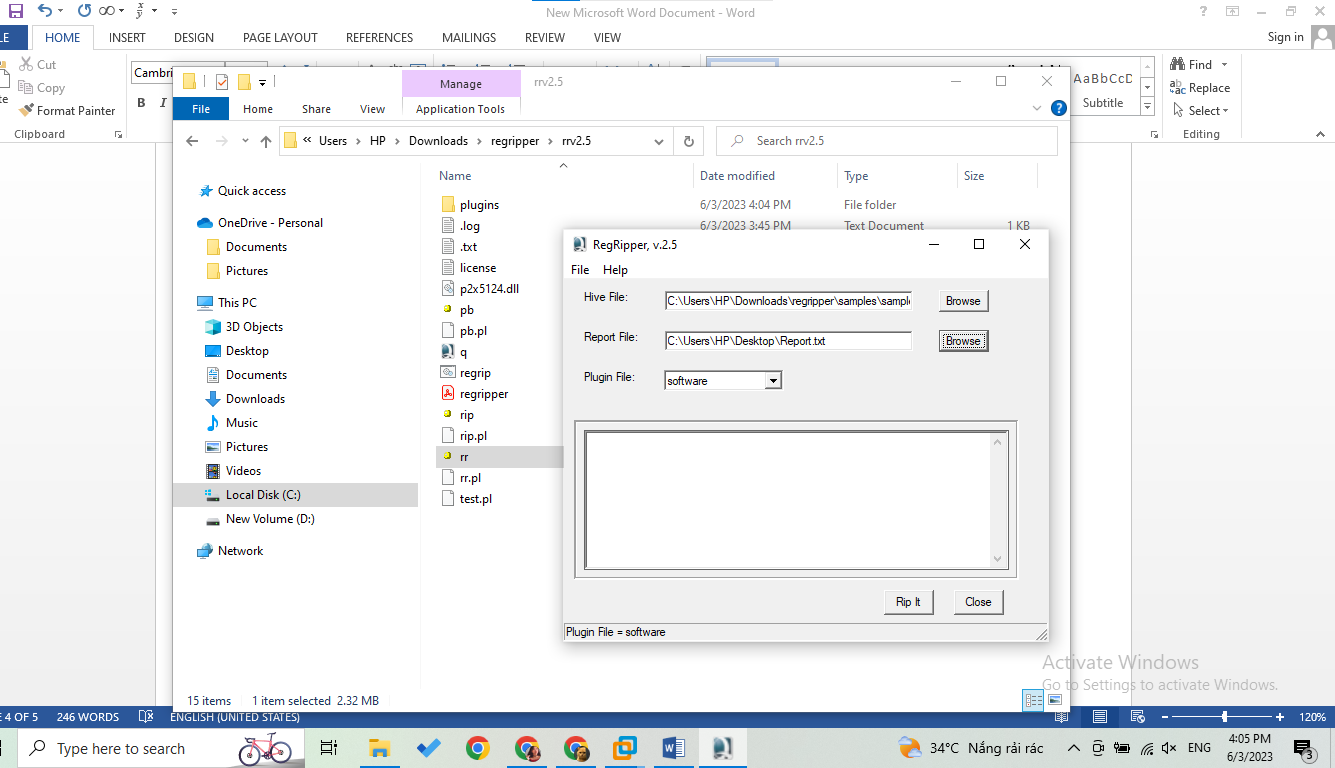


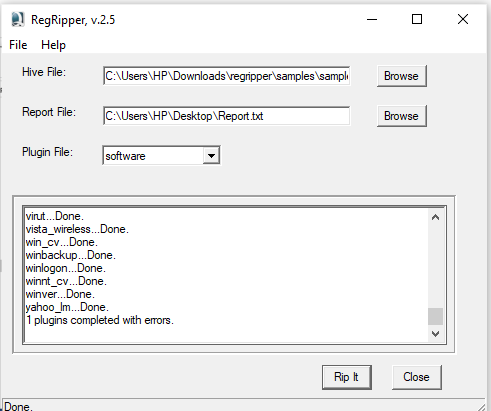
Then at the moment we open the folder rrv2.5, we should see the plugins folder here. The thing we have to do is that copy that folder



