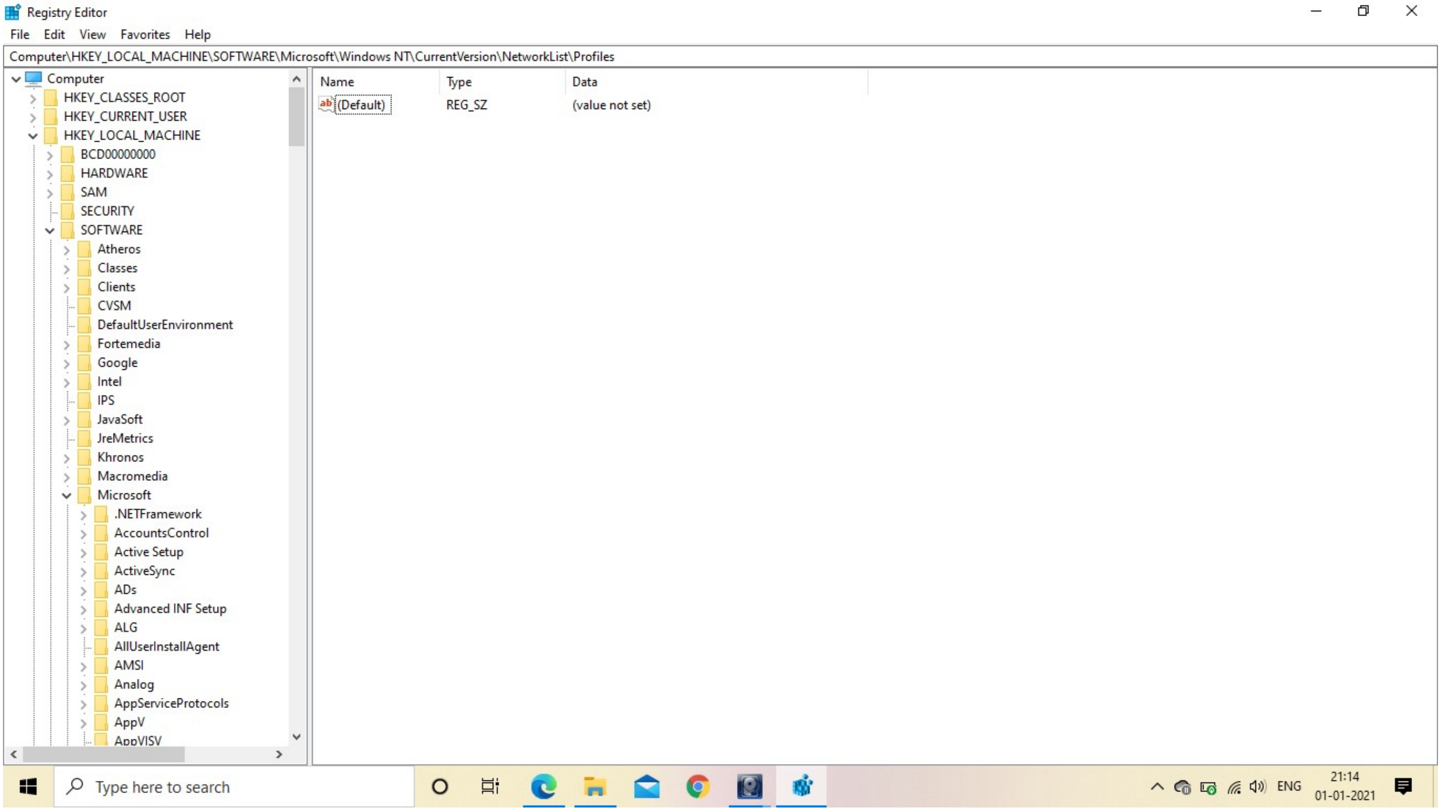
Practical No :9

Aim:Registry Editor

Type regedit in Start->Search

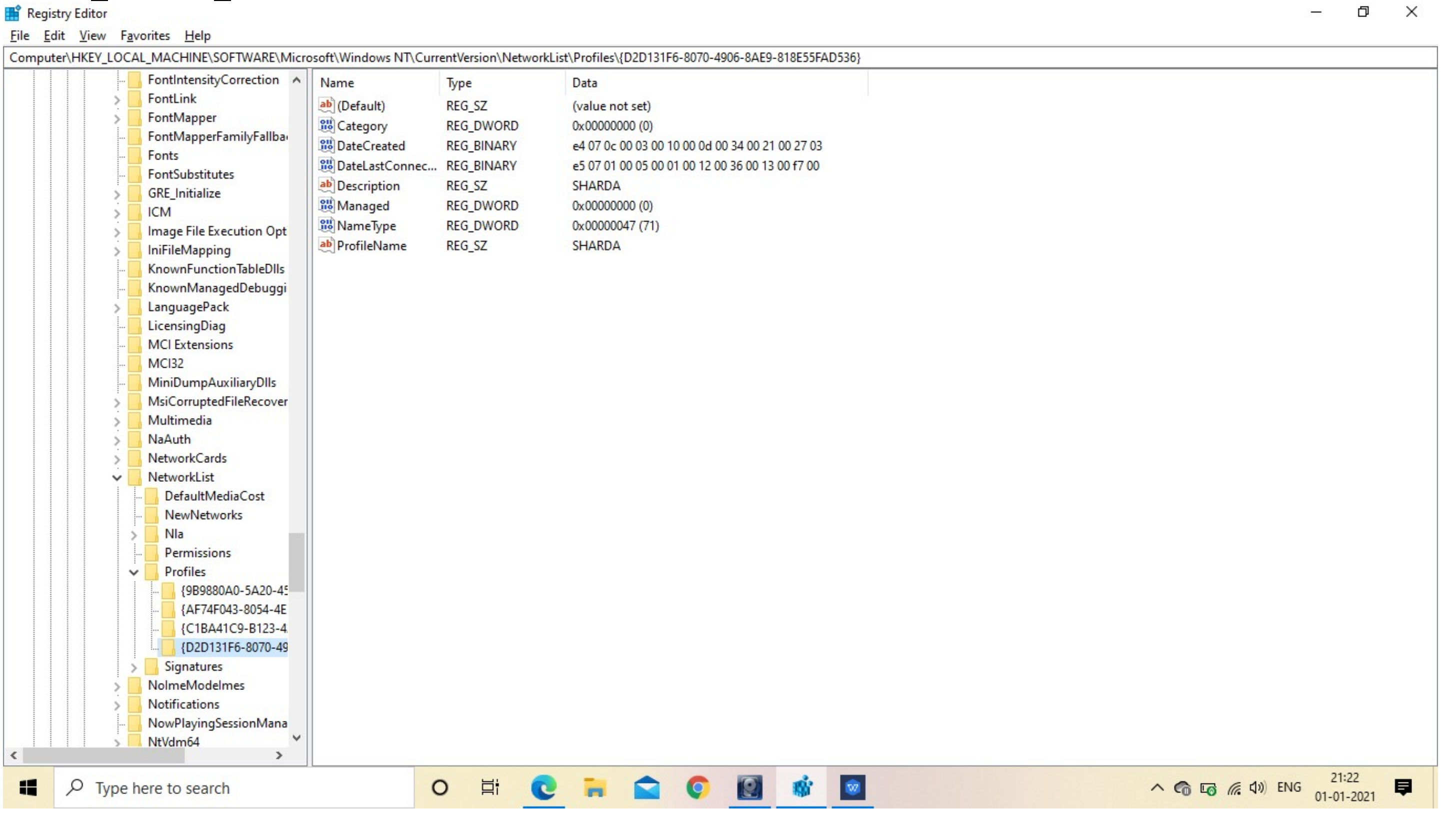


Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

Name	Type	Data
(Default)	REG_SZ	(value not set)

