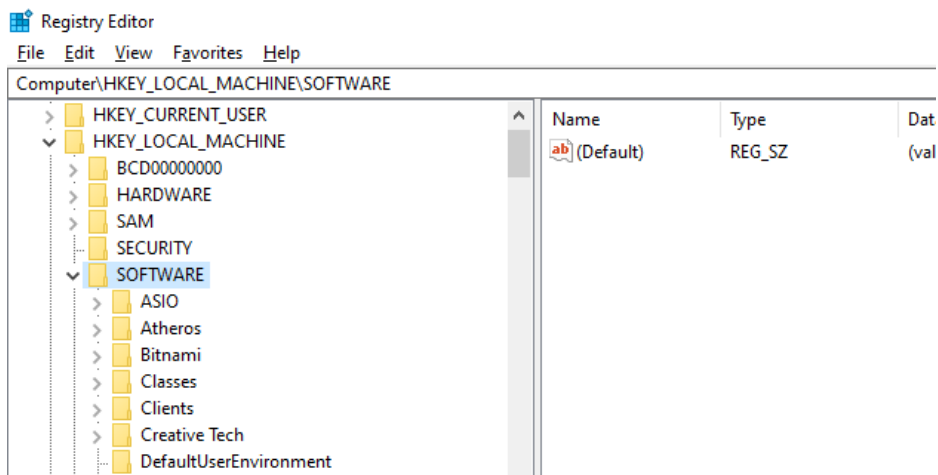
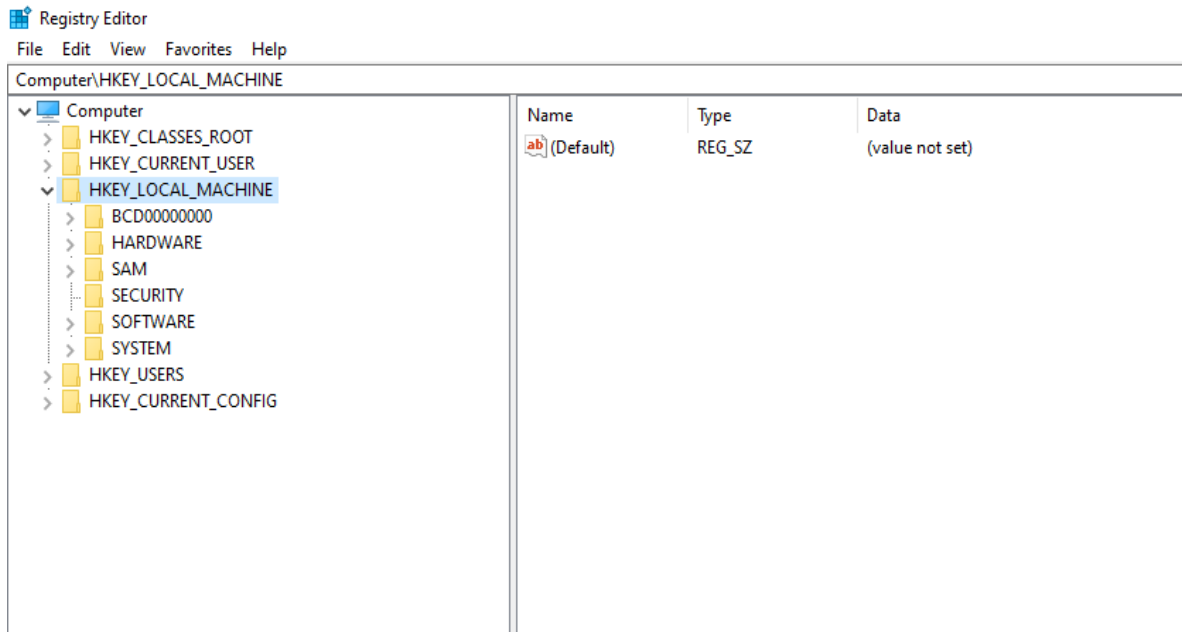


