How to study Forensics Evidence of PC using P2 Commander (Part 2)

May 18, 2015 By Raj Chandel

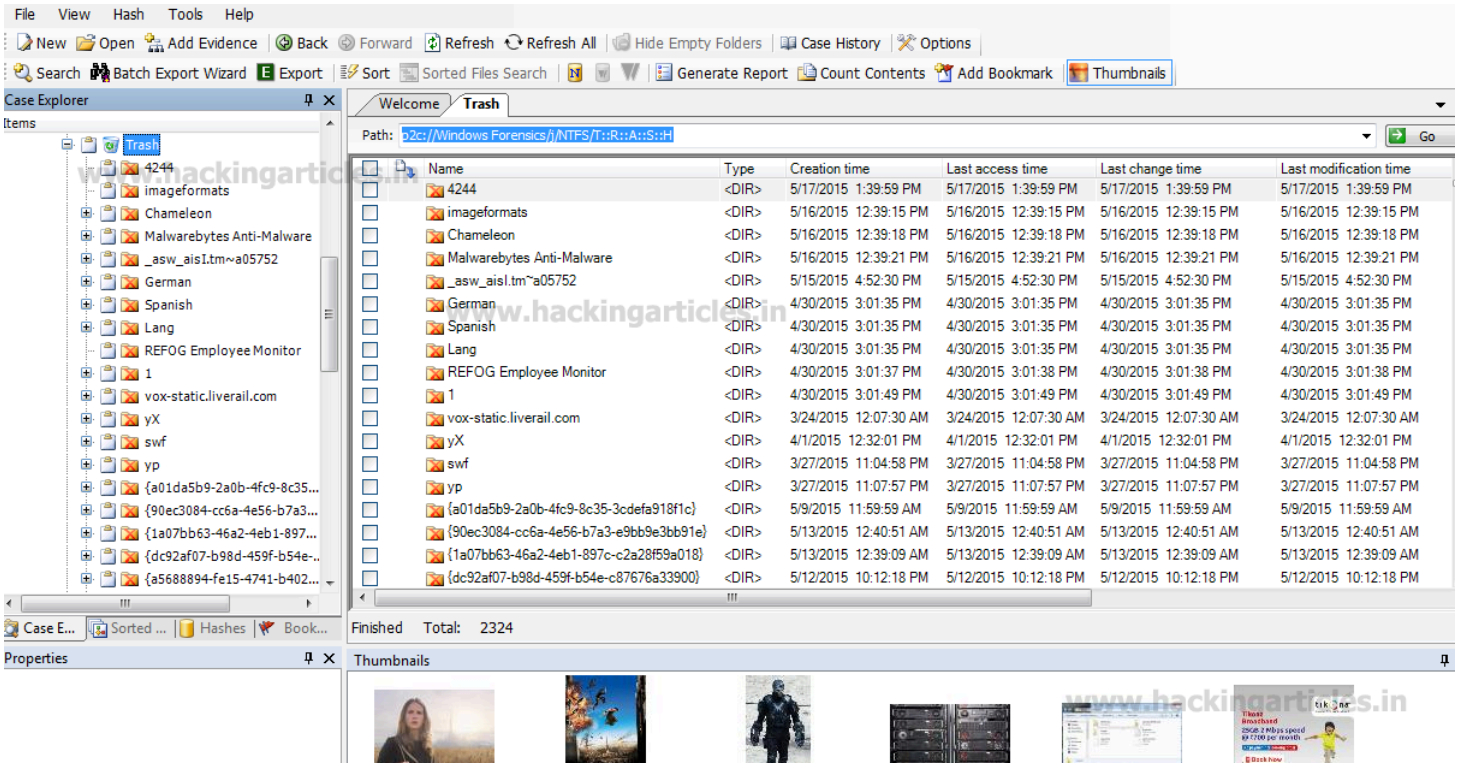
Now we are studying about the forensic evidence which we have collected in the previous article.

If you are interested to see the collection of forensic evidence, please click on the below link.

http://www.hackingarticles.in/how-to-collect-forensics-evidence-of-pc-using-p2-commander-part-1/

