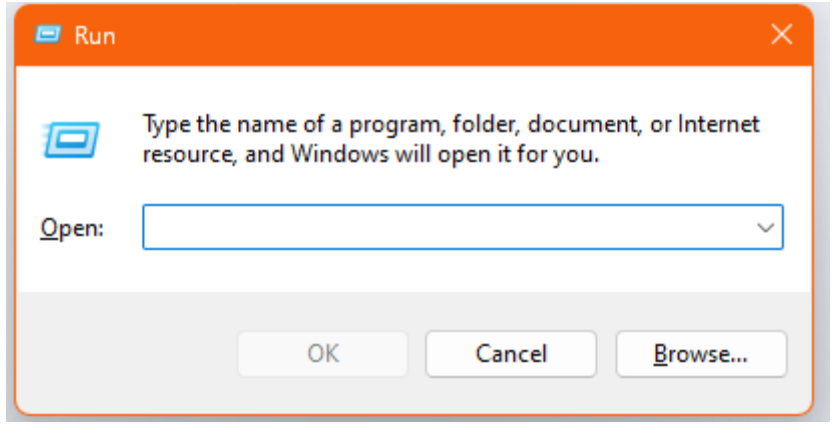
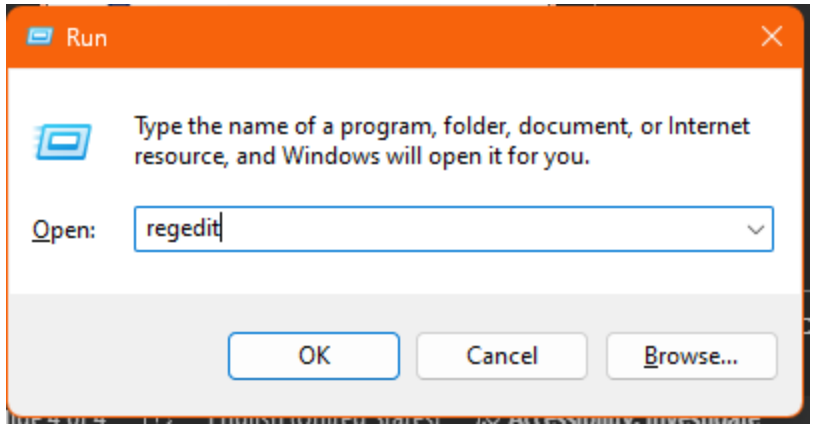
برنامه نویسی سیستمی