Wireless Evidence in the Registry

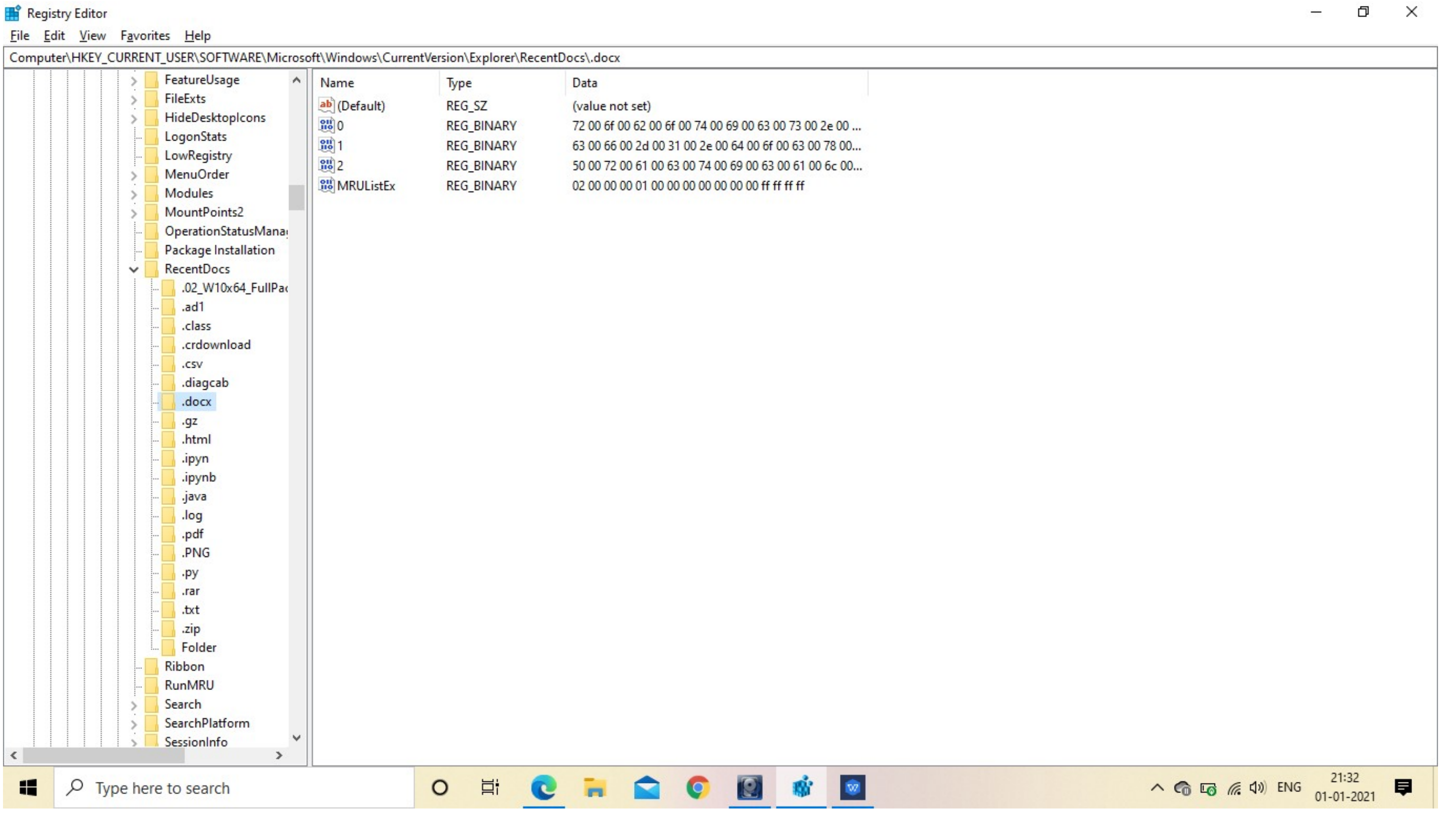
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\{D2D131F6-8070-4906-8AE9-818E55FAD536}

Name	Type	Data
(Default)	REG_SZ	(value not set)
Category	REG_DWORD	0x00000000 (0)
DateCreated	REG_BINARY	e4 07 0c 00 03 00 10 00 0d 00 34 00 21 00 27 03
DateLastConnec...	REG_BINARY	e5 07 01 00 05 00 01 00 12 00 36 00 13 00 f7 00
Description	REG_SZ	SHARDA
Managed	REG_DWORD	0x00000000 (0)
NameType	REG_DWORD	0x00000047 (71)
ProfileName	REG_SZ	SHARDA

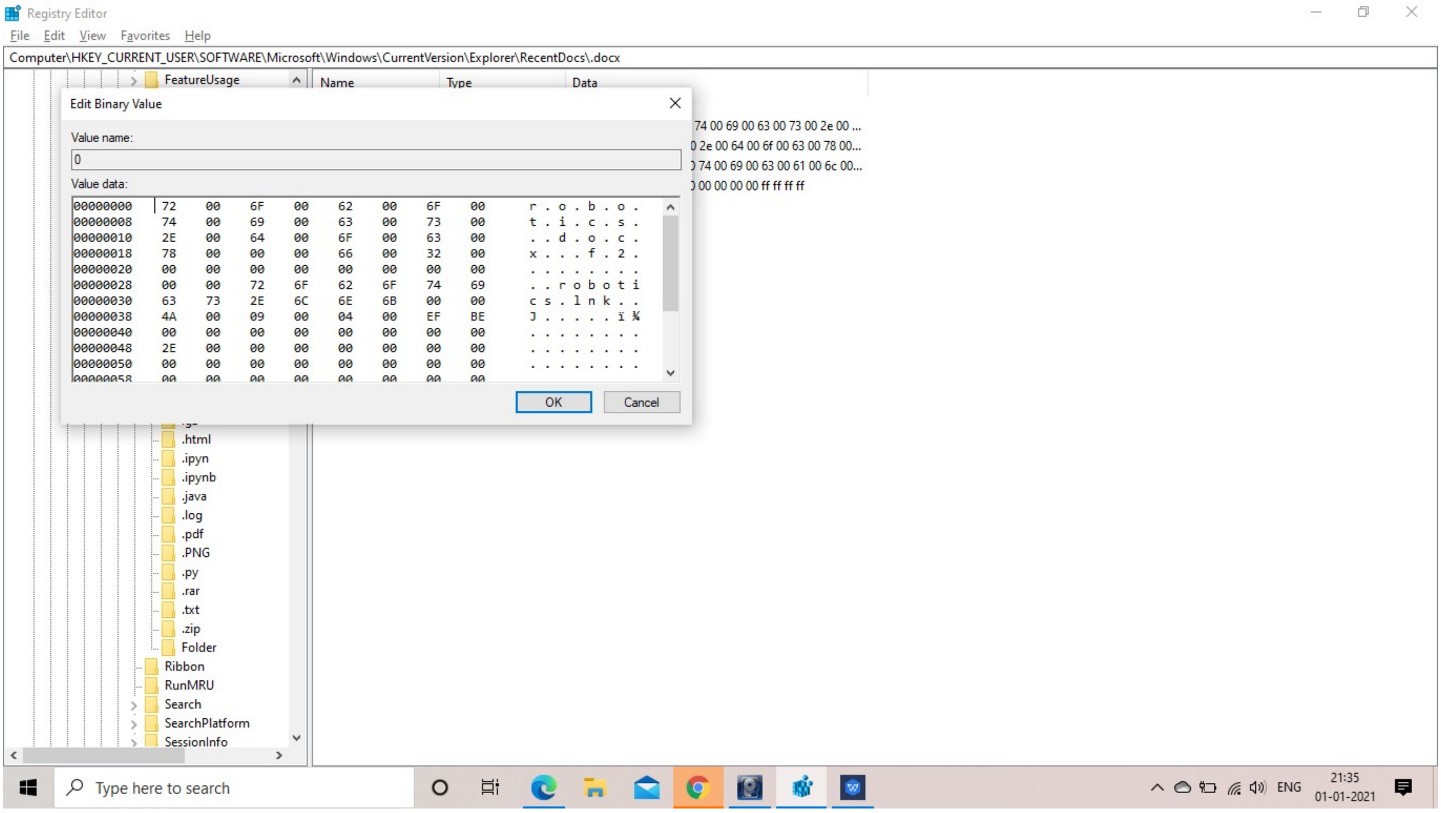
The RecentDocs Key
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx

