**Name-** Jayant**a** Ghosh

**Roll no -**190112

**Access and extract relevant information from Windows Registry for investigation process using Registry View, perform data analysis and bookmark the findings with respect to:**

**(i) Computer System; (ii) Computer Network**

**Procedure:**

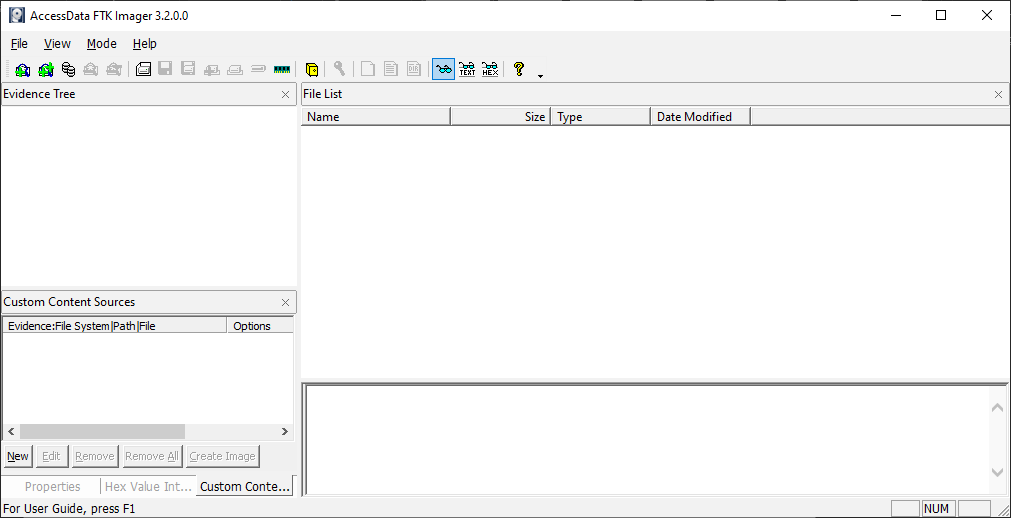
1. Registry Files Acquisition

First, we need to acquire the Image of the Registry files using the tool FTK Imager.

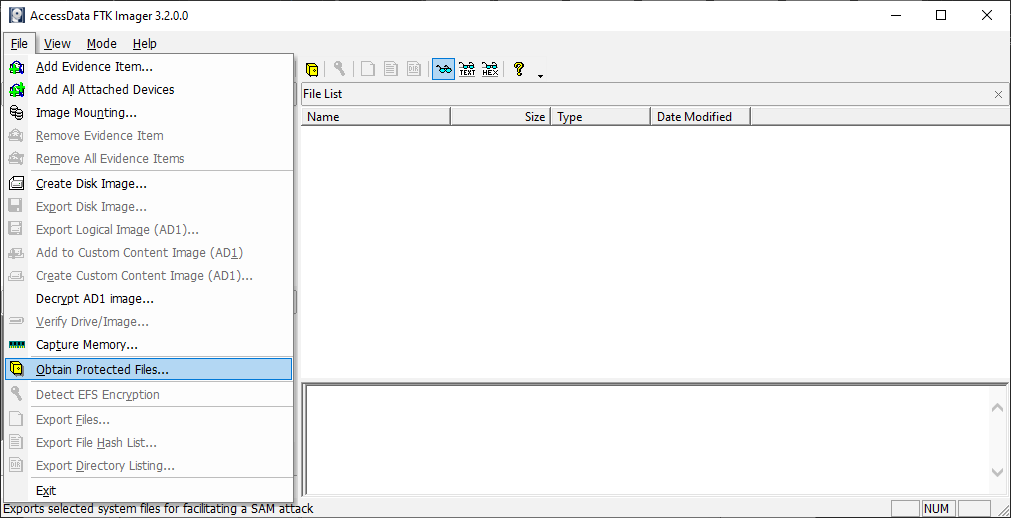
**Step 1:**

Download & Install FTK Imager from Access Data.