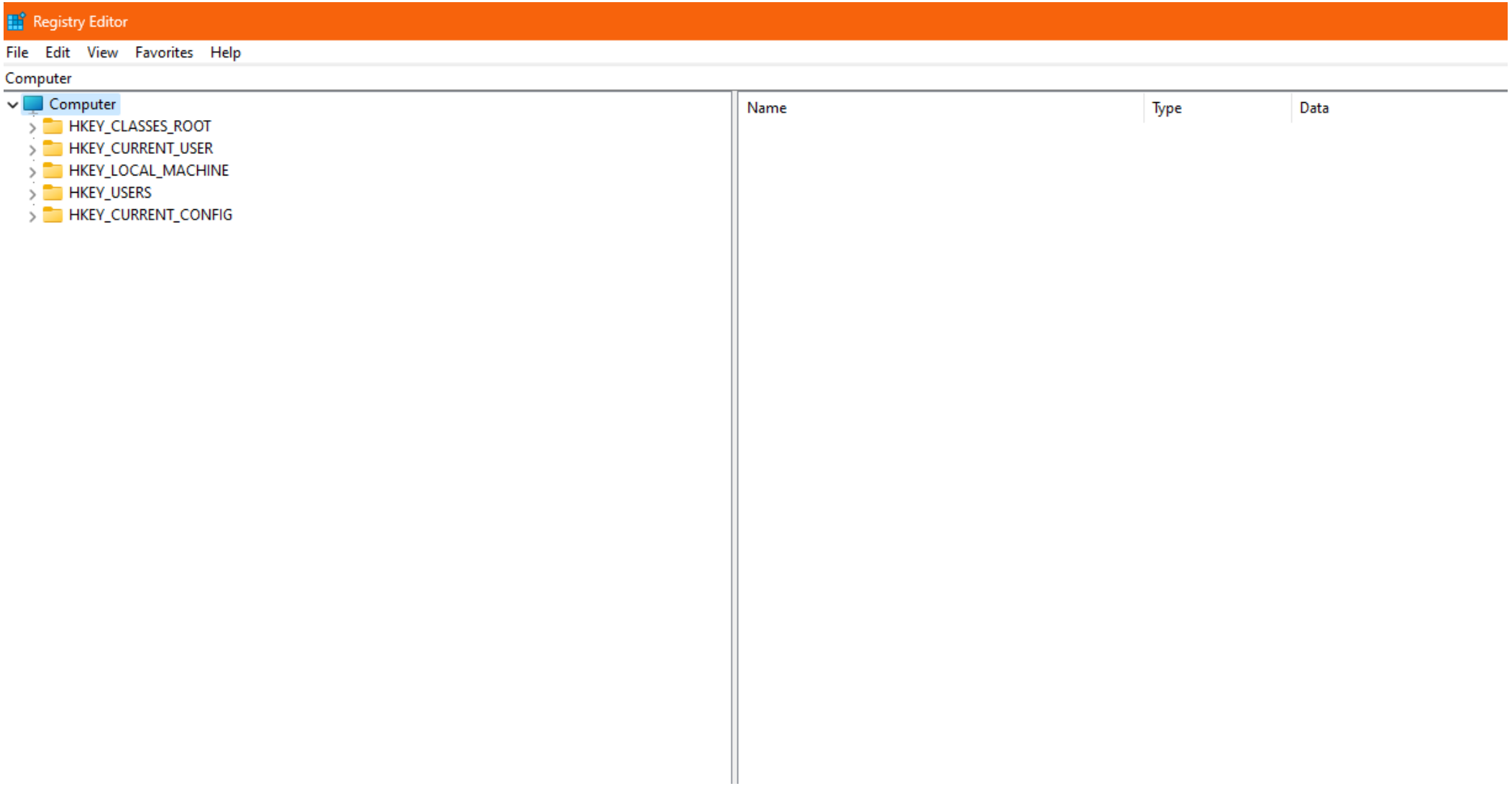
Windows Internals

کاوه حقیقی

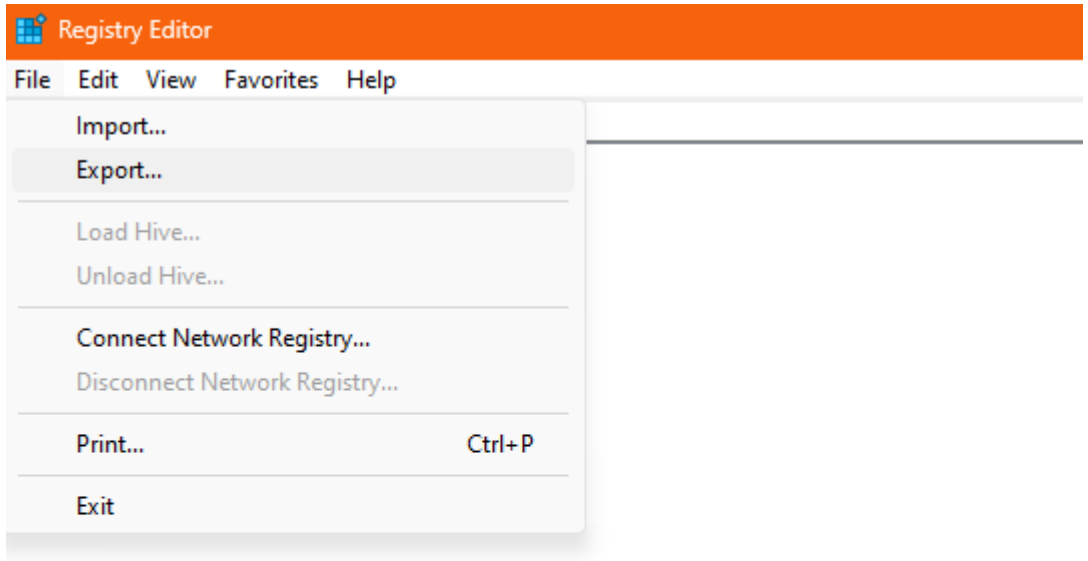
آشنایی با رجیستری


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
OK
Cancel
Browse...


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
regedit
OK
Cancel
Browse...