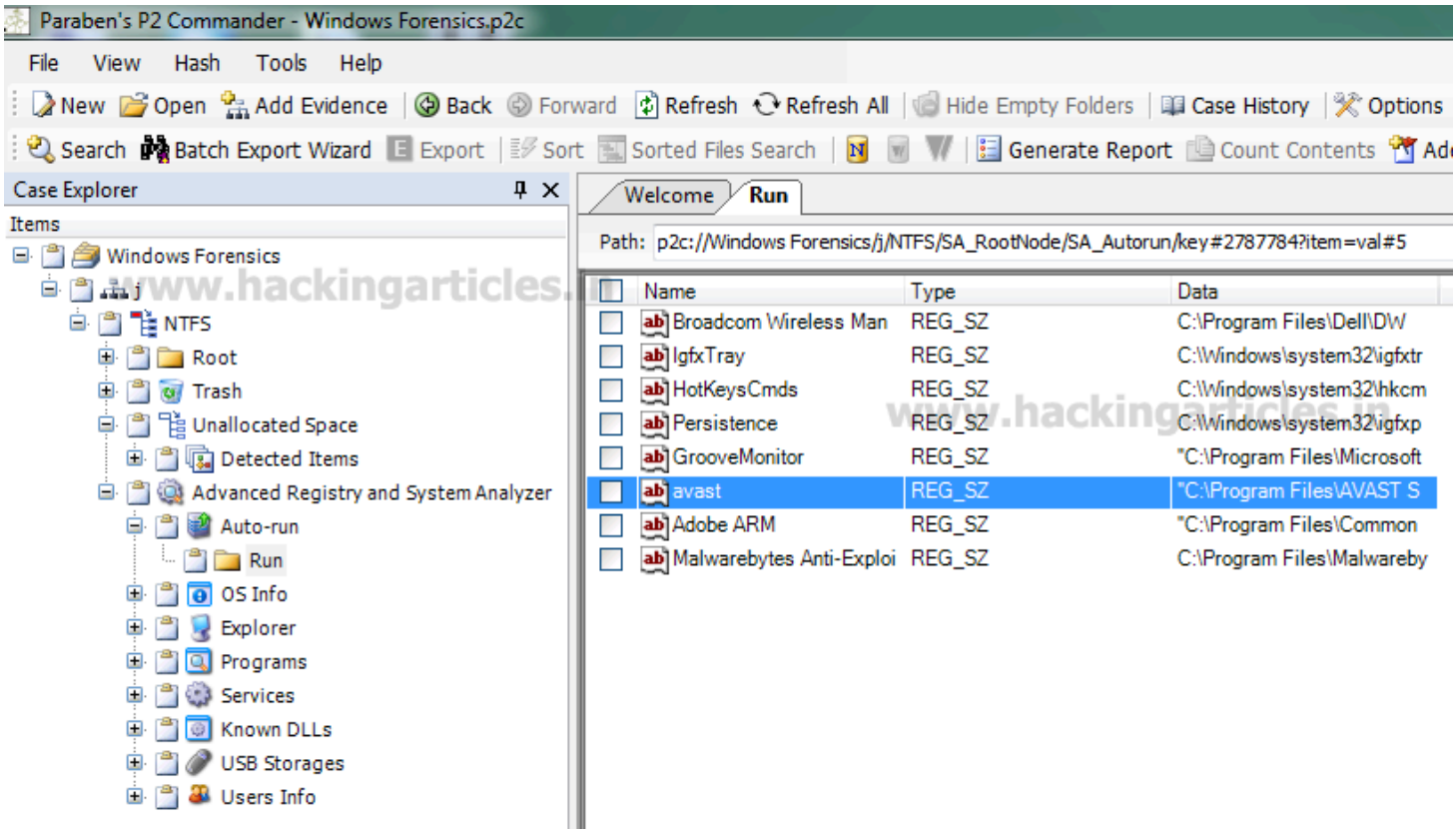
First of all, we will look into the **Trash folder** (which contains the files and folders deleted by the user but not erased permanently from system yet).

By clicking on **Trash folder**, it will show us the different files and folders with their Creation Time, Last Access Time, Last Change Time, and File Size.