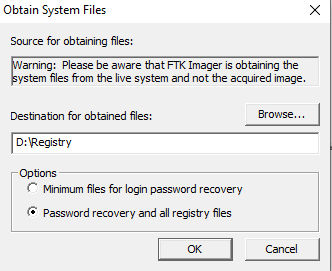
Open FTK Imager.



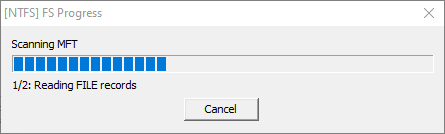
Click on File >> Obtain Protected Files.



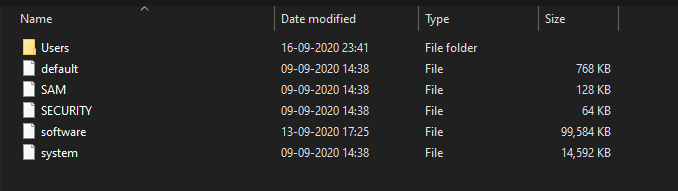
Next, select the Folder to save your image of the Registry and choose Password Recovery and all Registry Files for backup and click OK.



The backup process will start as follows:



Now, your registry is saved to your specified directory.



1. Registry Files Analysis

**Open Registry Viewer.**

Click on File >> Open >> Select the Registry Files that had previously created an image of for further analysis of the Registry.

A) Computer Investigation:

Following are some registry keys of forensic value

1)NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePidMRU

MRU is the abbreviation for most-recently-used. This key maintains a list of recently opened or saved files via typical Windows Explorer-style common dialogue boxes.

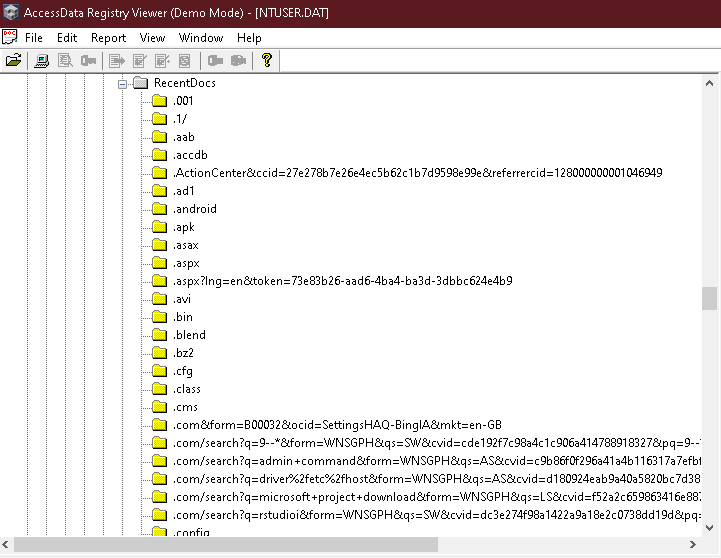


2) NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRu

This key maintains a list of entries (e.g. full file path or commands like cmd, regedit, compmgmt.msc) executed using the start>run command.