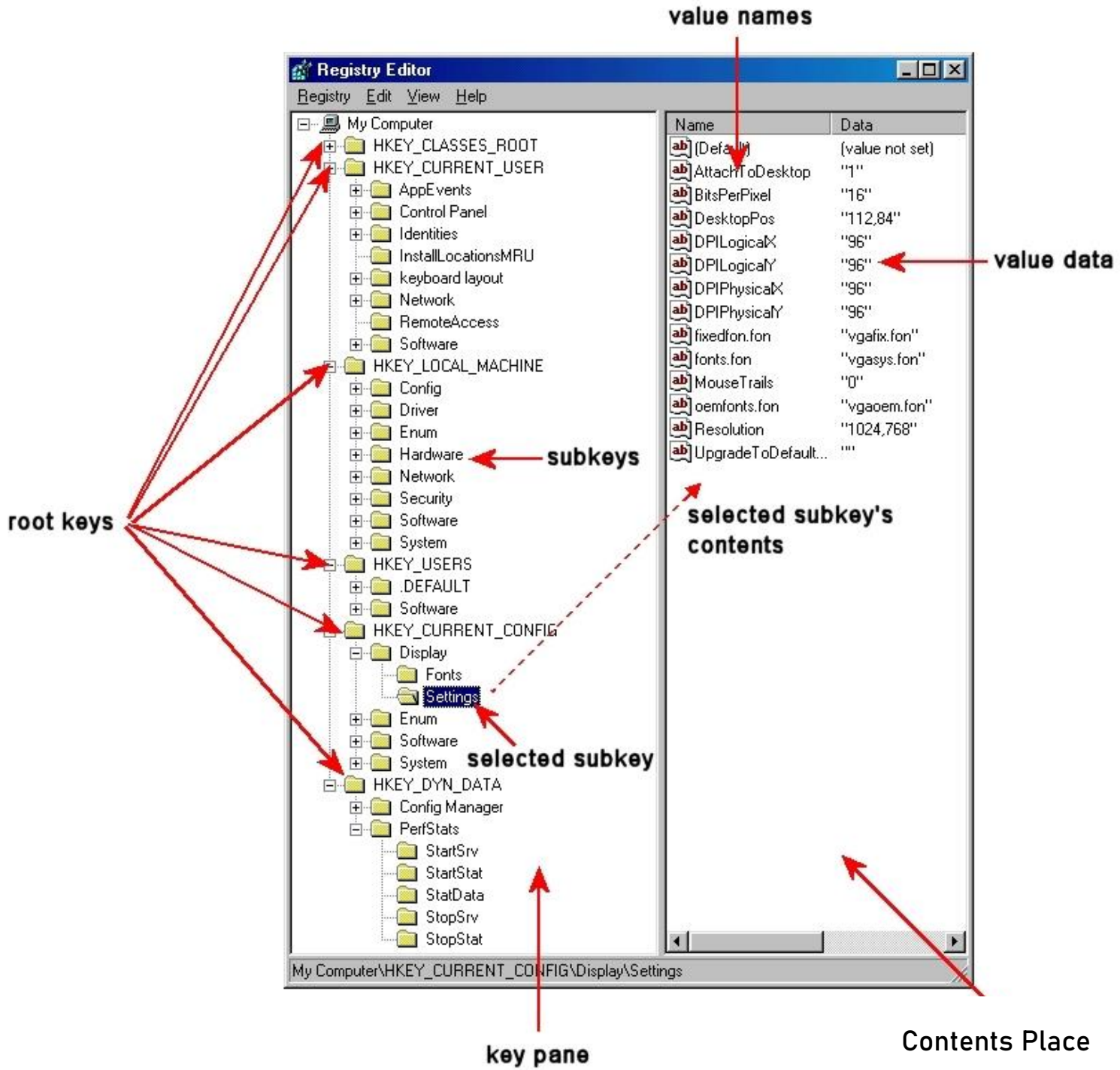

Registry Editor
File Edit View Favorites Help
Computer
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
HKEY_CURRENT_CONFIG
Name
Type
Data

بکاپ گیری از رجیستری ویندوز


Registry Editor
File
Edit
View
Favorites
Help
Import...
Export...
Load Hive...
Unload Hive...
Connect Network Registry...
Disconnect Network Registry...
Print... Ctrl+P
Exit

راه دوم؟

ساختار رجیستری ویندوز


value names
Registry Editor
Registry Edit View Help
My Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
AppEvents
Control Panel
Identities
InstallLocationsMRU
keyboard layout
Network
RemoteAccess
Software
HKEY_LOCAL_MACHINE
Config
Driver
Enum
Hardware
Network
Security
Software
System
HKEY_USERS
.DEFAULT
Software
HKEY_CURRENT_CONFIG
Display
Fonts
Settings
Enum
Software
System
HKEY_DYN_DATA
Config Manager
PerfStats
StartSrv
StartStat
StatData
StopSrv
StopStat
Name
Data
(Default)
(value not set)
AttachToDesktop
"1"
BitsPerPixel
"16"
DesktopPos
"112,84"
DPILogicalX
"96"
DPILogicalY
"96"
DPIPhysicalX
"96"
DPIPhysicalY
"96"
fixedfon.fon
"vgafix.fon"
fonts.fon
"vgasys.fon"
MouseTrails
"0"
oemfonts.fon