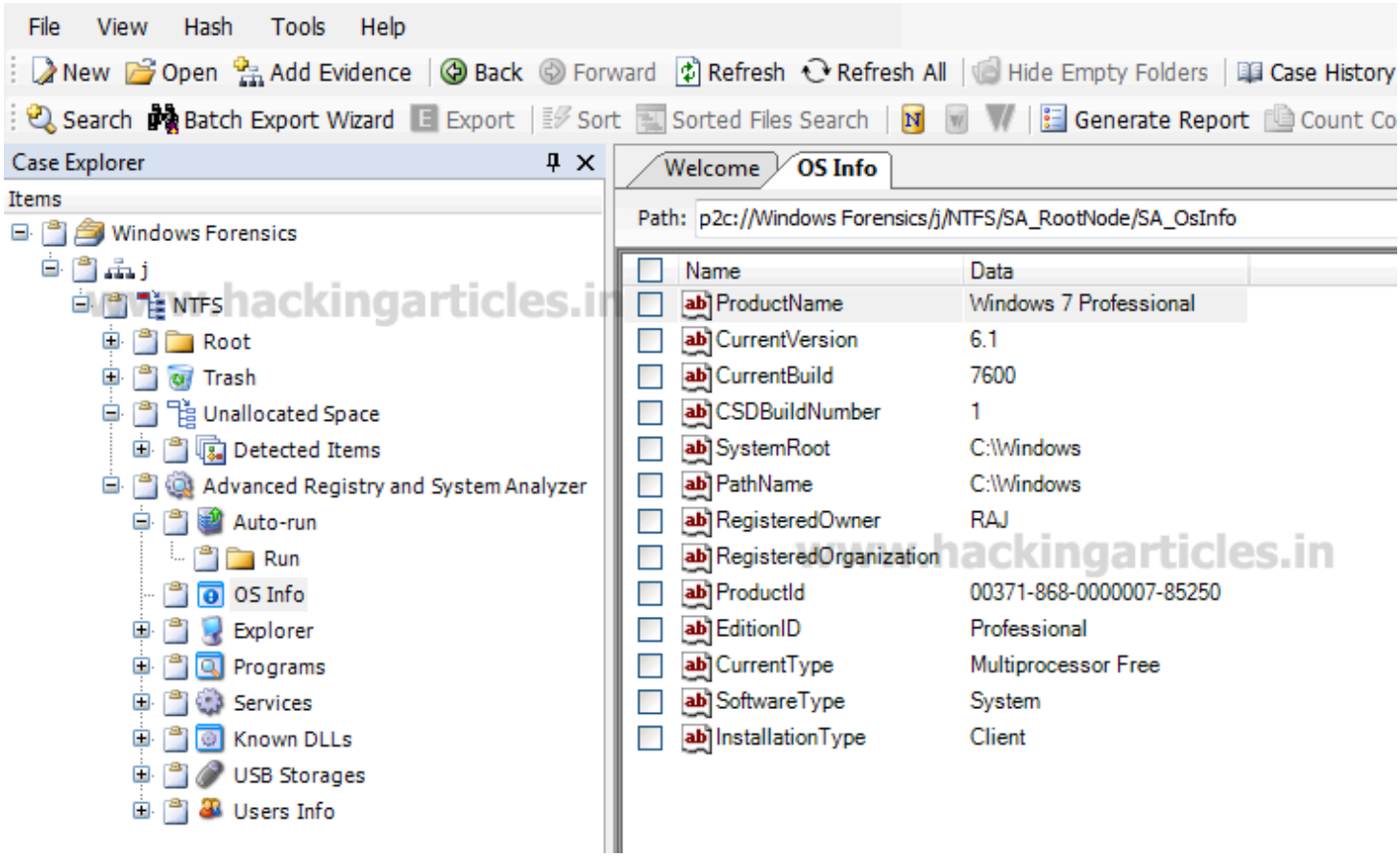


Now click on **Advanced Registry and System Analyzer** and then **Auto Run** Option.

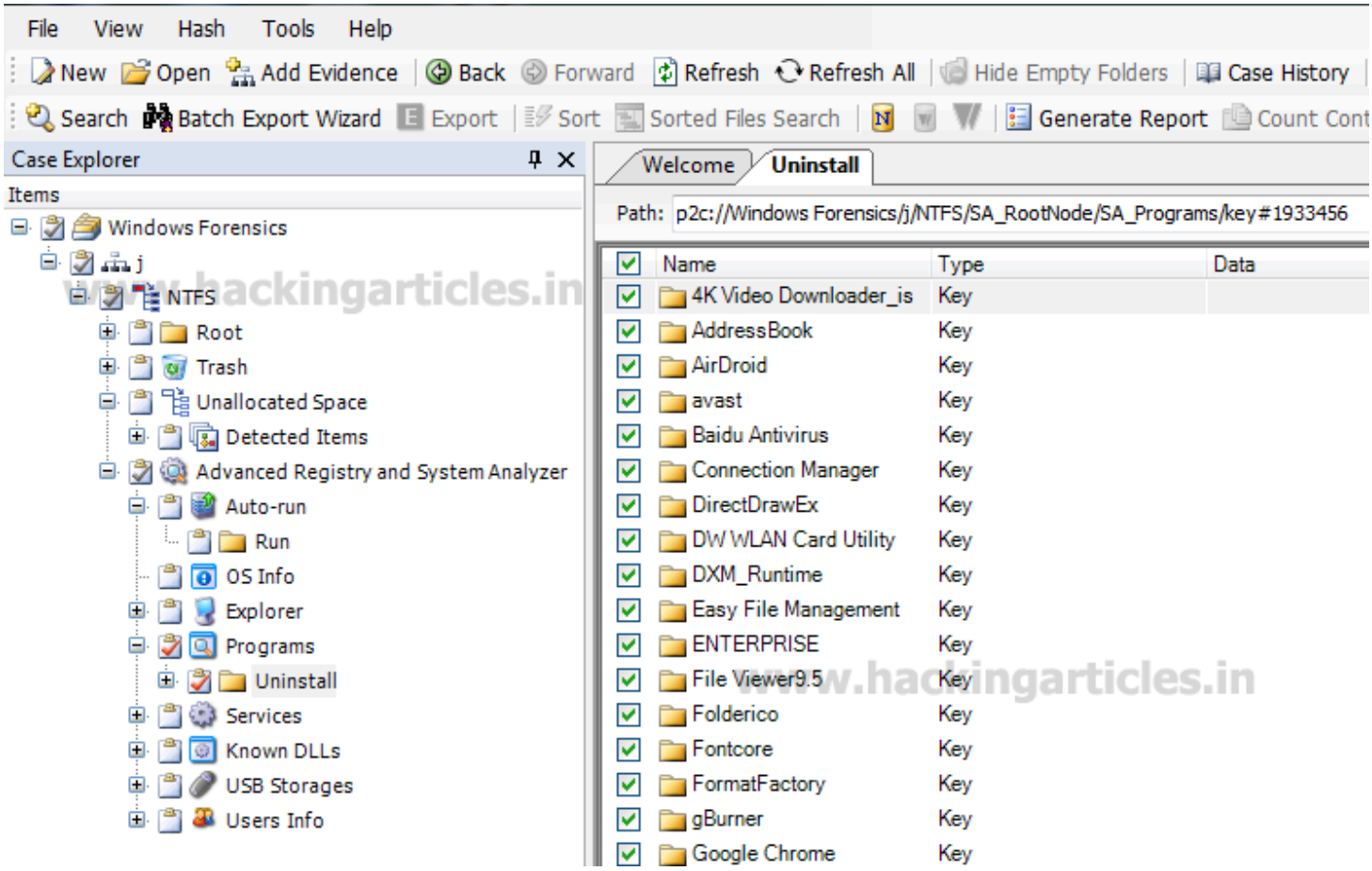
Go to **Run** option. It will Show all the programs that can run automatically at the time of booting of the system.