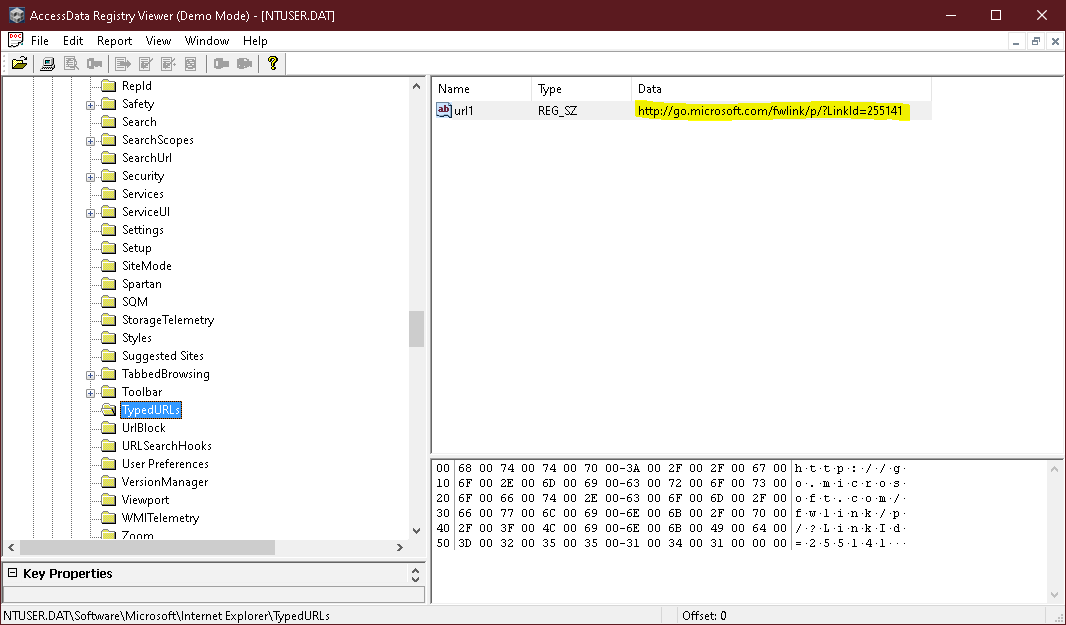
3) NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\

This key shows the recent documents that were opened.



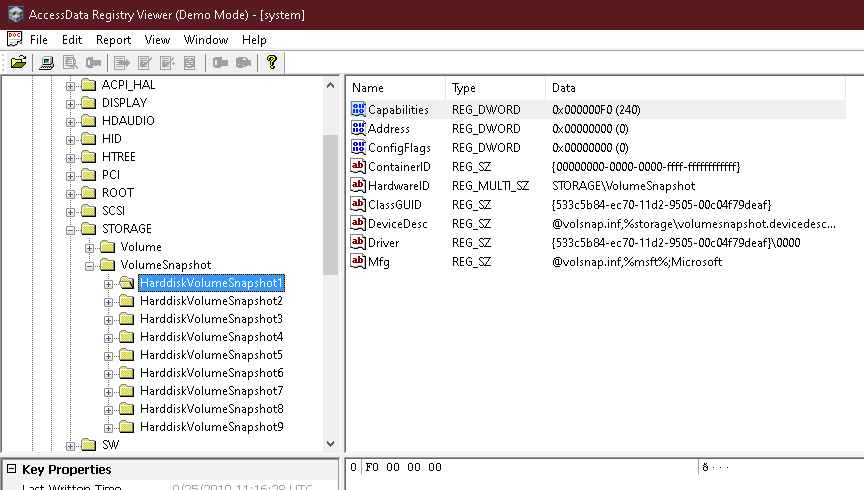
4) NTUSER.DAT\Software\Microsoft\ Internet Explorer\TypedURLs\

This key shows the typed URLs in Internet Explorer



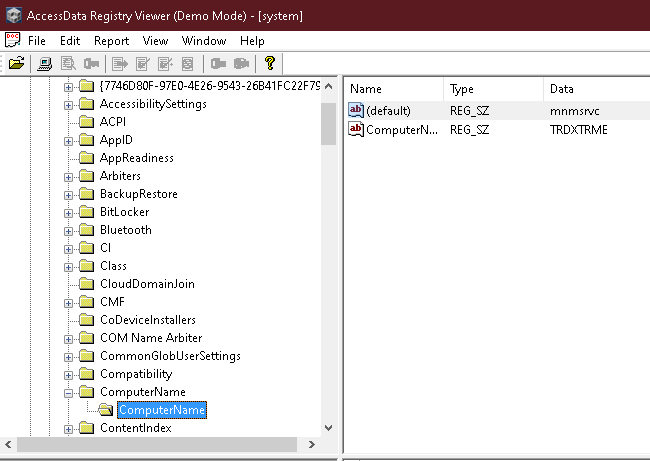
5) SYSTEM\ControlSet001\ Enum\STORAGE\VolumnSnapShot

Keeps a snapshot of hard drive storage.