And go to plugins20130404 folder to paste the folder plugins as following 

Then open rr tool, browse the sample, choose plugins file as software => press rip it

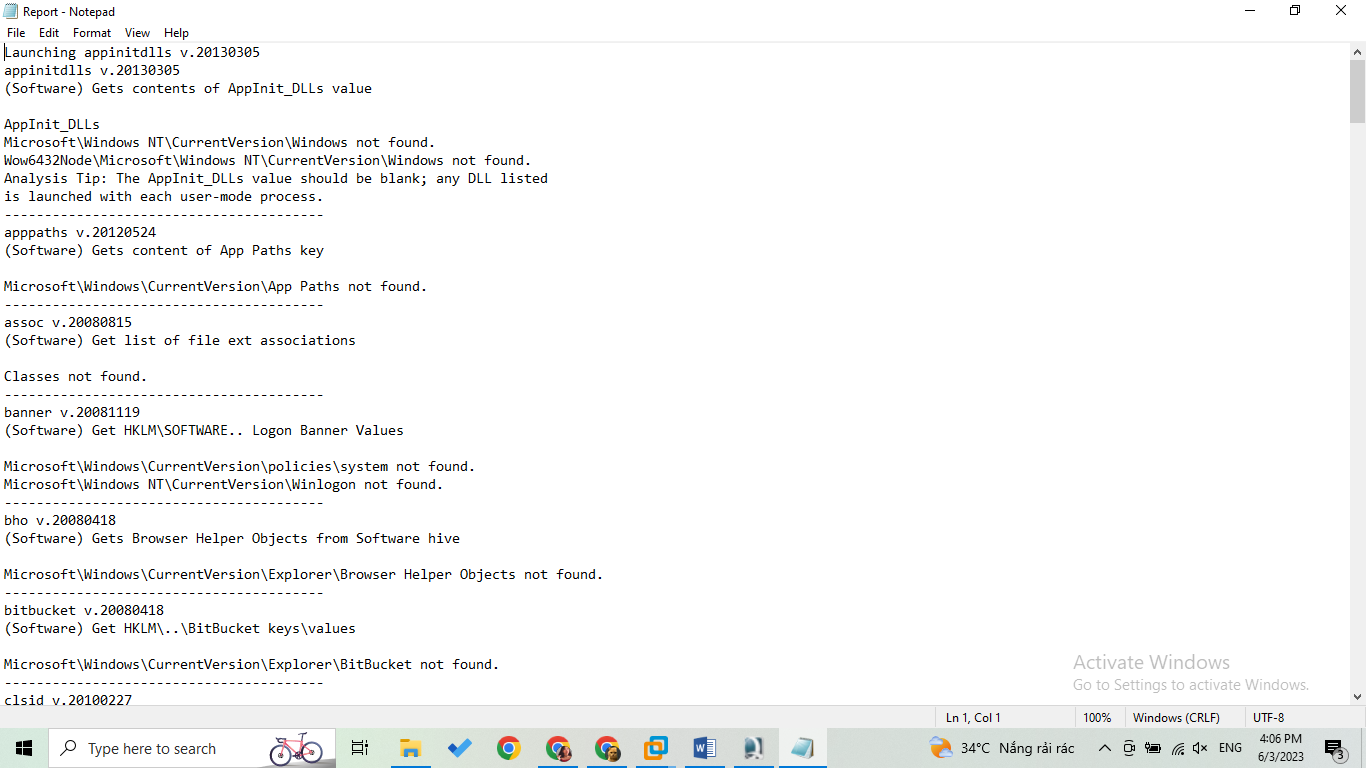




* Process was done
* Save it and name report

On our desktop gonna extract a new txt file named report

Open the that text file:



* That was the way forensic science team make evidence report.

These are only a handful of the plugins available with the RegRipper tool used in Windows registry forensics. The beauty of this tool lies in its flexibility and scalability.

When they encounter a Windows box, Windows registry proves to be a critical source of information during the investigation