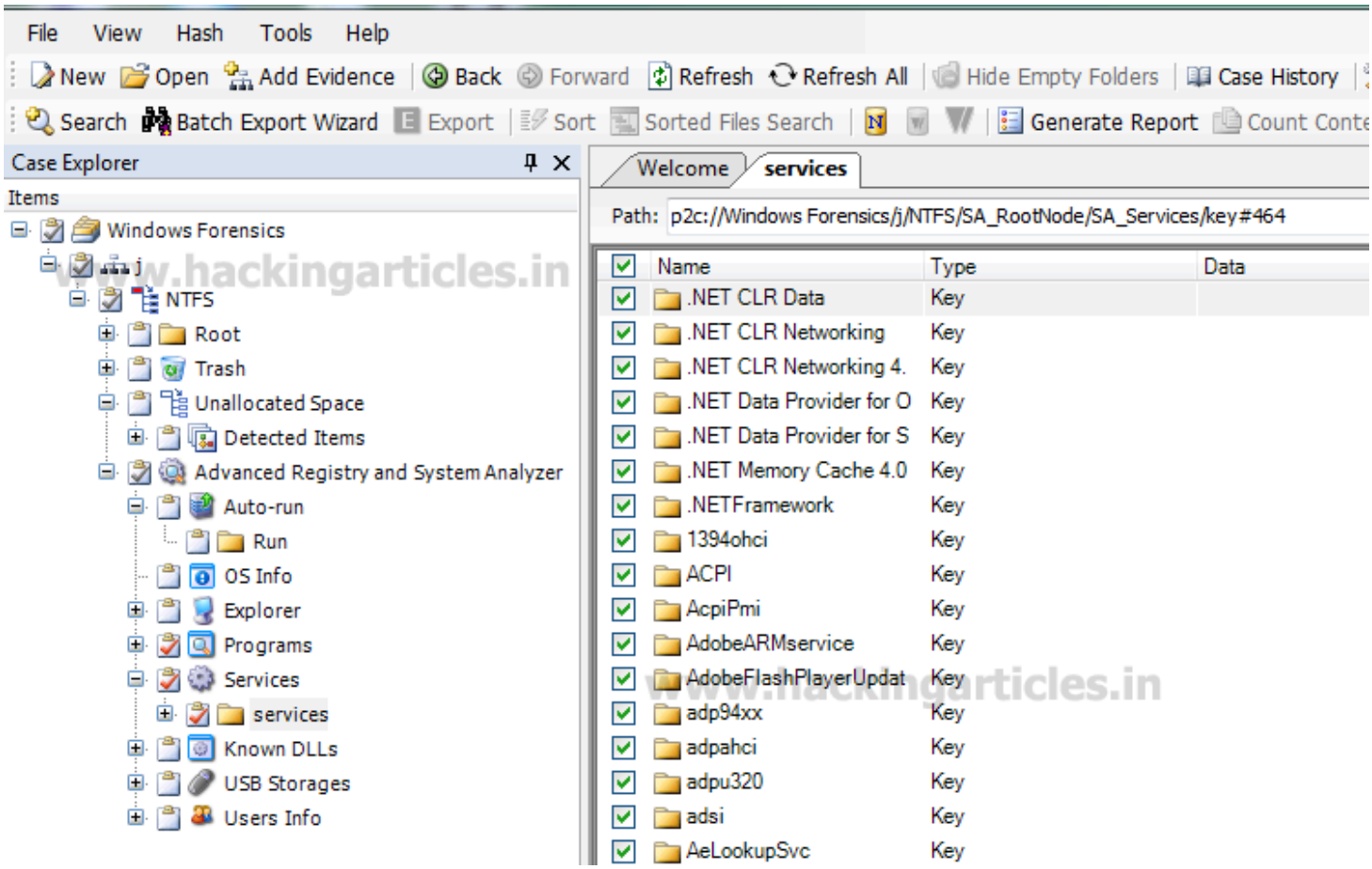
Now Select **OS Info** option. Through **OS Info**, we can see the Root Path, Current Version, Registered User, Product ID, Edition ID, and Installation Type.