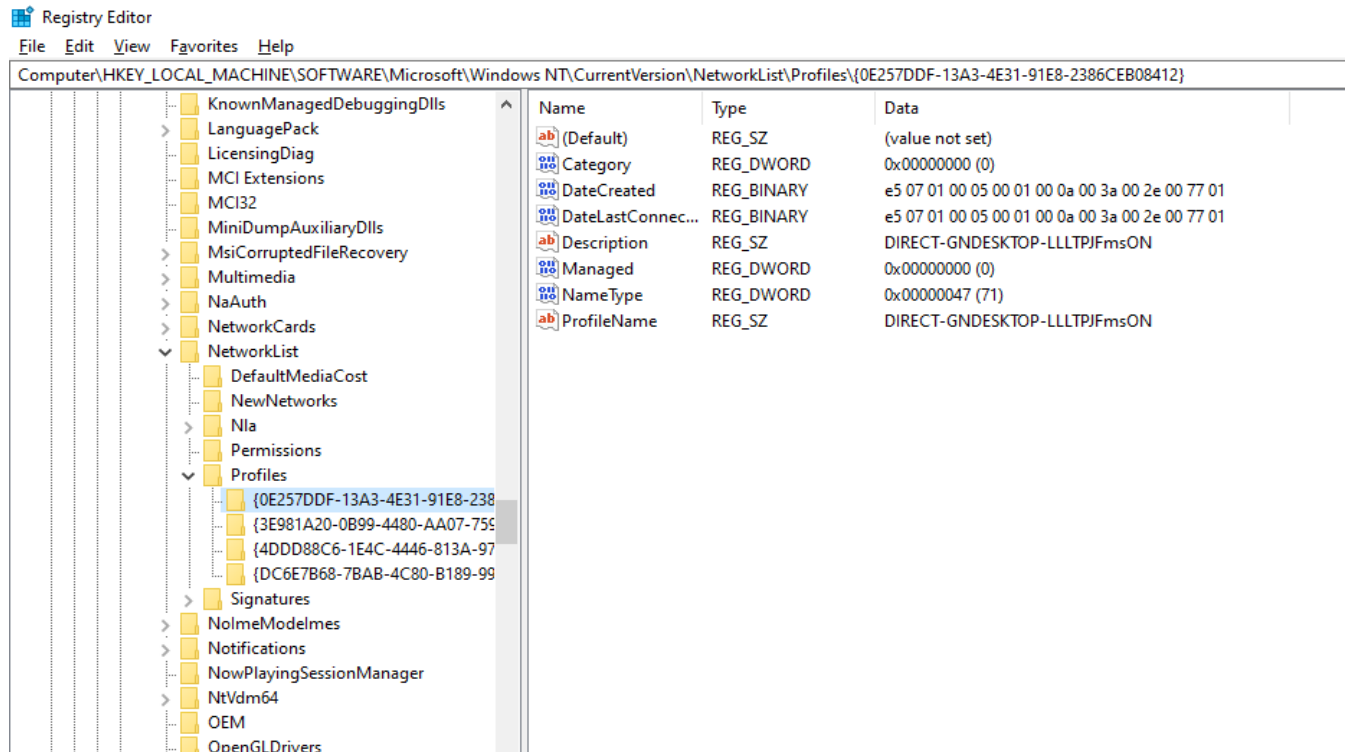
Practical 9: Registry Editor

- Accessing the Registry, Type regedit in Start Search

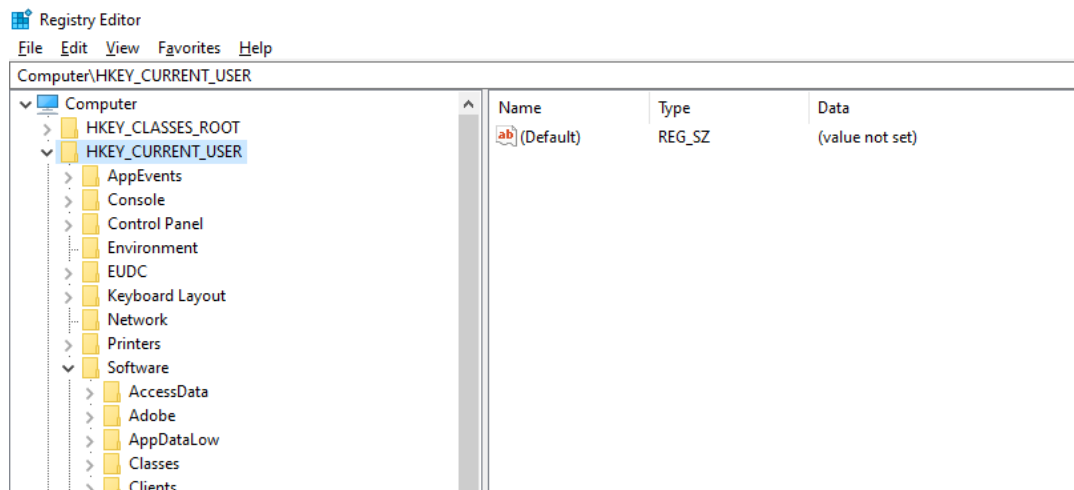
