**DIGITAL FORENSICS LAB**

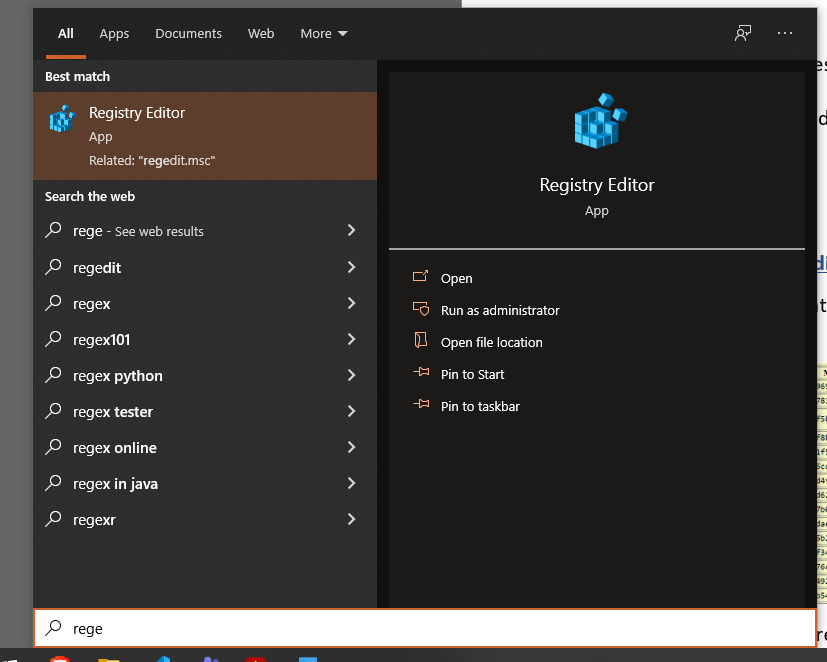
|  |  |
| --- | --- |
| Exercise 12 | |
| Name | S Shyam Sundaram |
| Registration Number | 19BCE1560 |
| Slot | L39+L40 |
| Faculty | Dr. Seshu Babu Pulagara |
| Date | 23rd November, 2021 |

**AIM**

Exploring the windows registry keys and values.

**PROCESS**

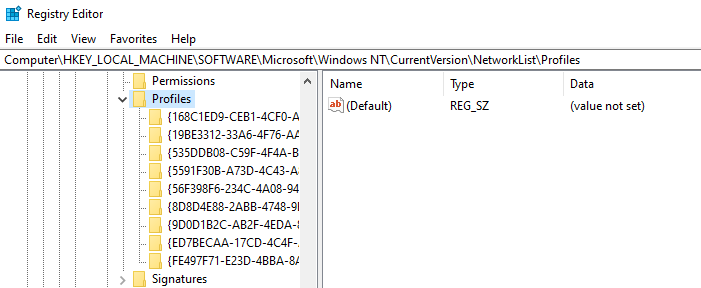
1. Open up ‘Run’ or press the windows key.
2. Search for Regedit.
3. Open the ‘Registry Editor’.