"vgaoem.fon"
Resolution
"1024,768"
UpgradeToDefault...
""
My Computer\HKEY_CURRENT_CONFIG\Display\Settings
value data
subkeys
root keys
selected subkey's contents
selected subkey
key pane
Contents Place

HKEY_CLASSES_ROOT

تنظیمات نرم افزار در مورد فایل سیستم، اطلاعات میانبر (shortcut information) ، اطلاعات در مورد file associations و سایر رابطهای کاربری در این مجتمع ذخیره می شوند. اطلاعات مربوط به association file اساسا توسط ویندوز برای استفاده برنامه ها می باشد.

HKEY_USERS

تنظیمات پیکربندی برای هر Itemاسخت افزار و نرم افزار در سیستم کامپیوتری،مربوط به هر یک از کاربران سیستم کامپیوتری در این مجتمع ذخیره می شود. اطلاعات موجود در پوشه های کاربر، انتخاب تم های کاربر، رنگ ها و تنظیمات Control Panel، به عنوان پروفایل کاربر ذخیره می شوند. این مجتمع دارای یکsubkey به ازای هر پروفایل کاربر است.

HKEY_CURRENT_USER

تنظیمات پیکربندی برای هر مورد سخت افزار و نرم افزار در سیستم کامپیوتری، مربوط به کاربر جاری در این مجتمع ذخیره می شود. این مجتمع بصورت داینامیک است یعنی به عنوان مثال هر کاربر که به سیستم Log inکند، تنظیمات مربوط به کاربر از Subkeyمربوط به H_KEY_USERS، به عنوان پروفایل کاربر بازیابی شده در این مجتمع ذخیره می شود.