Wireless Evidence in the Registry

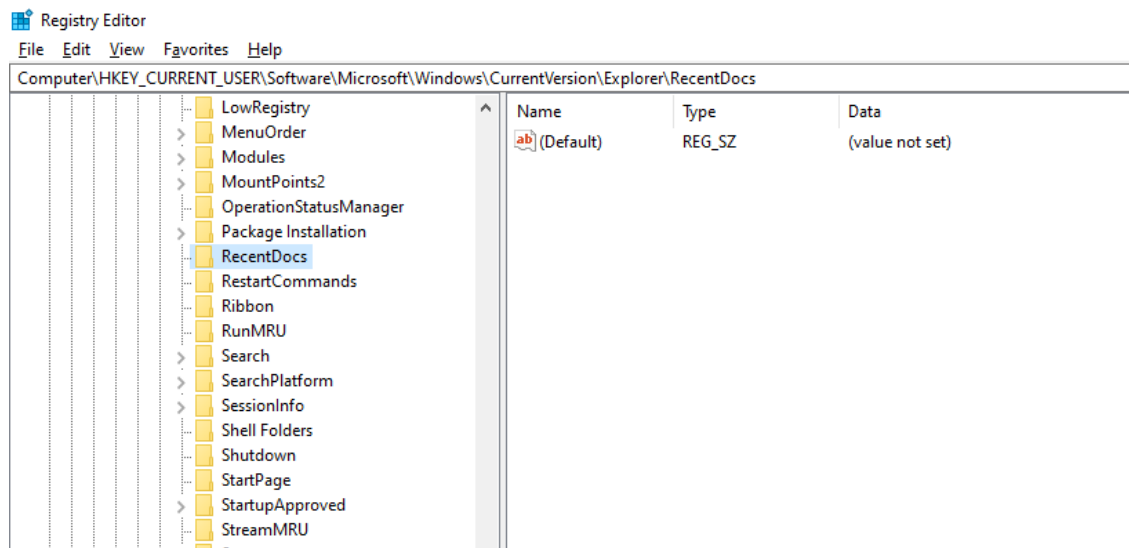
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\NetworkList\Profiles