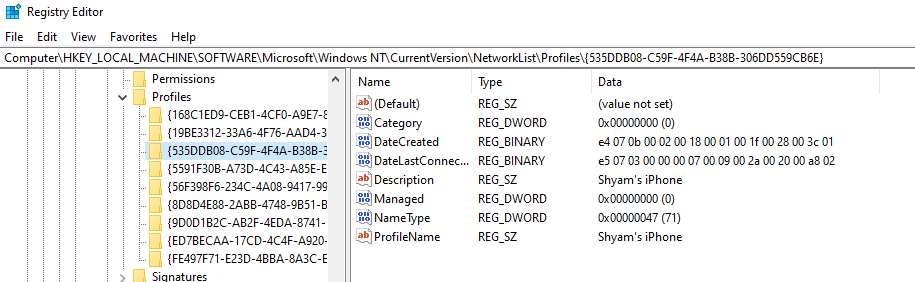


**OBSERVATIONS**

**List of GUIDs of Wireless access points connected**

**Path:** Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\

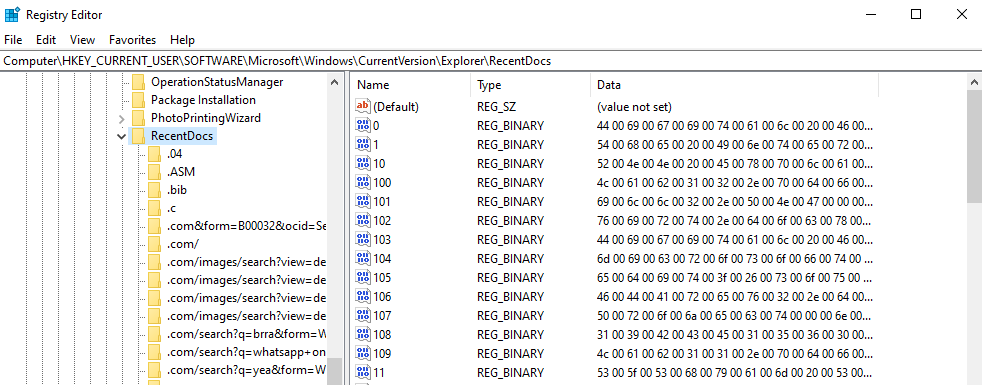




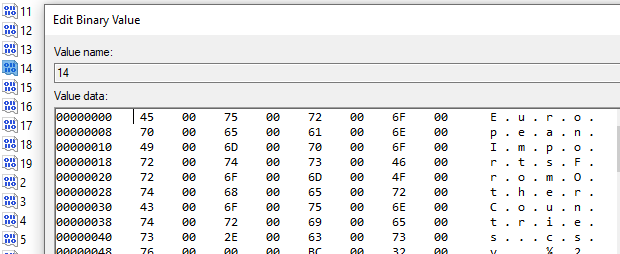
It shows the list of networks connected to in the past in folders. In the screenshot we see that one of the networks was an iPhone’s hotspot.

**Recent Documents**

**Path:** Computer\HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



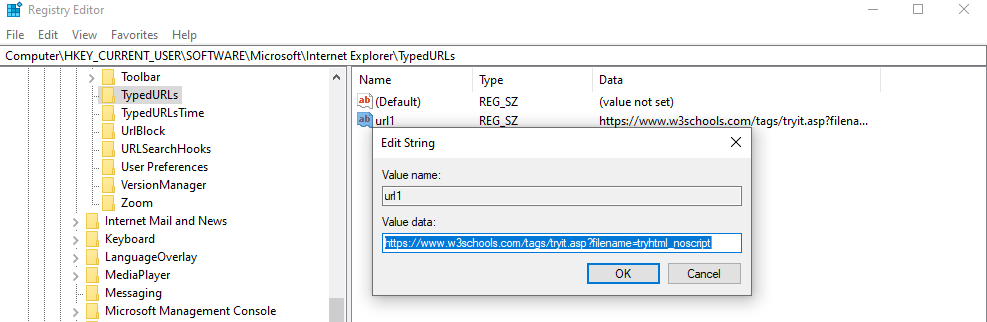
We can see a list of file types, each containing details of files accessed. We can also see the names. For example, below is an entry with the name of the CSV file accessed in the rightmost column.



It reads ‘EuropeanImportsFromOtherCountries’. This is a CSV file used for FDA lab.