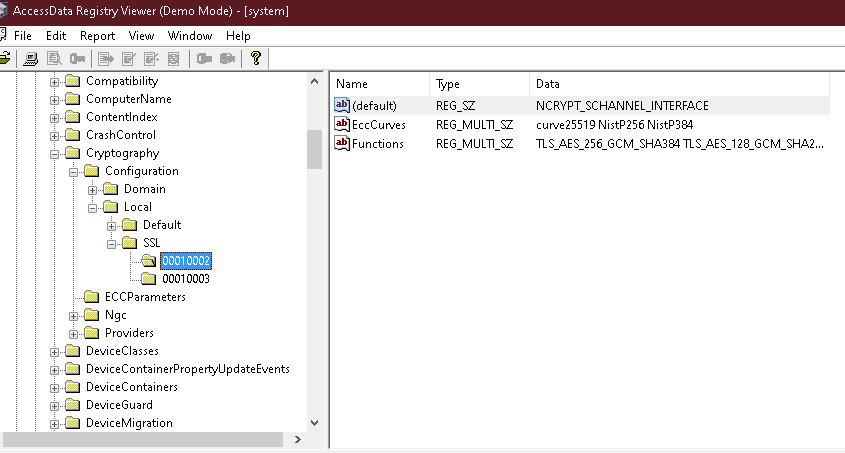
6) SYSTEM\ControlSet001\Control\ComputerName

To get computer system name



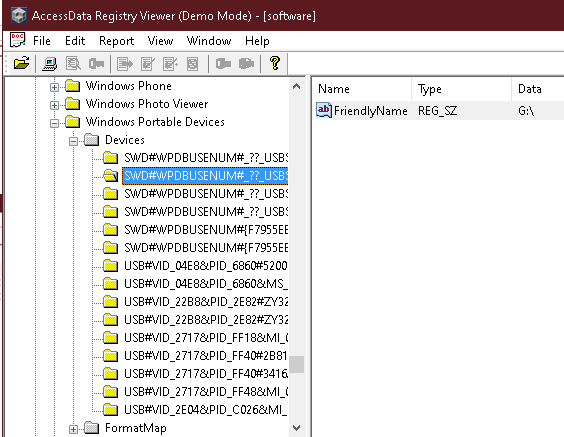
7) SYSTEM\ControlSet001\Control\Cryptography\Local

To get Cryptography description of System



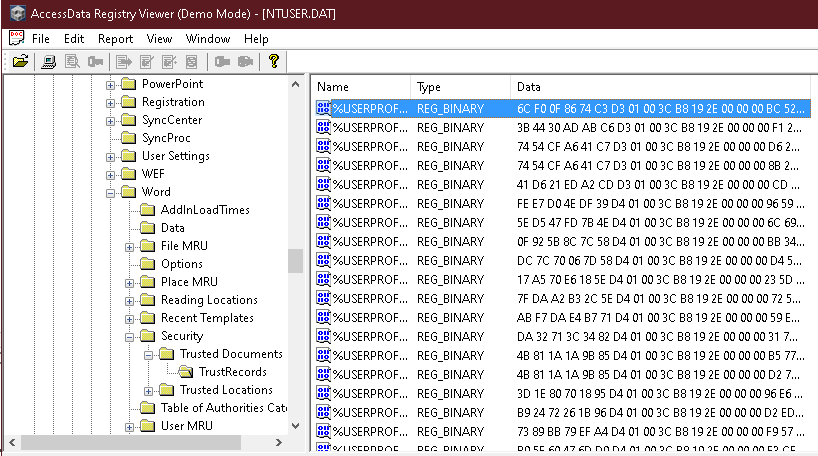
8) SOFTWARE\Microsoft\Windows Portable Devices\Devices

to display any portable device attached to the system .