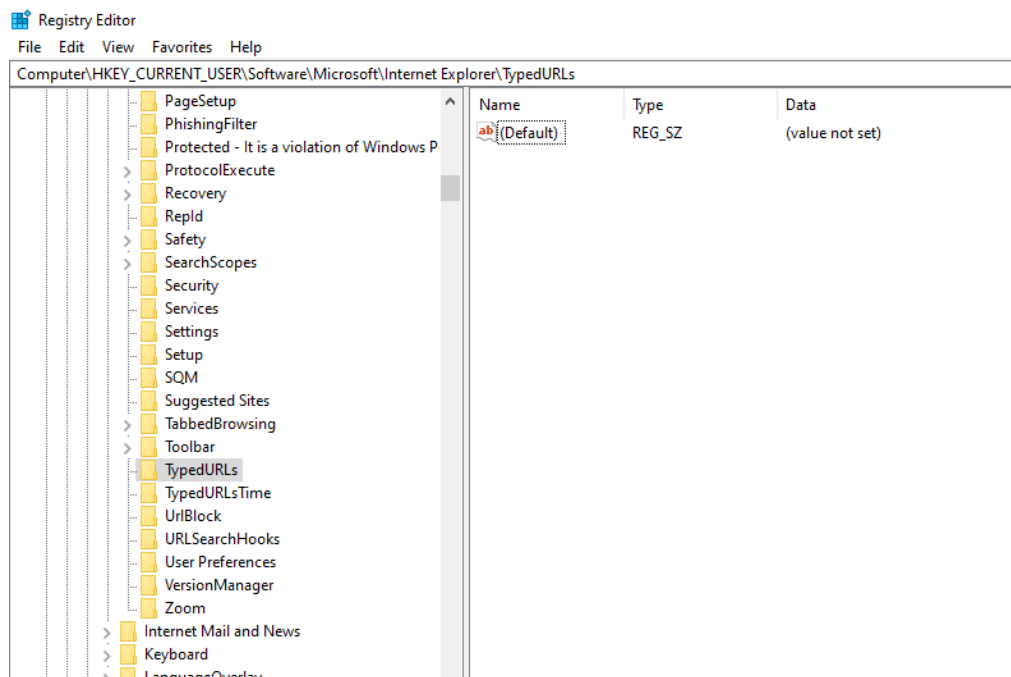


- **The RecentDocs Key**
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs





- **TypedURLs Key:**
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs



- **IP Addresses**

HKEY_LOCAL_MACHINE\System\Services\CurrentControlSet\services\Tcpip\Parameters\Interface

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{37aaf5b1-88bf-4ba6-ba1c-5303cfc84966}

Name	Type	Data
(Default)	REG_SZ	(value not set)
AddressType	REG_DWORD	0x00000000 (0)
DhcpConnForce...	REG_DWORD	0x00000000 (0)
DhcpDefaultGat...	REG_MULTI_SZ	192.168.1.1
DhcpGatewayH...	REG_BINARY	c0 a8 01 01 06 00 00 00 00 1e a6 59 85 a0
DhcpGatewayH...	REG_DWORD	0x00000001 (1)
DhcpInterfaceO...	REG_BINARY	fc 00 00 00 00 00 00 00 00 00 00 00 00 00 27 12...
DhcpIPAddress	REG_SZ	192.168.1.105
DhcpNameServer	REG_SZ	8.8.8.103.50.76.14
DhcpNetworkHint	REG_SZ	96022616C6C602
DhcpServer	REG_SZ	192.168.1.1
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	0x00015180 (86400)
LeaseObtainedTi...	REG_DWORD	0x5fef2088 (1609506952)
LeaseTerminates...	REG_DWORD	0x5ff07208 (1609593352)
NameServer	REG_SZ	
T1	REG_DWORD	0x5fefc948 (1609550152)
T2	REG_DWORD	0x5ff047d8 (1609582552)