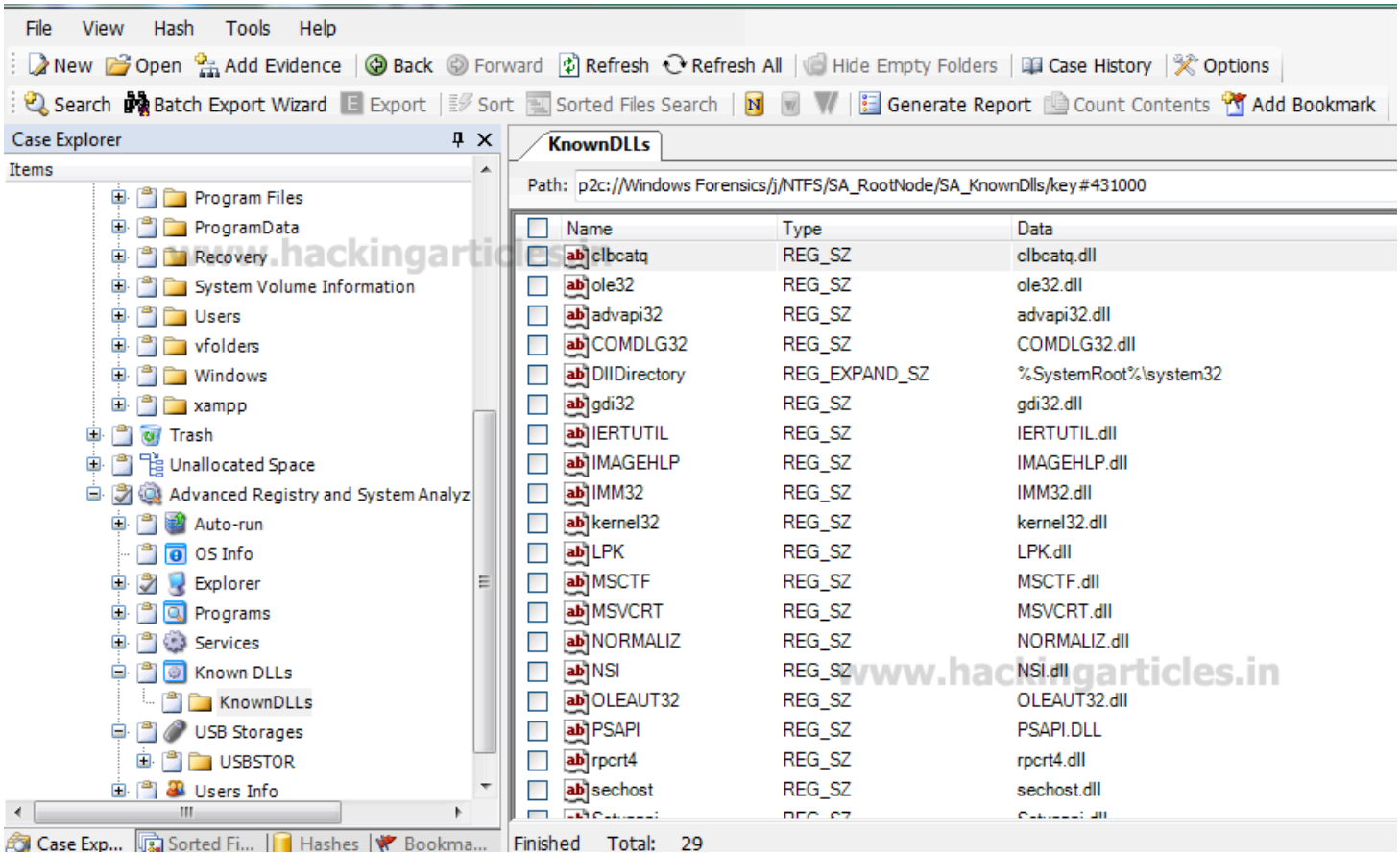
Now select **Uninstall Option** from **Programs Option.** By **Uninstall Option**, we can see all the programs which are installed in the system.