Name	Type	Data
(Default)	REG_SZ	(value not set)
0	REG_BINARY	72 00 6f 00 62 00 6f 00 74 00 69 00 63 00 73 00 2e 00 ...
1	REG_BINARY	63 00 66 00 2d 00 31 00 2e 00 64 00 6f 00 63 00 78 00...
2	REG_BINARY	50 00 72 00 61 00 63 00 74 00 69 00 63 00 61 00 6c 00...
MRUListEx	REG_BINARY	02 00 00 00 01 00 00 00 00 00 00 00 ff ff ff ff

Click on any of the file



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.docx

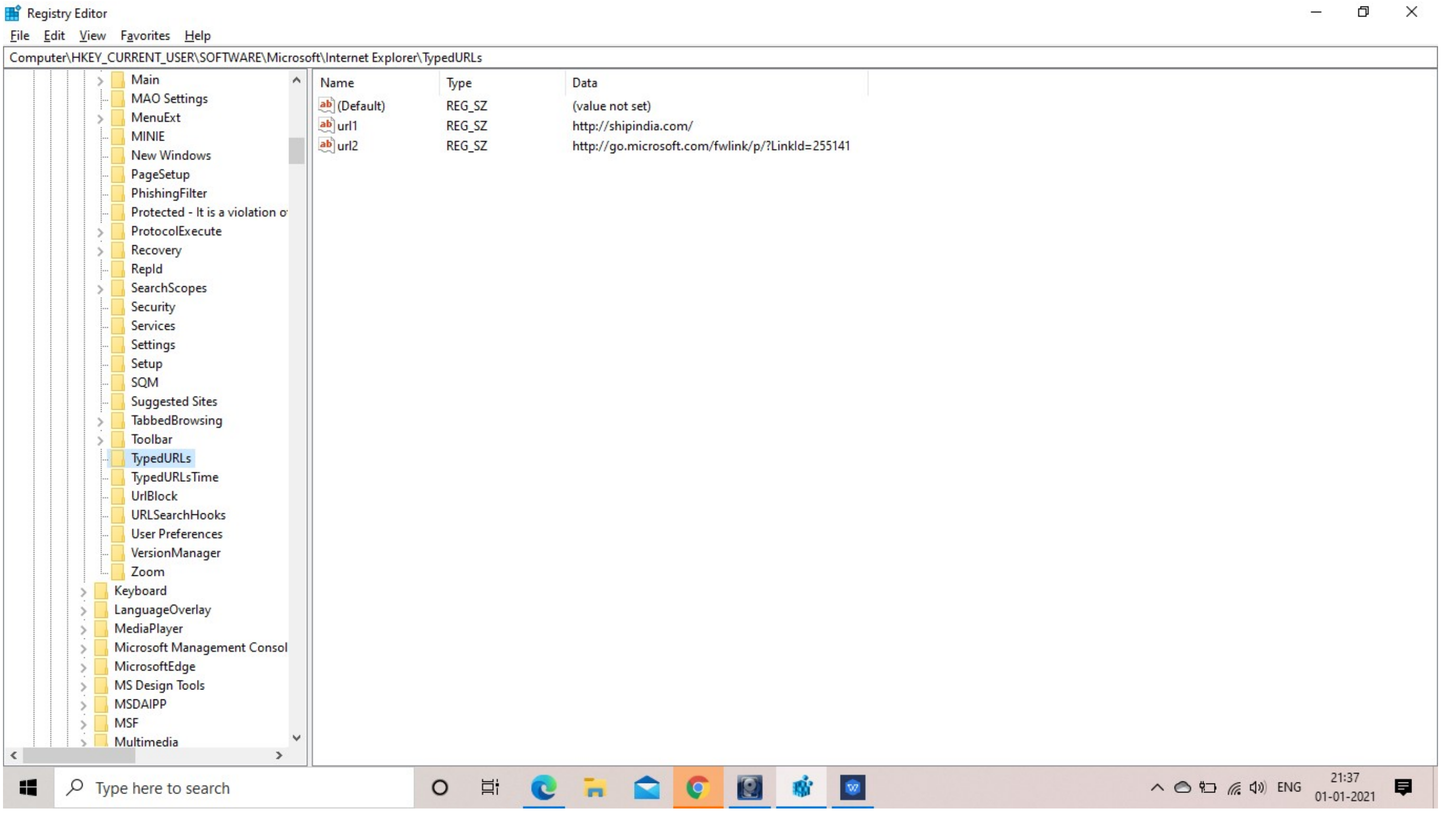
Value name: 0

Value data:

```
00000000   72  00  6F  00  62  00  6F  00    r . o . b . o .
00000008   74  00  69  00  63  00  73  00    t . i . c . s .
00000010   2E  00  64  00  6F  00  63  00    . . d . o . c .
00000018   78  00  00  00  66  00  32  00    x . . . f . 2 .
00000020   00  00  00  00  00  00  00  00    . . . . . . . .
00000028   00  00  72  6F  62  6F  74  69    . . r o b o t i
00000030   63  73  2E  6C  6E  6B  00  00    c s . l n k . .
00000038   4A  00  09  00  04  00  EF  BE    J . . . . . ï ¾
00000040   00  00  00  00  00  00  00  00    . . . . . . . .
00000048   2E  00  00  00  00  00  00  00    . . . . . . . .
00000050   00  00  00  00  00  00  00  00    . . . . . . . .
00000058   00  00  00  00  00  00  00  00
```