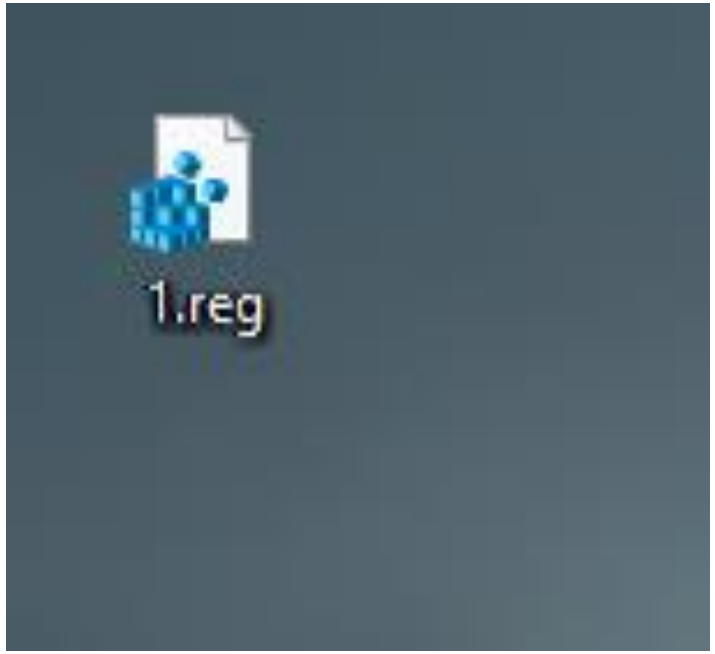
HKEY_LOCAL_MACHINE

تنظیمات پیکربندی سخت افزار و نرم افزار برای همه کاربران کامپیوتر در این مجتمع ذخیره می شود. یعنی دیگر فرقی ندارد که چه کاربری پشت این سیستم بصورتinteractive نشسته و لاگین می کند. تنظیمات این مجتمع برای همه کاربران اعمال خواهد شد.

HKEY_CURRENT_CONFIG

Contains information about the hardware profile that is used by the local computer at system startup.

فایل reg. چیست؟


1.reg

Registry Data Types

List of Registry Value Types		
0	REG_NONE	No type
1	REG_SZ	A string value
2	REG_EXPAND_SZ	An "expandable" string value that can contain environment variables
3	REG_BINARY	Binary data (any arbitrary data)
4	REG_DWORD/REG_DWORD_LITTLE_ENDIAN	A DWORD value, a 32-bit unsigned integer (numbers between 0 and 4,294,967,295 [2^{32} – 1]) (little-endian)
5	REG_DWORD_BIG_ENDIAN	A DWORD value, a 32-bit unsigned integer (numbers between 0 and 4,294,967,295 [2^{32} – 1]) (big-endian)
6	REG_LINK	symbolic link (UNICODE)
7	REG_MULTI_SZ	A multi-string value, which is an array of unique strings
8	REG_RESOURCE_LIST	Resource list Series of nested arrays designed to store a list of resources
9	REG_FULL_RESOURCE_DESCRIPTOR	Resource descriptor A list of resources used by a physical HW device
10	REG_RESOURCE_REQUIREMENTS_LIST	Resource Requirements List A list of HW resources used by a device driver
11	REG_QWORD/REG_QWORD_LITTLE_ENDIAN	A QWORD value, a 64-bit integer (either big- or little-endian, or unspecified) (Introduced in Windows 2000)