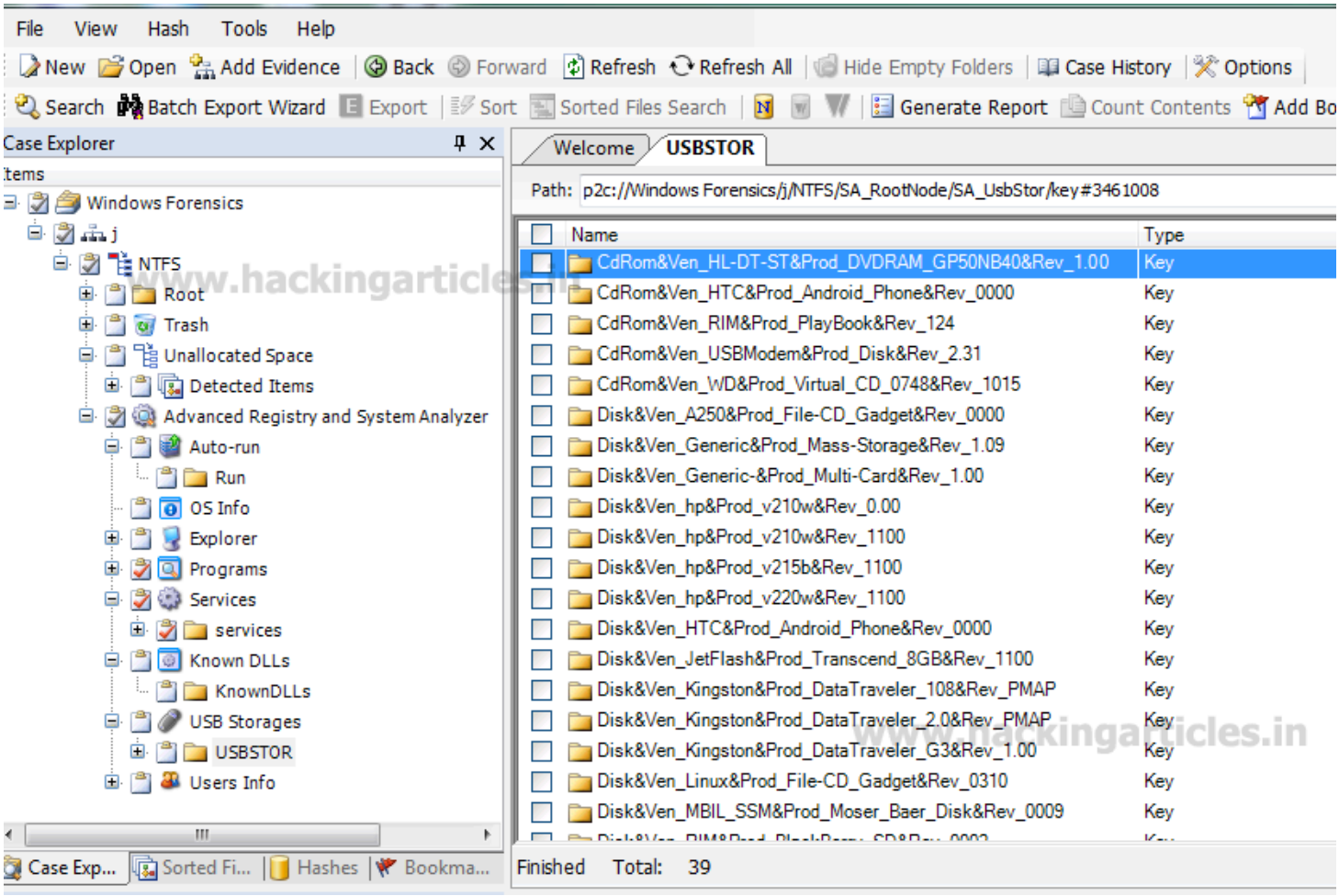
To see the running services in the system, select Services option.



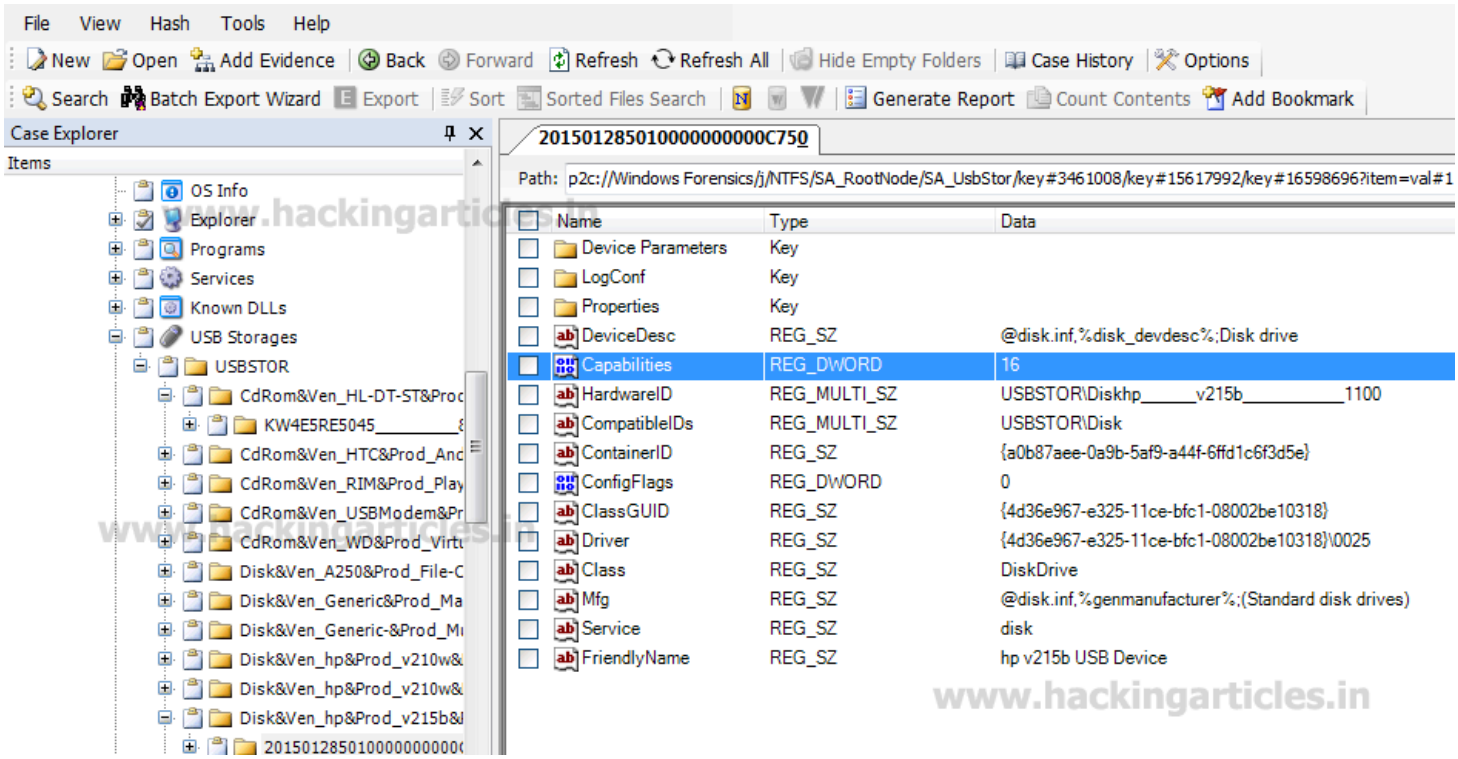
Now click on **Known DLLs** to see the Dynamic Link Libraries (which contains data and code that are used by different programs simultaneously.)