74 00 69 00 63 00 73 00 2e 00 ...
0 2e 00 64 00 6f 00 63 00 78 00...
0 74 00 69 00 63 00 61 00 6c 00...
0 00 00 00 00 ff ff ff ff

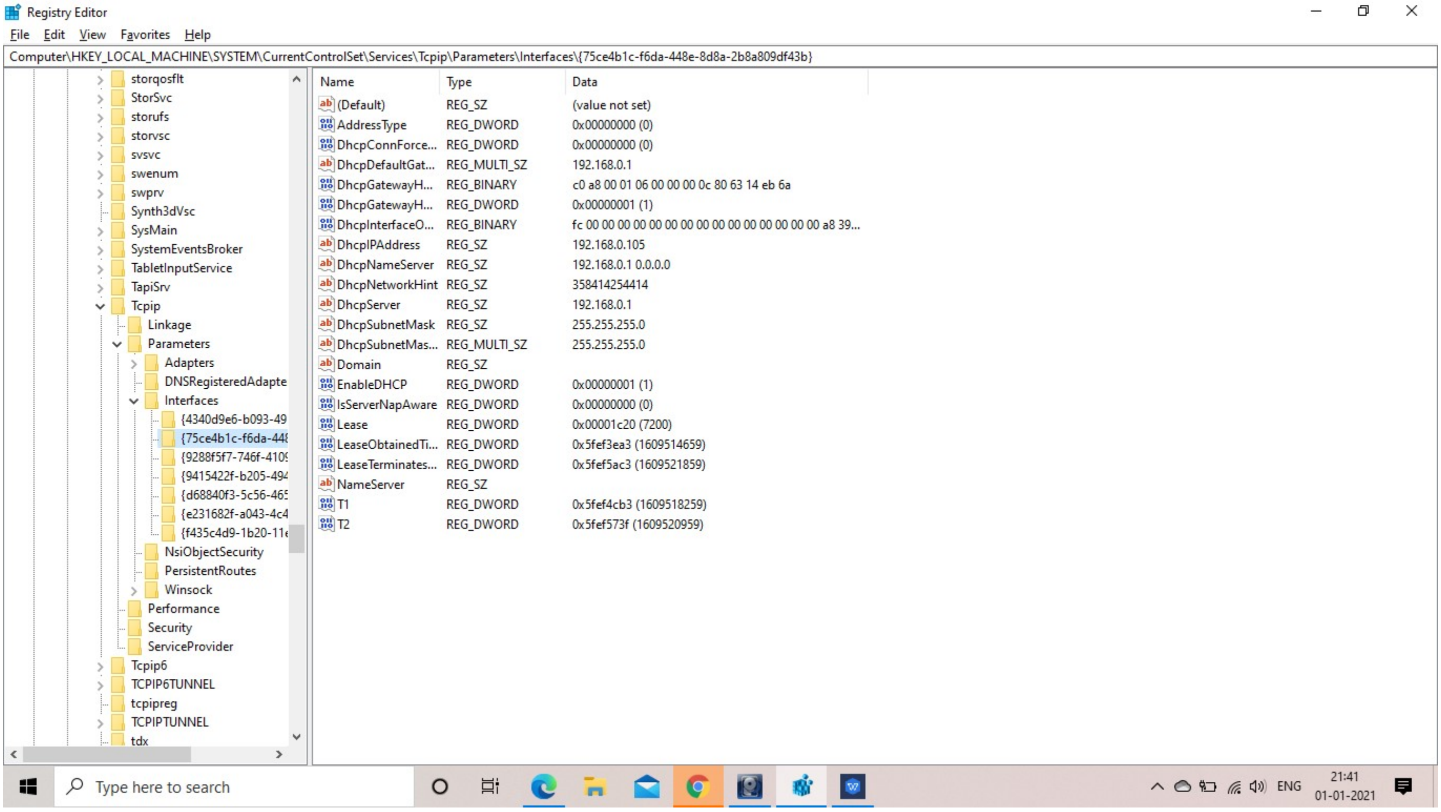
Typed URLs Key
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs



Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\TypedURLs

Name	Type	Data
(Default)	REG_SZ	(value not set)
url1	REG_SZ	http://shipindia.com/
url2	REG_SZ	http://go.microsoft.com/fwlink/p/?LinkId=255141

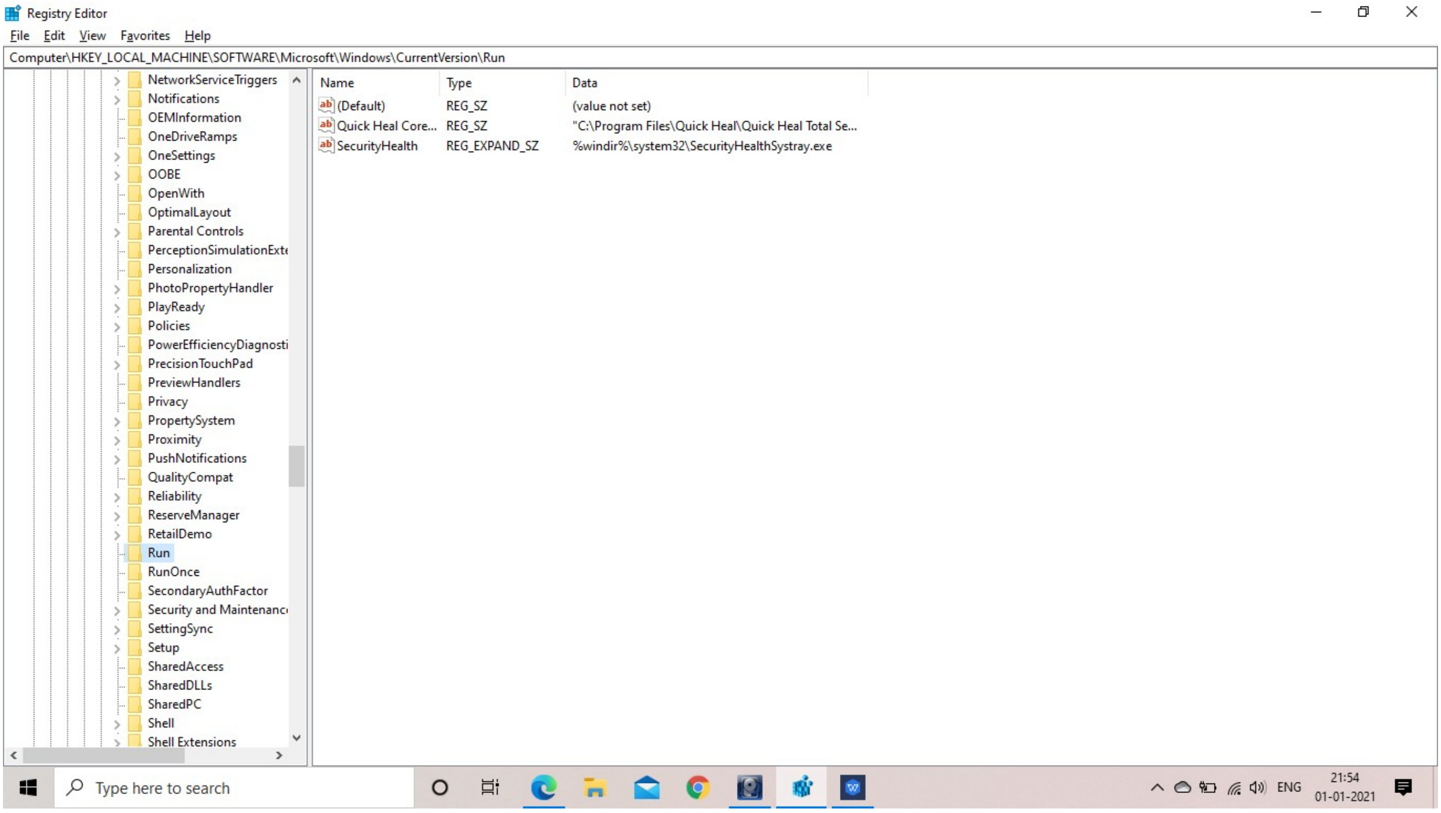
IP Addresses
HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Tcpip\Parameters\Interface