Data
0x12345678

Big Endian

Address	0x100	0x101	0x102	0x103
	0x12	0x34	0x56	0x78

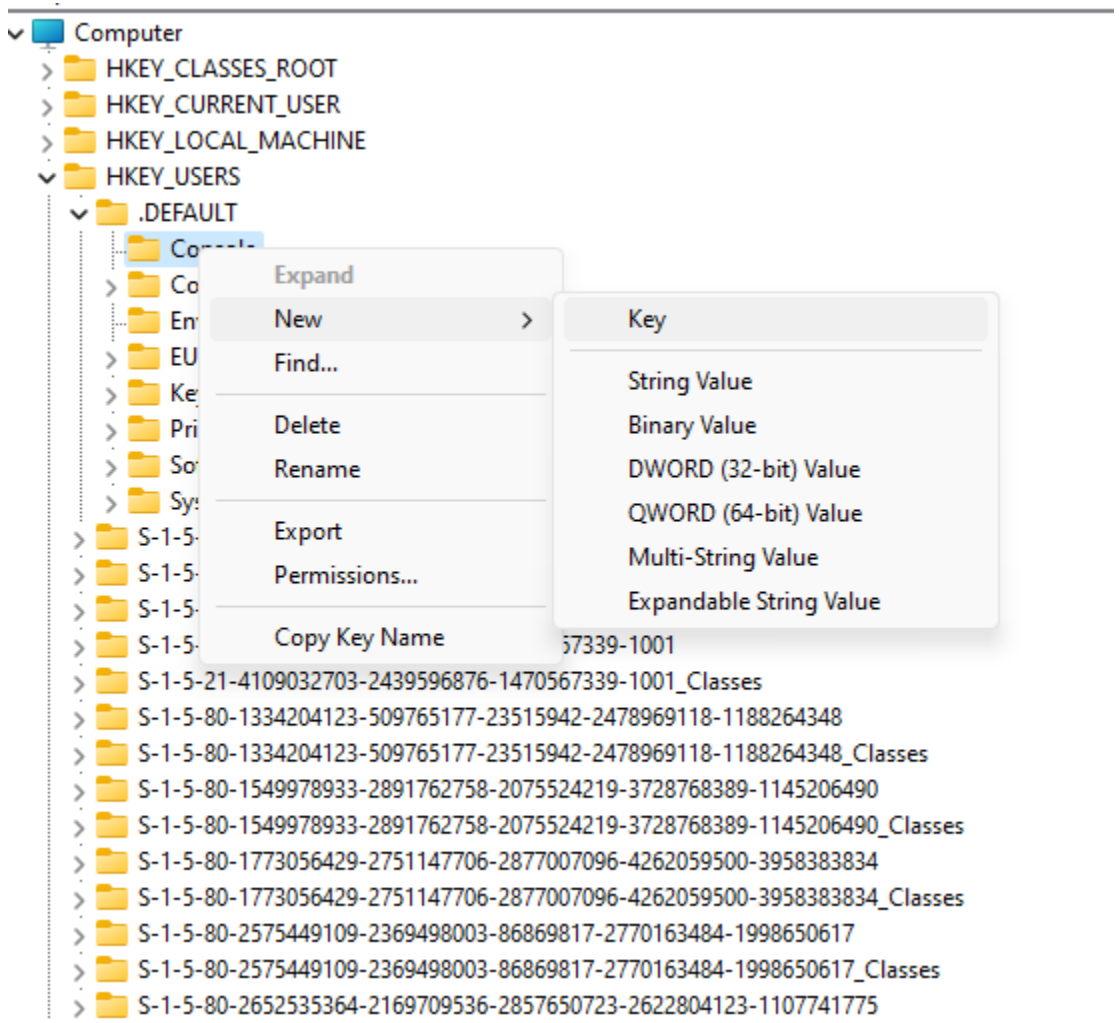
Little Endian

Address	0x100	0x101	0x102	0x103
	0x78	0x56	0x34	0x12

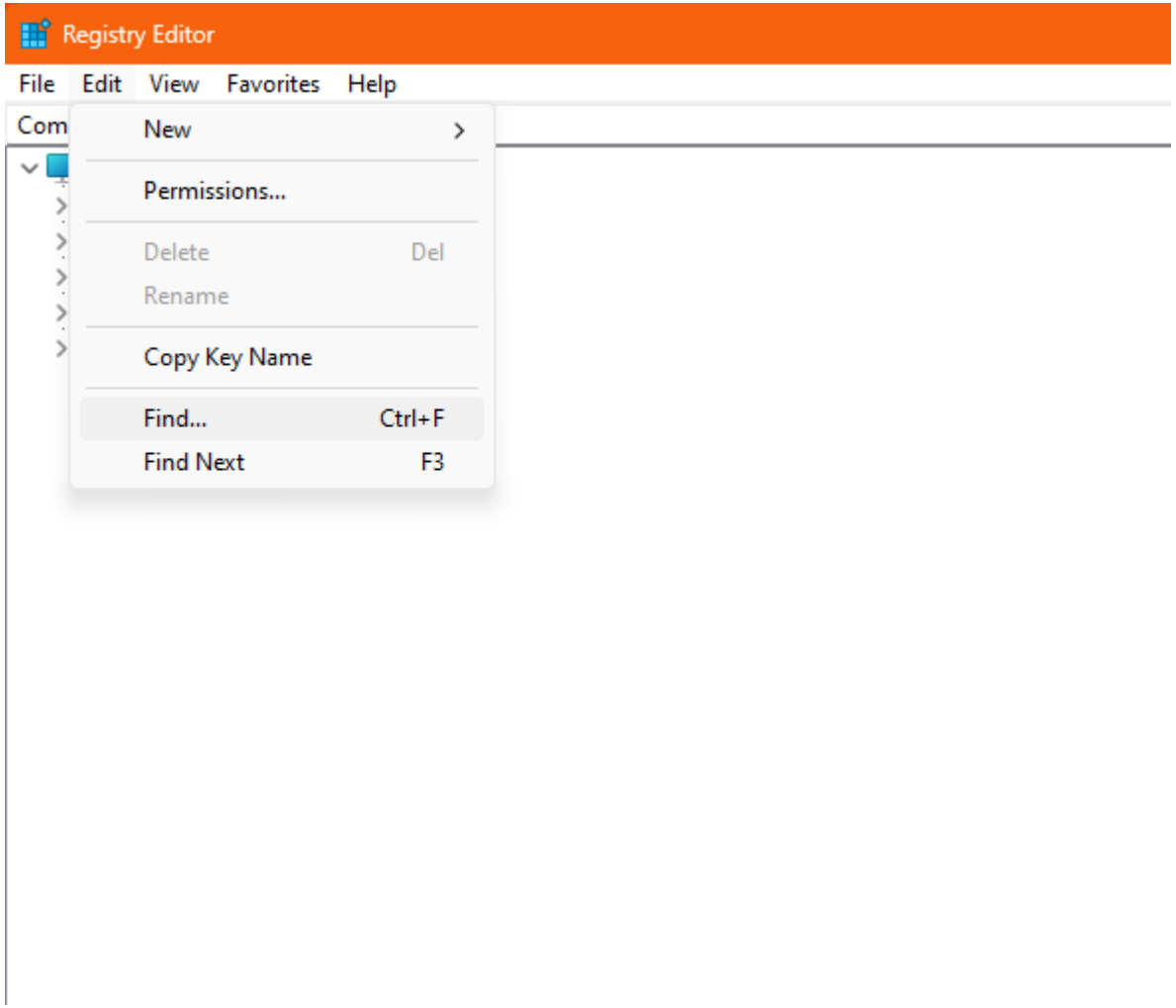
محل ذخیره فایل رجیستری

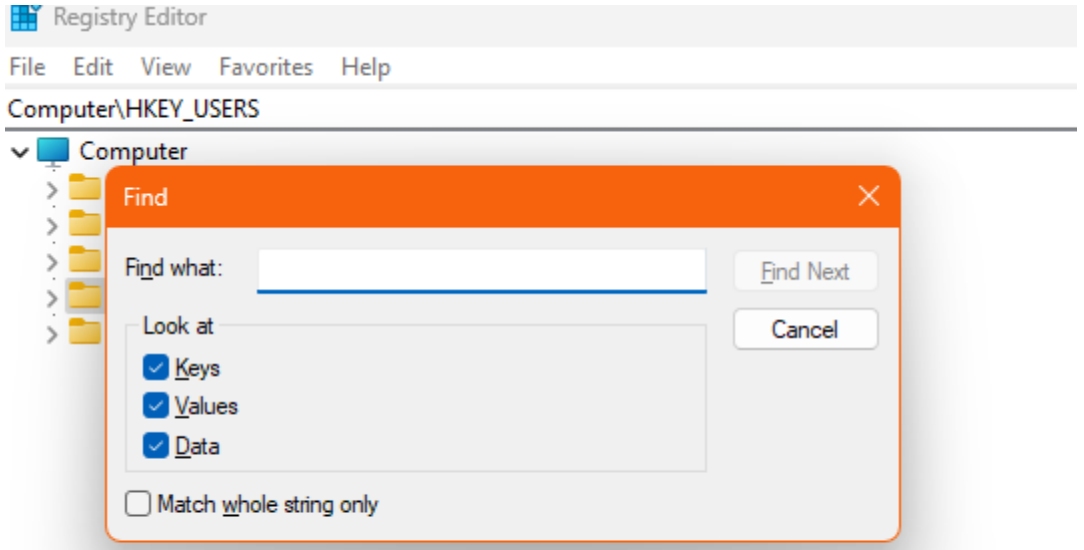
HKEY_LOCAL_MACHINE \SYSTEM : \system32\config\system
HKEY_LOCAL_MACHINE \SAM : \system32\config\sam
HKEY_LOCAL_MACHINE \SECURITY : \system32\config\security
HKEY_LOCAL_MACHINE \SOFTWARE : \system32\config\software
HKEY_USERS \UserProfile : \winnt\profiles\username