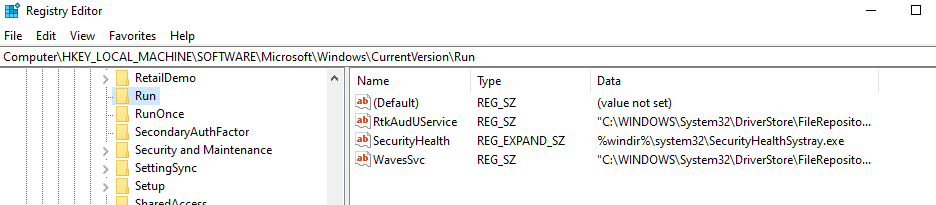
**URLS typed in internet explorer**

**Path:** Computer\HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Internet Explorer\TypedURLs



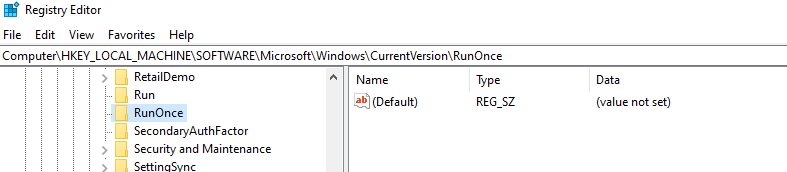
**Applications Run when system starts**

**Path:** Computer\HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run



**Applications Run Once**

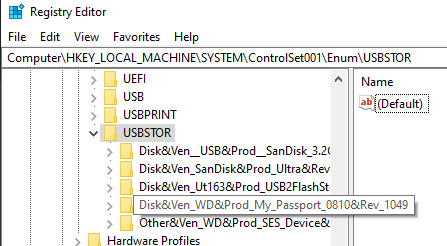
**Path:** Computer\HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce



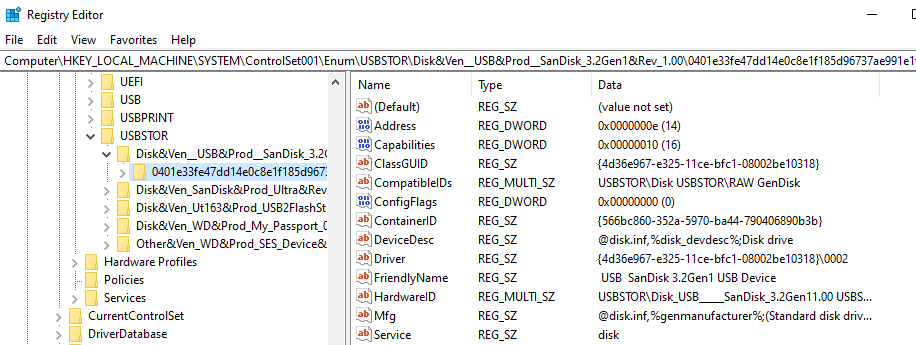
There are no such applications.

**Check if USB was inserted**

**Path:** Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR

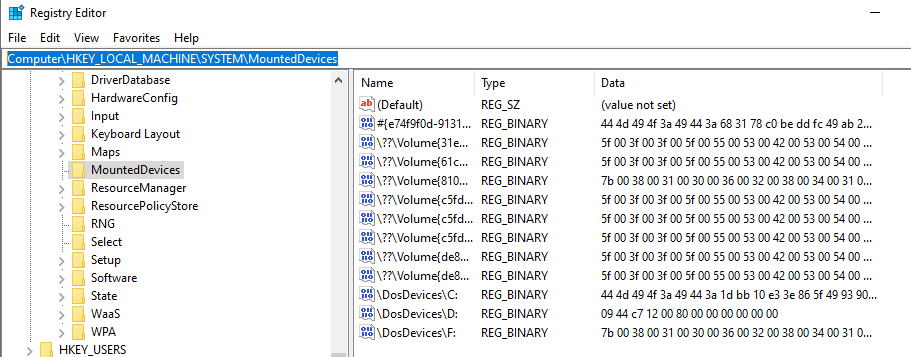


Each device inserted has its own sub-folder. The contents of one of them are shown below:



**Check for devices that were mounted**

**Path:** Computer\HKEY\_LOCAL\_MACHINE\SYSTEM\MountedDevices



**CONCLUSION**

Thus, we have seen a handful of samples regarding the kinds of information that can be extracted about a device from its registry.