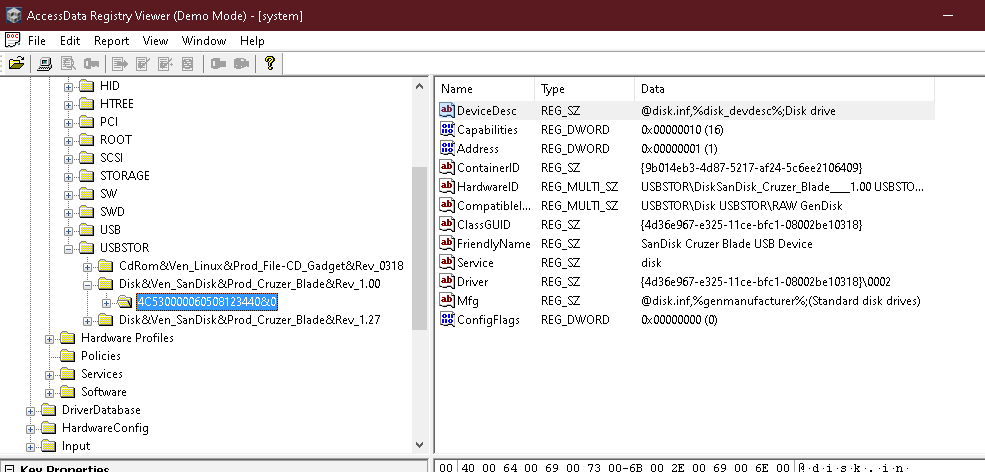
9) NTUSER.DAT\SOFTWARE\Microsoft\Office\15.0\Word\Security\Trusted Documents\TrustRecords

Trusted Documents



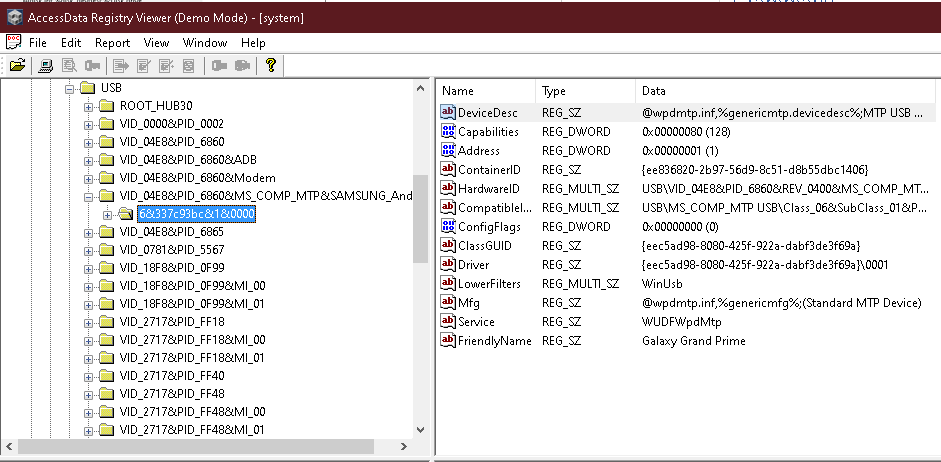
10) SYSTEM\ControlSet001\ Enum\USBSTOR

to search any attached USB storage device attached to system.



11) SYSTEM\ControlSet001\Control\Enum\USB\

Have set key for all connected device through USB port.