- **Start Up Locations in the Registry**

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Registry Editor

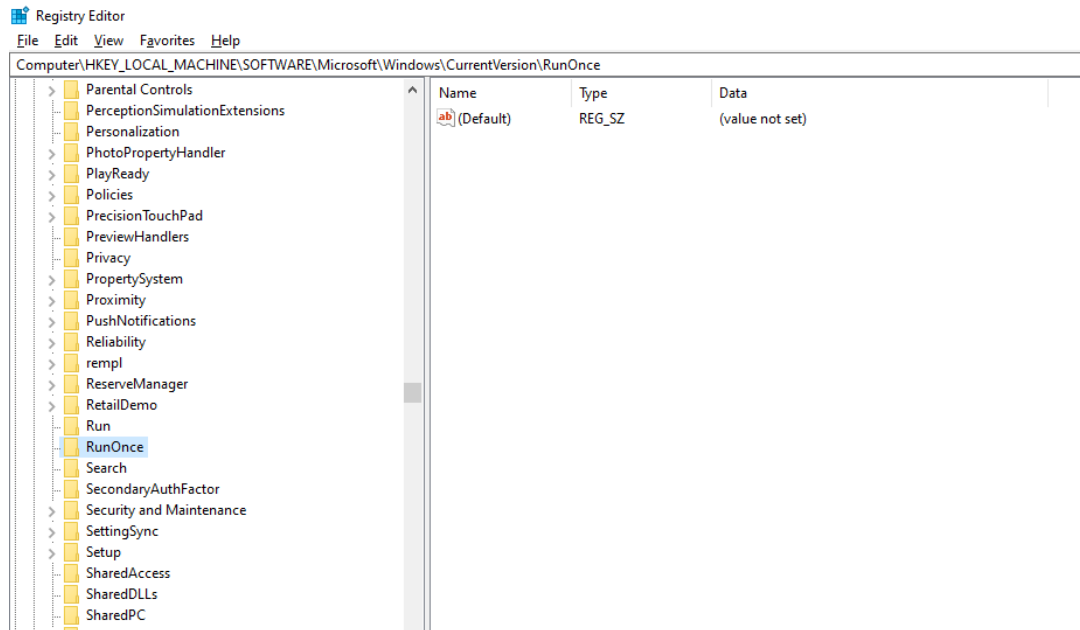
File Edit View Favorites Help

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

Name	Type	Data
(Default)	REG_SZ	(value not set)
IAStoricon	REG_SZ	"C:\Program Files\Intel\Intel(R) Rapid Storage Tech...
RtHDVBg_PushB...	REG_SZ	"C:\Program Files\Realtek\Audio\HDA\RAVBg64.e...
RTHDVCPL	REG_SZ	"C:\Program Files\Realtek\Audio\HDA\RtkNGU64...
SecurityHealth	REG_EXPAND_SZ	%windir%\system32\SecurityHealthSystray.exe
WavesSvc	REG_SZ	"C:\Program Files\Waves\MaxxAudio\WavesSvc64...