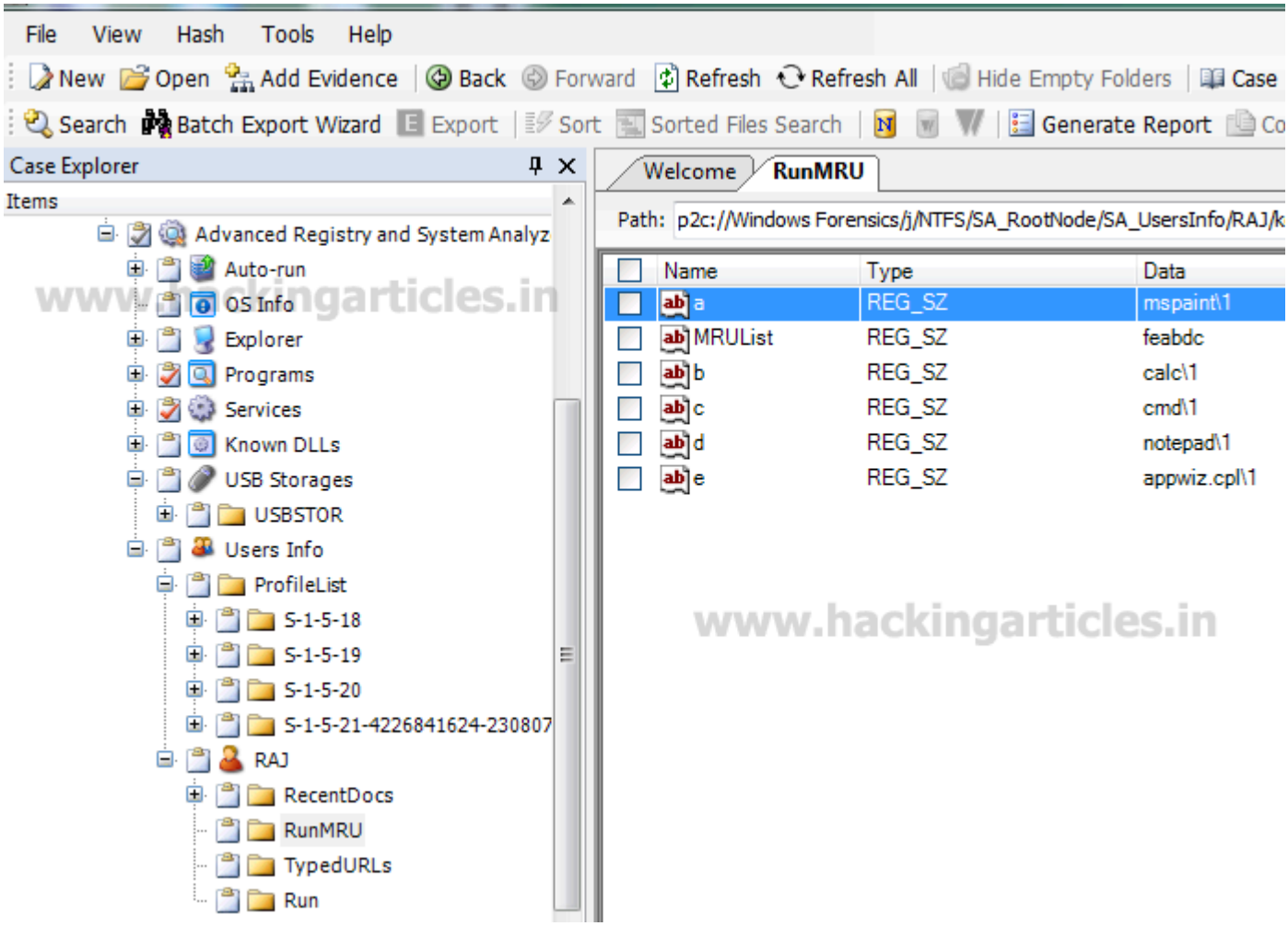
Now to get the information about the removable disks used recently or in the past, first click on USB **Storage** and then select **USBSTOR.** It will show the name of the Disks.