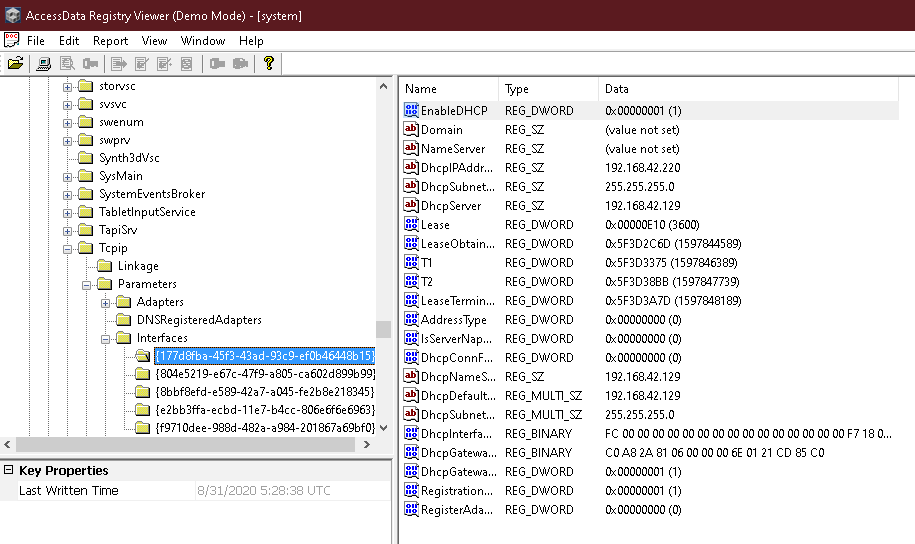


B) Computer Network.

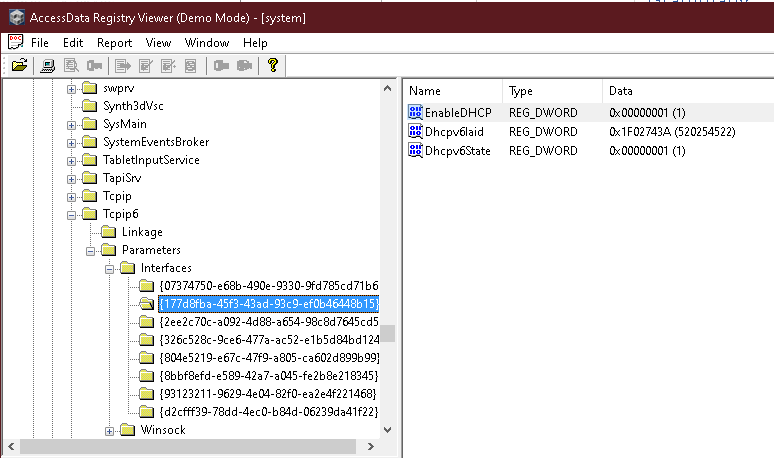
1)SYSTEM\ControlSet001\ Services\Tcpip\Parameters\Interfaces\

TCPIP Data, Domain Names, Internet Connection Info

addition to logging the name of the SSID, Windows also logs the network settings of that particular connection - such as the IP address, DHCP domain, subnet mask, etc.