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{75ce4b1c-f6da-448e-8d8a-2b8a809df43b}

Name	Type	Data
(Default)	REG_SZ	(value not set)
AddressType	REG_DWORD	0x00000000 (0)
DhcpConnForce...	REG_DWORD	0x00000000 (0)
DhcpDefaultGat...	REG_MULTI_SZ	192.168.0.1
DhcpGatewayH...	REG_BINARY	c0 a8 00 01 06 00 00 00 0c 80 63 14 eb 6a
DhcpGatewayH...	REG_DWORD	0x00000001 (1)
DhcpInterfaceO...	REG_BINARY	fc 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a8 39...
DhcpIPAddress	REG_SZ	192.168.0.105
DhcpNameServer	REG_SZ	192.168.0.1 0.0.0.0
DhcpNetworkHint	REG_SZ	358414254414
DhcpServer	REG_SZ	192.168.0.1
DhcpSubnetMask	REG_SZ	255.255.255.0
DhcpSubnetMas...	REG_MULTI_SZ	255.255.255.0
Domain	REG_SZ	
EnableDHCP	REG_DWORD	0x00000001 (1)
IsServerNapAware	REG_DWORD	0x00000000 (0)
Lease	REG_DWORD	0x00001c20 (7200)
LeaseObtainedTi...	REG_DWORD	0x5fef3ea3 (1609514659)
LeaseTerminates...	REG_DWORD	0x5fef5ac3 (1609521859)
NameServer	REG_SZ	
T1	REG_DWORD	0x5fef4cb3 (1609518259)
T2	REG_DWORD	0x5fef573f (1609520959)

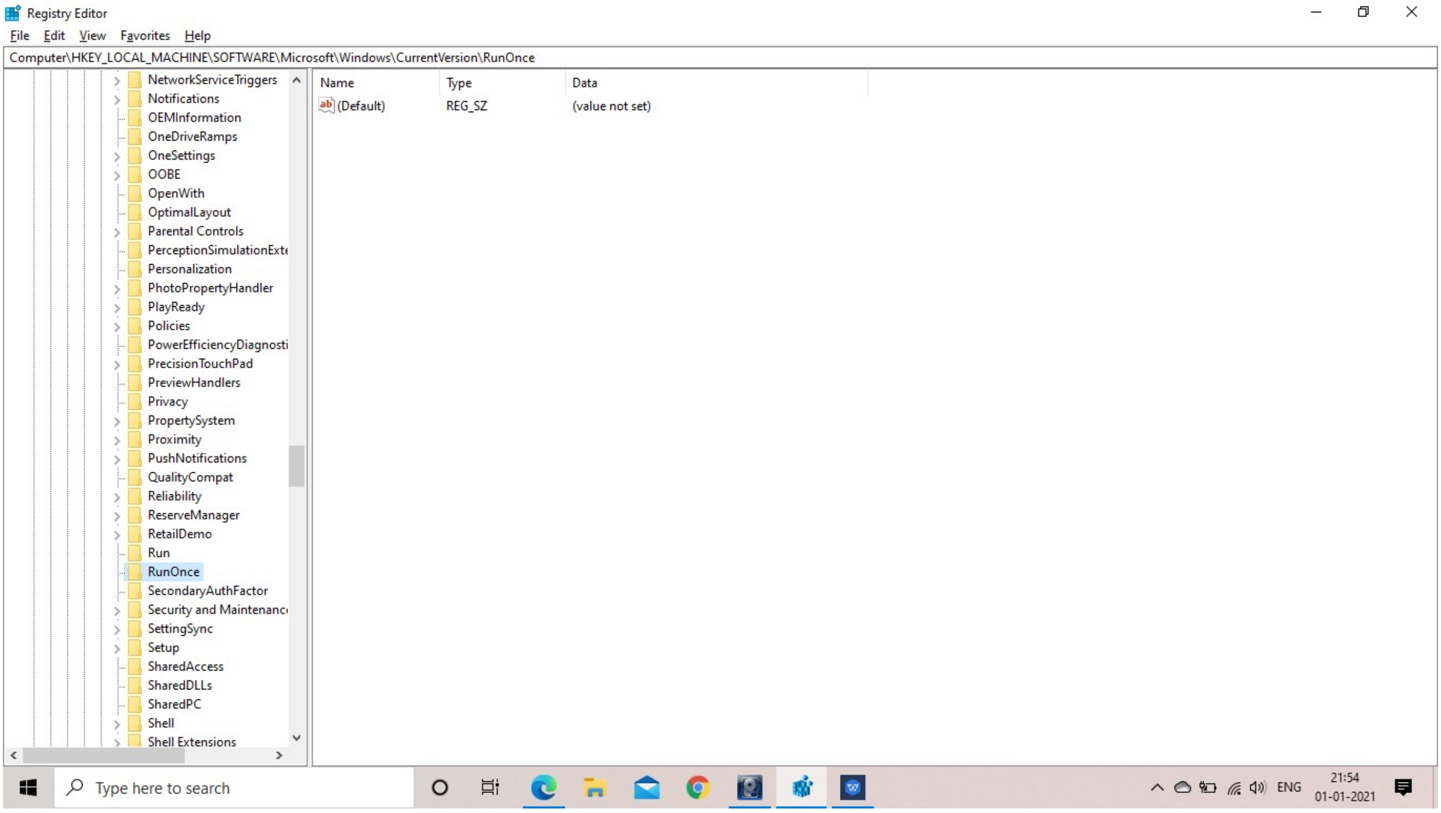
Start Up Locations in the Registry
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
Quick Heal Core...	REG_SZ	"C:\Program Files\Quick Heal\Quick Heal Total Se...
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe