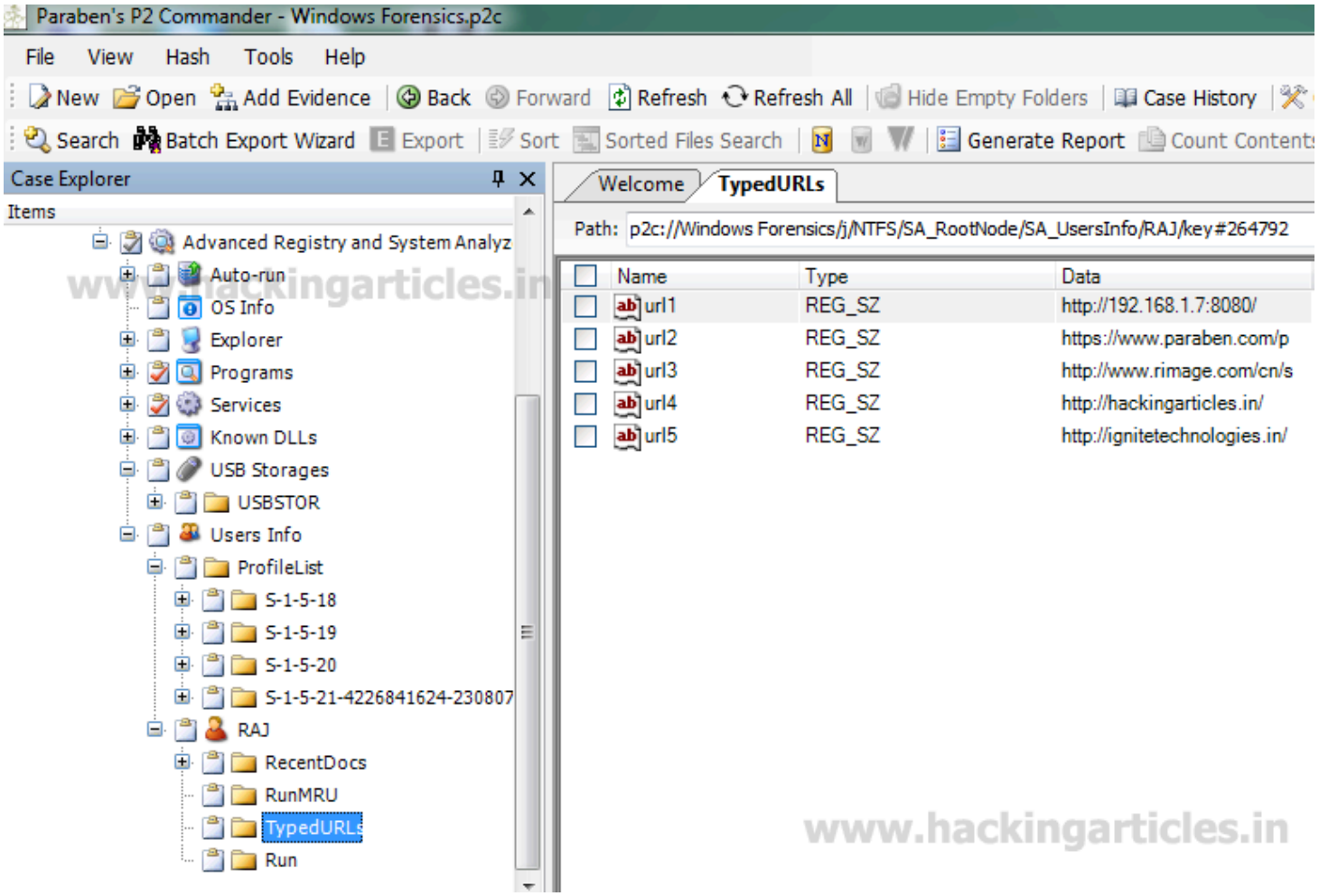
Now select any one of the disk and it will show us the size as well as the manufacturer name.



To see the history of most recently used commands from the Run command on the Start menu click on Users Info Option. Select a user; in my case we are selecting Raj. Now click on RunMRU.



To see the user-based web activities, click on the **TypedURLs, which** will show the recently visited web sites.


Paraben's P2 Commander - Windows Forensics.p2c
File View Hash Tools Help
New Open Add Evidence Back Forward Refresh Refresh All Hide Empty Folders Case History
Search Batch Export Wizard Export Sort Sorted Files Search Generate Report Count Contents
Case Explorer
Items
Advanced Registry and System Analyz
Auto-run
OS Info
Explorer
Programs
Services
Known DLLs
USB Storages
USBSTOR
Users Info
ProfileList
S-1-5-18
S-1-5-19
S-1-5-20
S-1-5-21-4226841624-230807
RAJ
RecentDocs
RunMRU
TypedURLs
Run
Welcome
TypedURLs
Path: p2c://Windows Forensics/j/NTFS/SA_RootNode/SA_UsersInfo/RAJ/key#264792
Name
Type
Data
url1 REG_SZ http://192.168.1.7:8080/
url2 REG_SZ https://www.paraben.com/p
url3 REG_SZ http://www.rimage.com/cn/s
url4 REG_SZ http://hackingarticles.in/
url5 REG_SZ http://ignitetechnologies.in/
www.hackingarticles.in