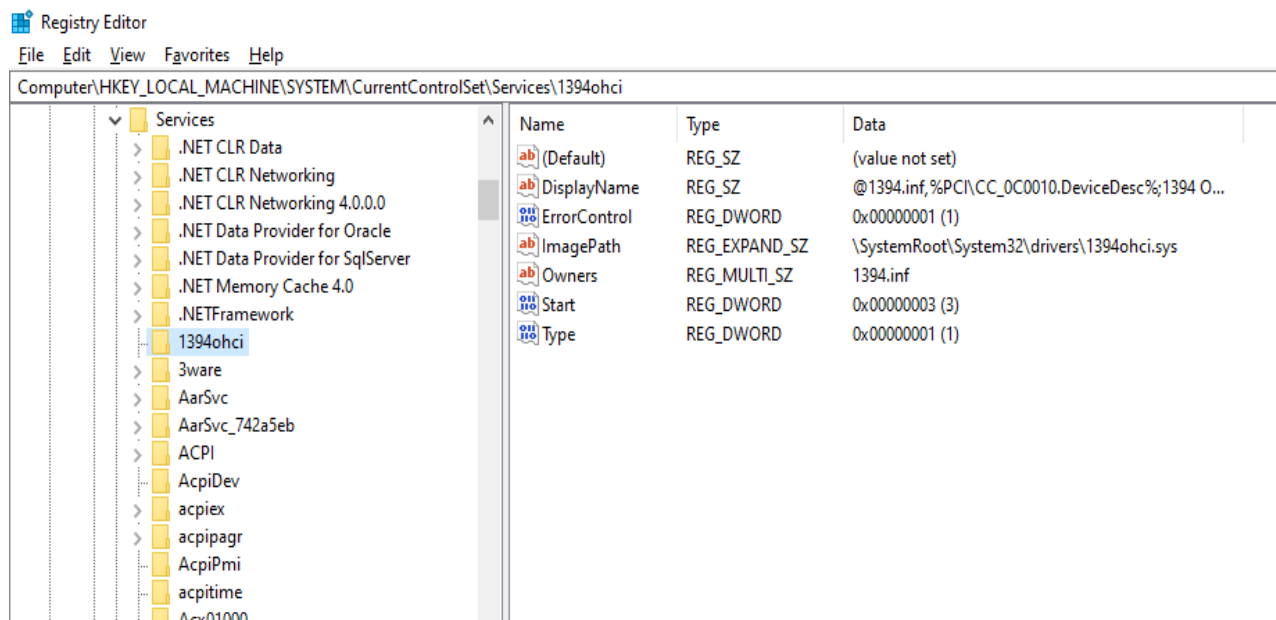
- **RunOnce Startup**

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

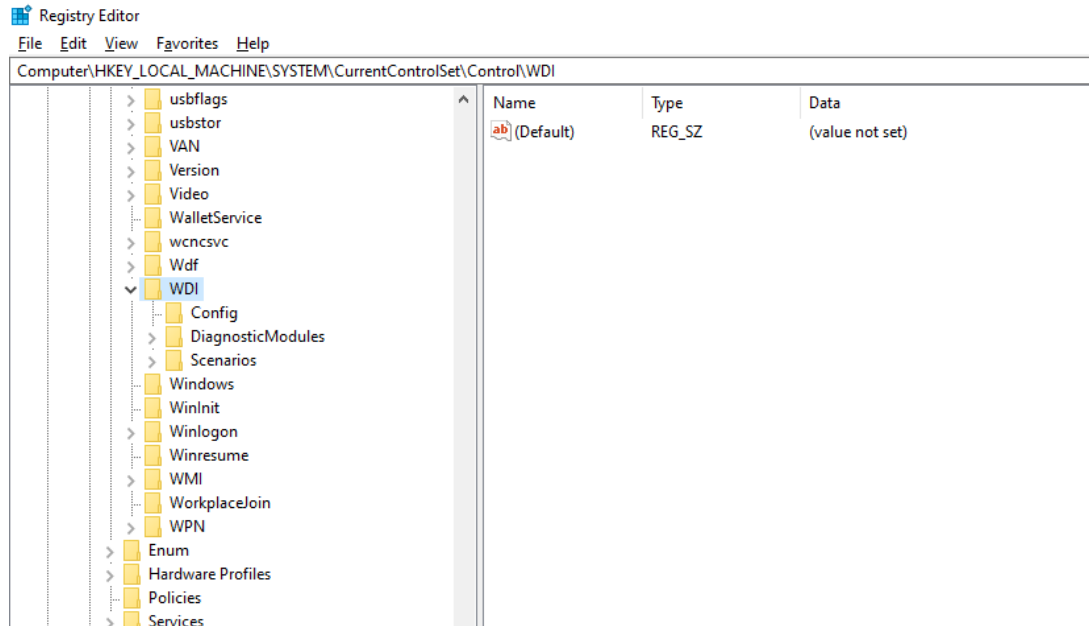


- **Start Up Services**

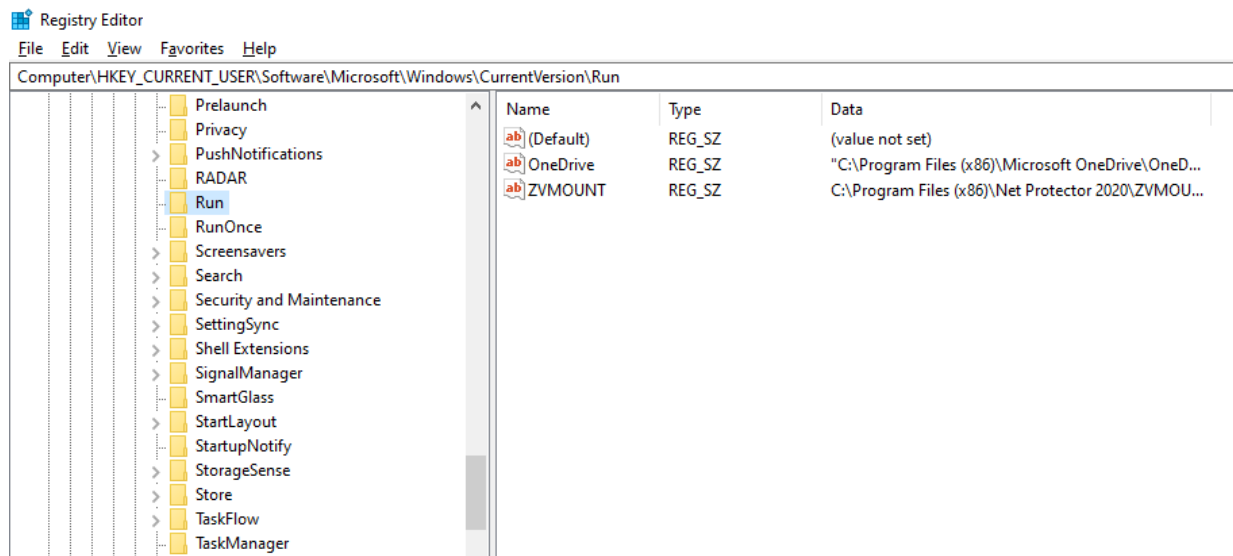
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services



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



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



- **USB Storage Devices**
HKEY_LOCAL_MACHINE\System\ControlSet\Enum\USBSTOR

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_

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

Left pane tree structure:

- CurrentControlSet
 - Control
 - Enum
 - {5d624f94-8850-40c3-a3fa-a4fd2080baf3}
 - ACPI
 - ACPI_HAL
 - BTH
 - DISPLAY
 - HDAUDIO
 - HID
 - HTREE
 - PCI
 - ROOT
 - SCSI
 - STORAGE
 - SW
 - SWD
 - USB
 - USBSTOR
 - Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_
 - Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_
 - Hardware Profiles
 - Policies
 - Services
 - Software
 - DriverDatabase
 - HardwareConfig

- **Mounted Devices**
HKEY_LOCAL_MACHINE\System\MountedDevices

Registry Editor

File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SYSTEM\MountedDevices

Name	Type	Data
(Default)	REG_SZ	(value not set)