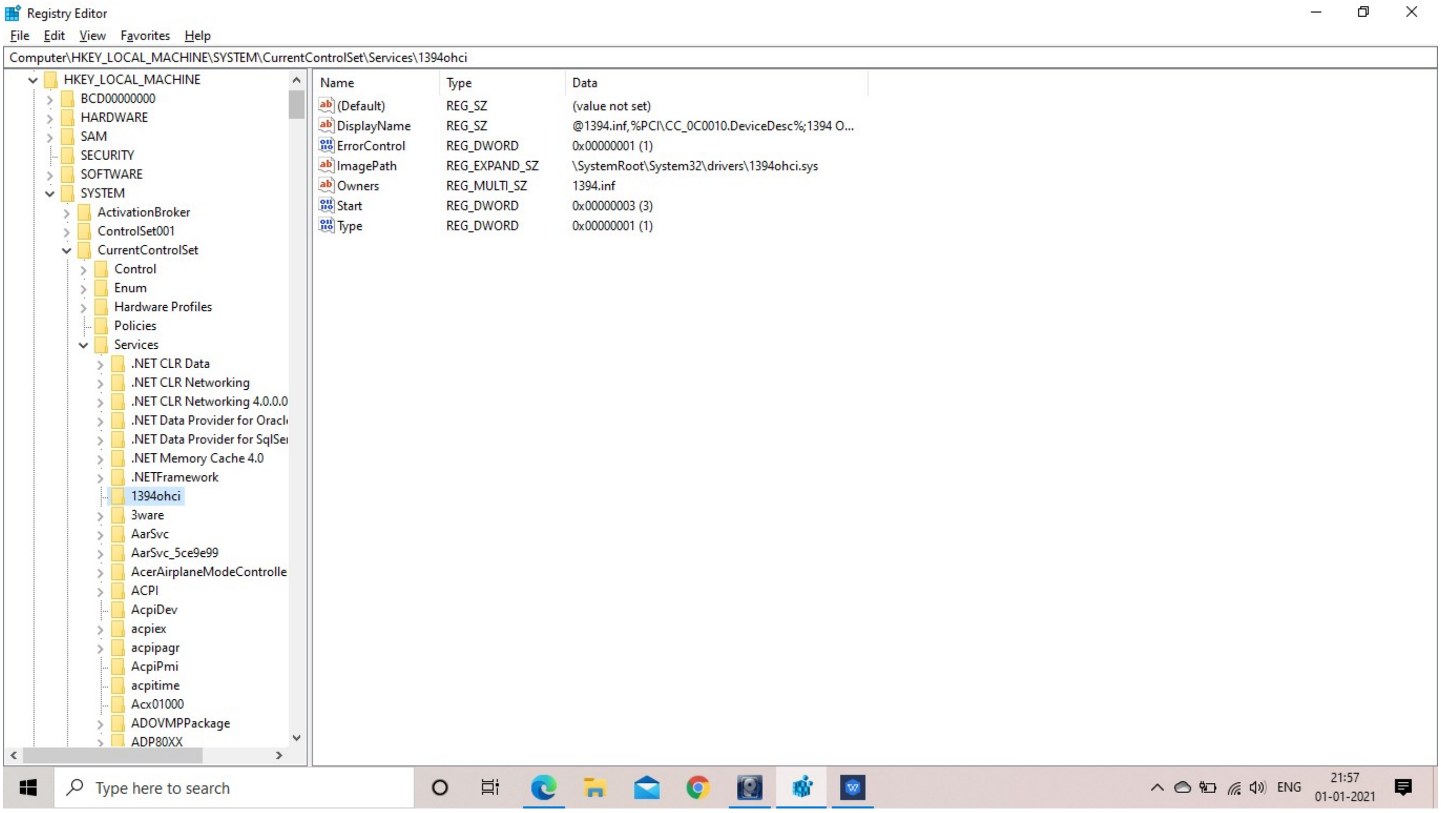
RunOnce Startup
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Name	Type	Data
(Default)	REG_SZ	(value not set)

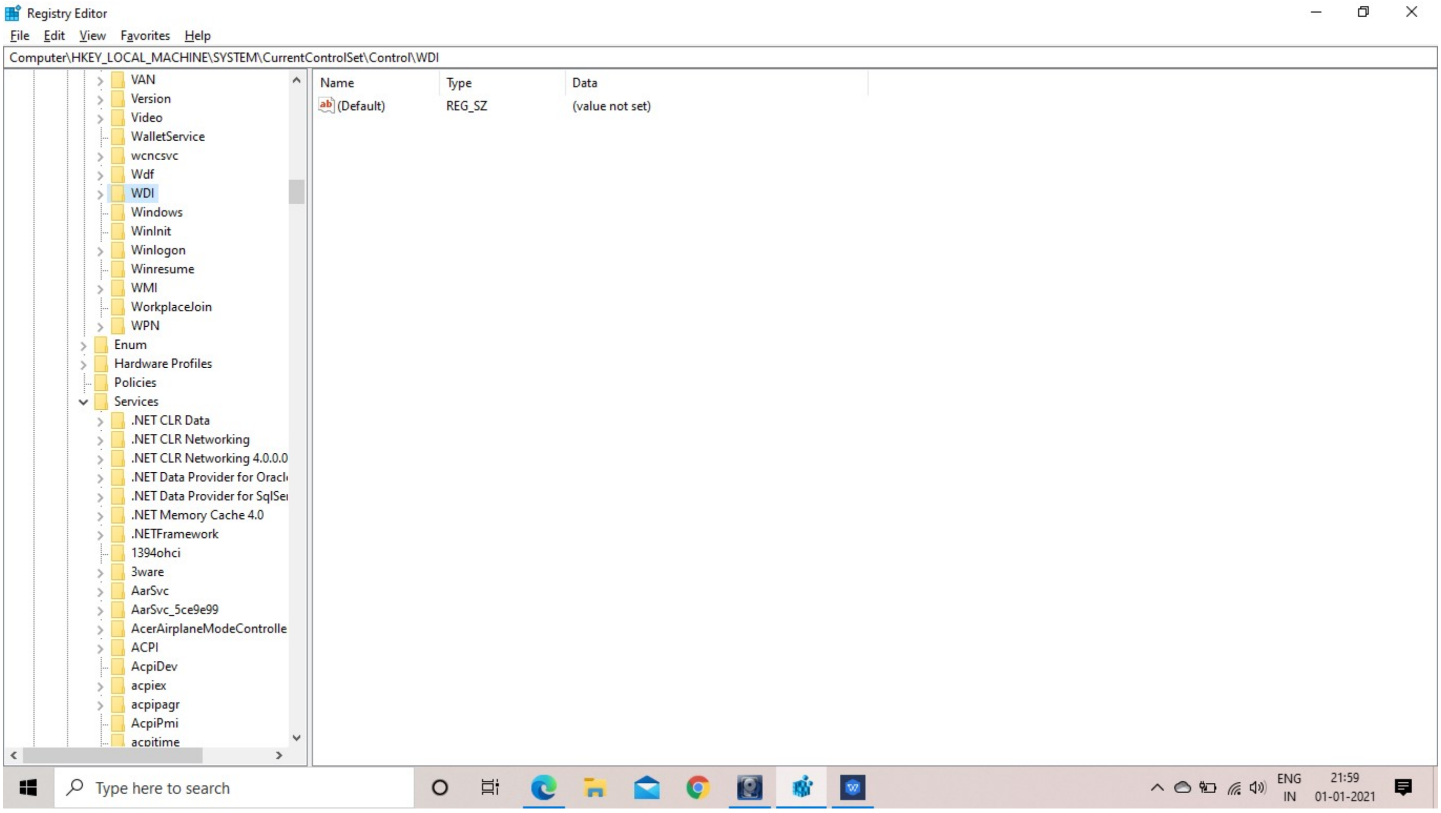
Start Up Services
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\1394ohci