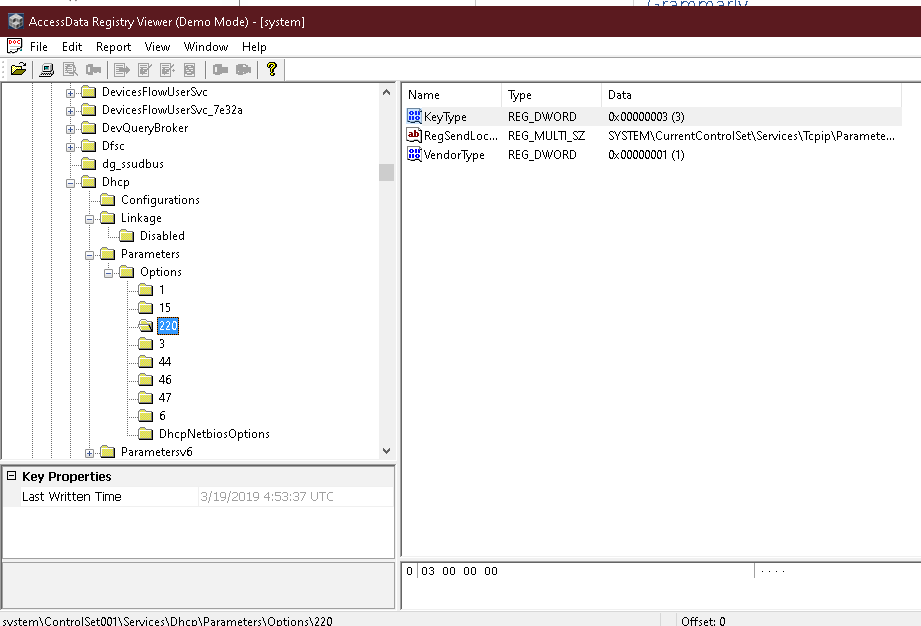


2) SYSTEM\ControlSet001\ Services\Tcpip6\Parameters\Interfaces\



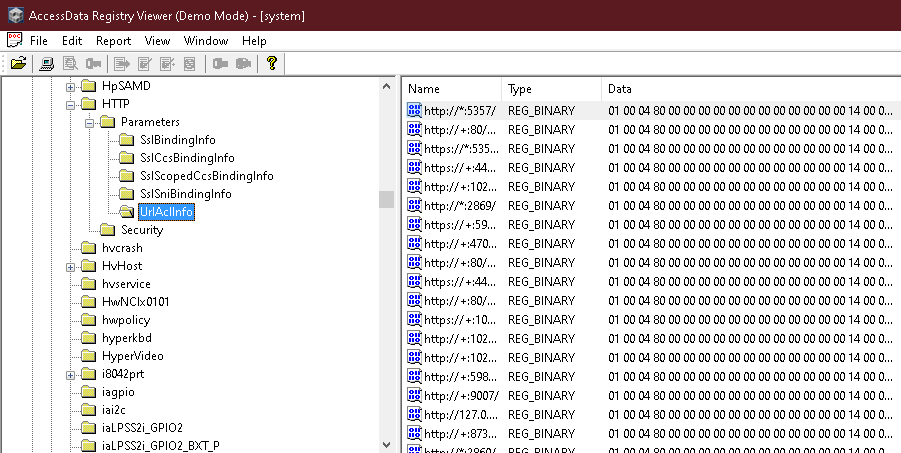
3) SYSTEM\ControlSet001\ Services\Dhcp

To View DHCP configuration



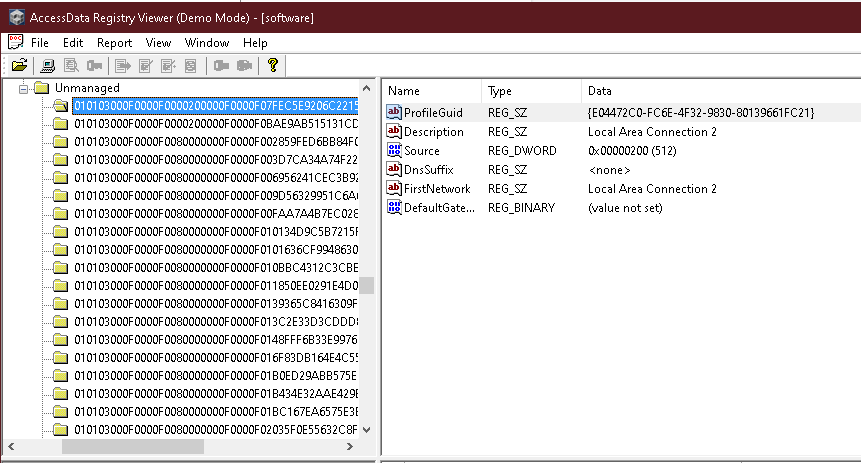
4) SYSTEM\ControlSet001\ Services\HTTP

Key consist of http transaction detail including ssl info



5) SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged

Has information about different network connection established on system



6) NTUSER.DAT\Software\Google\ Update\ClientState\{8A69D345- D564-463c-AFF1-A69D9Ec-AFF1-A69D9E530F96} / lastrun

This key has Google Chrome Last Browser Run Time