\\?\Volume{3af8...}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\\?\Volume{419...}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\\?\Volume{419...}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\\?\Volume{419...}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\\?\Volume{419...}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\\?\Volume{419...}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\\?\Volume{419...}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\\?\Volume{954...}	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\\DosDevices\C:	REG_BINARY	57 fb e0 00 00 40 24 00 00 00 00
\\DosDevices\D:	REG_BINARY	44 4d 49 4f 3a 49 44 3a 6f 8e ae 8f bc a7 da 41 a3 75 ...
\\DosDevices\E:	REG_BINARY	44 4d 49 4f 3a 49 44 3a 05 9e d6 c5 21 ff a9 4c 86 a2 ...
\\DosDevices\F:	REG_BINARY	44 4d 49 4f 3a 49 44 3a 0d 07 41 16 ec a7 59 4d 84 4...
\\DosDevices\G:	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...
\\DosDevices\H:	REG_BINARY	5f 00 3f 00 3f 00 5f 00 55 00 53 00 42 00 53 00 54 00 ...

Left pane tree structure:

- Computer
 - HKEY_CLASSES_ROOT
 - HKEY_CURRENT_USER
 - HKEY_LOCAL_MACHINE
 - BCD00000000
 - HARDWARE
 - SAM
 - SECURITY
 - SOFTWARE
 - SYSTEM
 - ActivationBroker
 - ControlSet001
 - CurrentControlSet
 - DriverDatabase
 - HardwareConfig
 - Input
 - Keyboard Layout
 - Maps
 - MountedDevices
 - ResourceManager
 - ResourcePolicyStore
 - RNG
 - Select
 - Setup
 - Software