Name	Type	Data
(Default)	REG_SZ	(value not set)
DisplayName	REG_SZ	@1394.inf,%PCI\CC_0C0010.DeviceDesc%;1394 O...
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	\SystemRoot\System32\drivers\1394ohci.sys
Owners	REG_MULTI_SZ	1394.inf
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000001 (1)

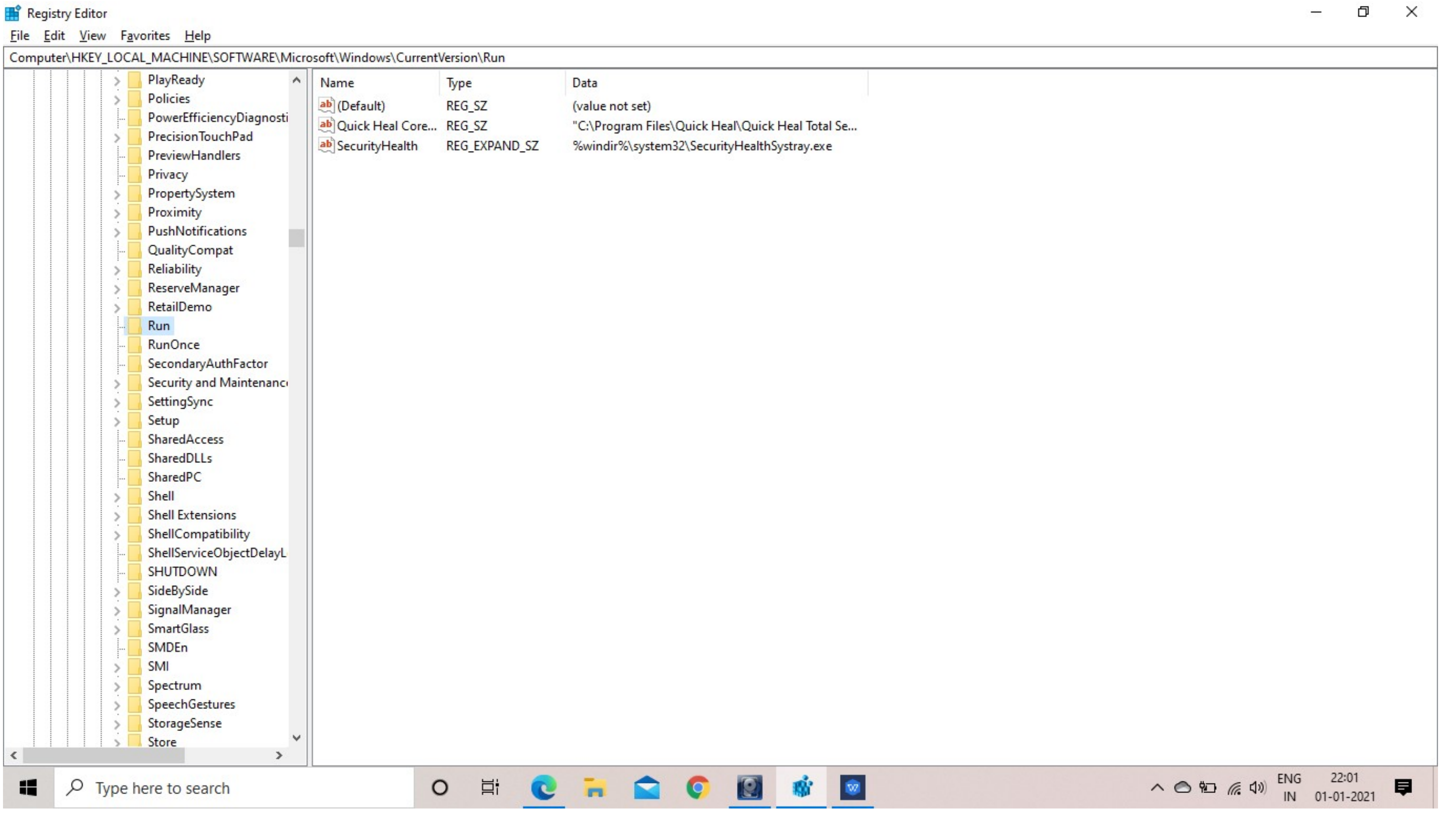
Start Legacy Applications
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\WDI



Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WDI

Name	Type	Data
(Default)	REG_SZ	(value not set)

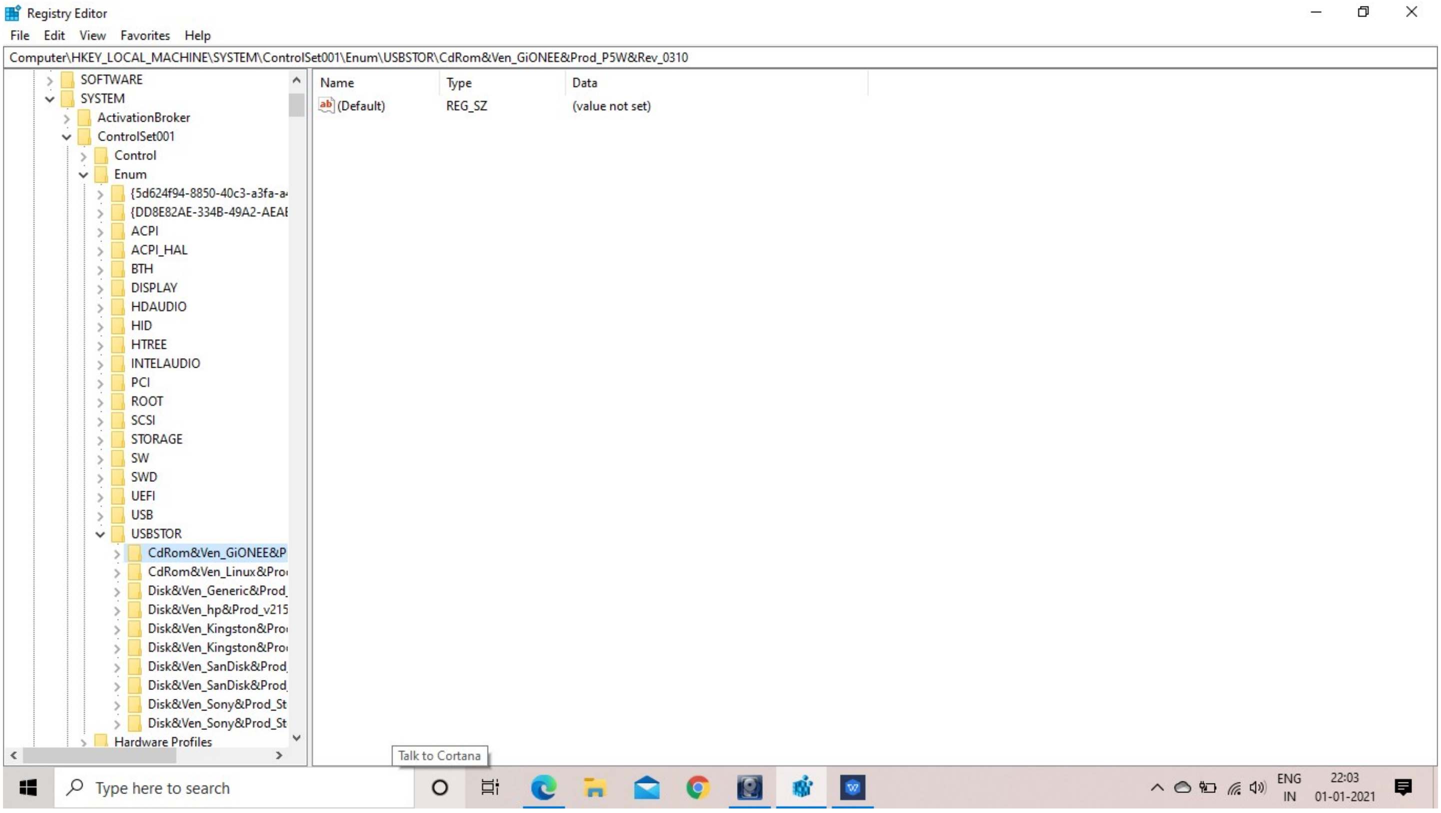
Start When a Particular User Logs On
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
Quick Heal Core...	REG_SZ	"C:\Program Files\Quick Heal\Quick Heal Total Se...
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe

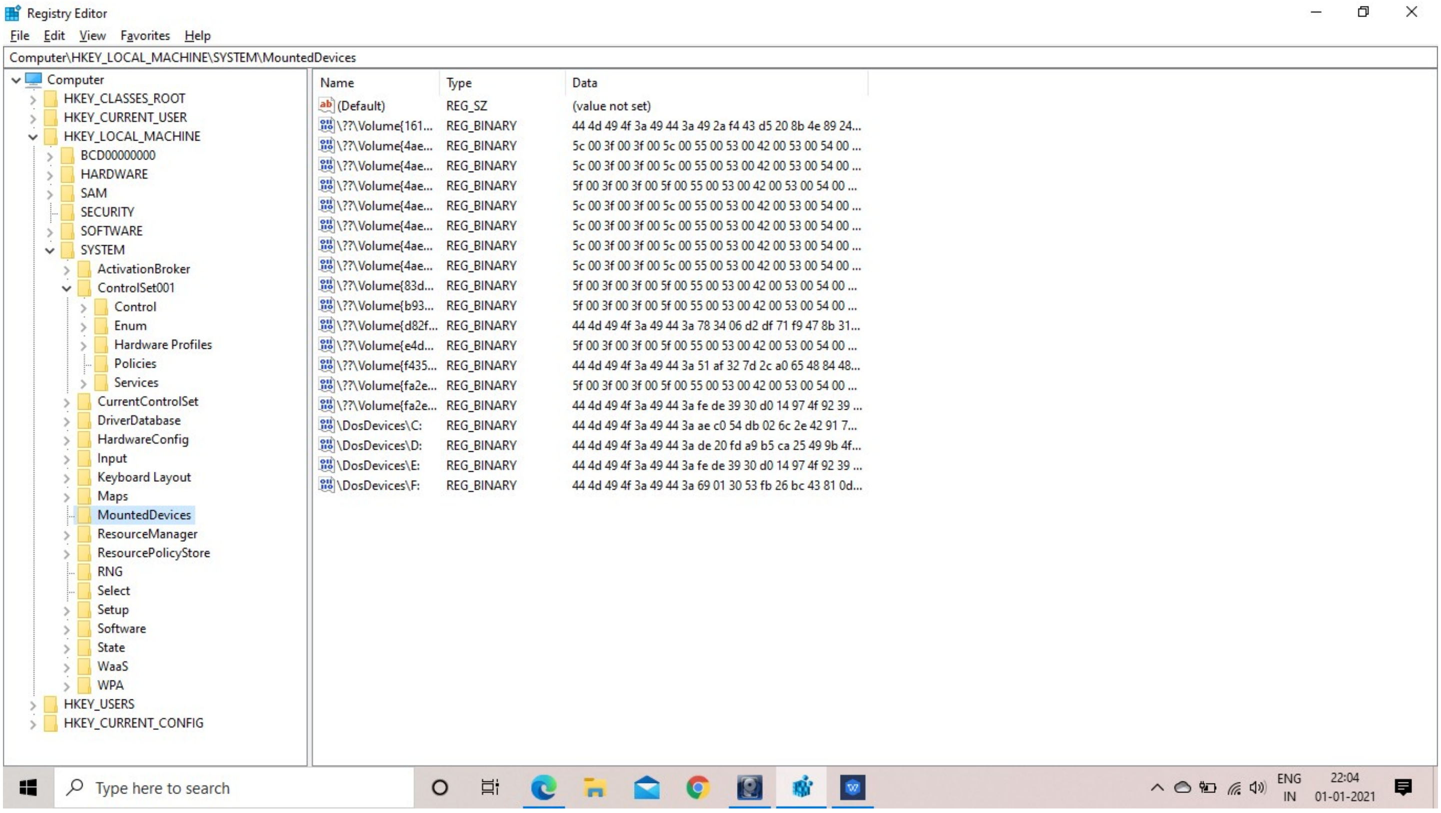
USB Storage Devices
HK_Local_Machine\System\ControlSet00x\Enum\USBSTOR



Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\CdRom&Ven_GiONEE&Prod_P5W&Rev_0310

Name	Type	Data
(Default)	REG_SZ	(value not set)

Mounted Devices
HKEY_LOCAL_MACHINE\System\MountedDevices



Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

Name	Type	Data
(Default)	REG_SZ	(value not set)
\??\Volume{161...	REG_BINARY	44 4d 49 4f 3a 49 44 3a 49 2a f4 43 d5 20 8b 4e 89 24...
\??\Volume{4ae...	REG_BINARY	5c 00 3f 00 3f 00 5c 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{4ae...	REG_BINARY	5c 00 3f 00 3f 00 5c 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{4ae...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{4ae...	REG_BINARY	5c 00 3f 00 3f 00 5c 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{4ae...	REG_BINARY	5c 00 3f 00 3f 00 5c 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{4ae...	REG_BINARY	5c 00 3f 00 3f 00 5c 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{4ae...	REG_BINARY	5c 00 3f 00 3f 00 5c 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{83d...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{b93...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{d82f...	REG_BINARY	44 4d 49 4f 3a 49 44 3a 78 34 06 d2 df 71 f9 47 8b 31...
\??\Volume{e4d...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{f435...	REG_BINARY	44 4d 49 4f 3a 49 44 3a 51 af 32 7d 2c a0 65 48 84 48...
\??\Volume{fa2e...	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\??\Volume{fa2e...	REG_BINARY	44 4d 49 4f 3a 49 44 3a fe de 39 30 d0 14 97 4f 92 39 ...
\DosDevices\C:	REG_BINARY	44 4d 49 4f 3a 49 44 3a ae c0 54 db 02 6c 2e 42 91 7...
\DosDevices\D:	REG_BINARY	44 4d 49 4f 3a 49 44 3a de 20 fd a9 b5 ca 25 49 9b 4f...
\DosDevices\E:	REG_BINARY	44 4d 49 4f 3a 49 44 3a fe de 39 30 d0 14 97 4f 92 39 ...
\DosDevices\F:	REG_BINARY	44 4d 49 4f 3a 49 44 3a 69 01 30 53 fb 26 bc 43 81 0d...