HKEY_USERS.DEFAULT : \system32\config\default

ایجاد Keyها در Windows Registry


Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
HKEY_USERS
.DEFAULT
Expand
New
Find...
Delete
Rename
Export
Permissions...
Copy Key Name
Key
String Value
Binary Value
DWORD (32-bit) Value
QWORD (64-bit) Value
Multi-String Value
Expandable String Value
S-1-5-21-4109032703-2439596876-1470567339-1001_Classes
S-1-5-80-1334204123-509765177-23515942-2478969118-1188264348
S-1-5-80-1334204123-509765177-23515942-2478969118-1188264348_Classes
S-1-5-80-1549978933-2891762758-2075524219-3728768389-1145206490
S-1-5-80-1549978933-2891762758-2075524219-3728768389-1145206490_Classes
S-1-5-80-1773056429-2751147706-2877007096-4262059500-3958383834
S-1-5-80-1773056429-2751147706-2877007096-4262059500-3958383834_Classes
S-1-5-80-2575449109-2369498003-86869817-2770163484-1998650617
S-1-5-80-2575449109-2369498003-86869817-2770163484-1998650617_Classes
S-1-5-80-2652535364-2169709536-2857650723-2622804123-1107741775

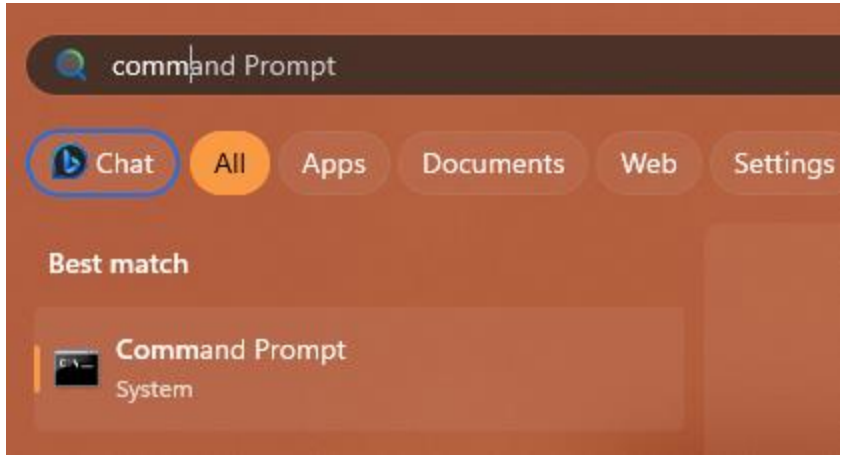
چگونه در رجیستری جستجو کنیم؟

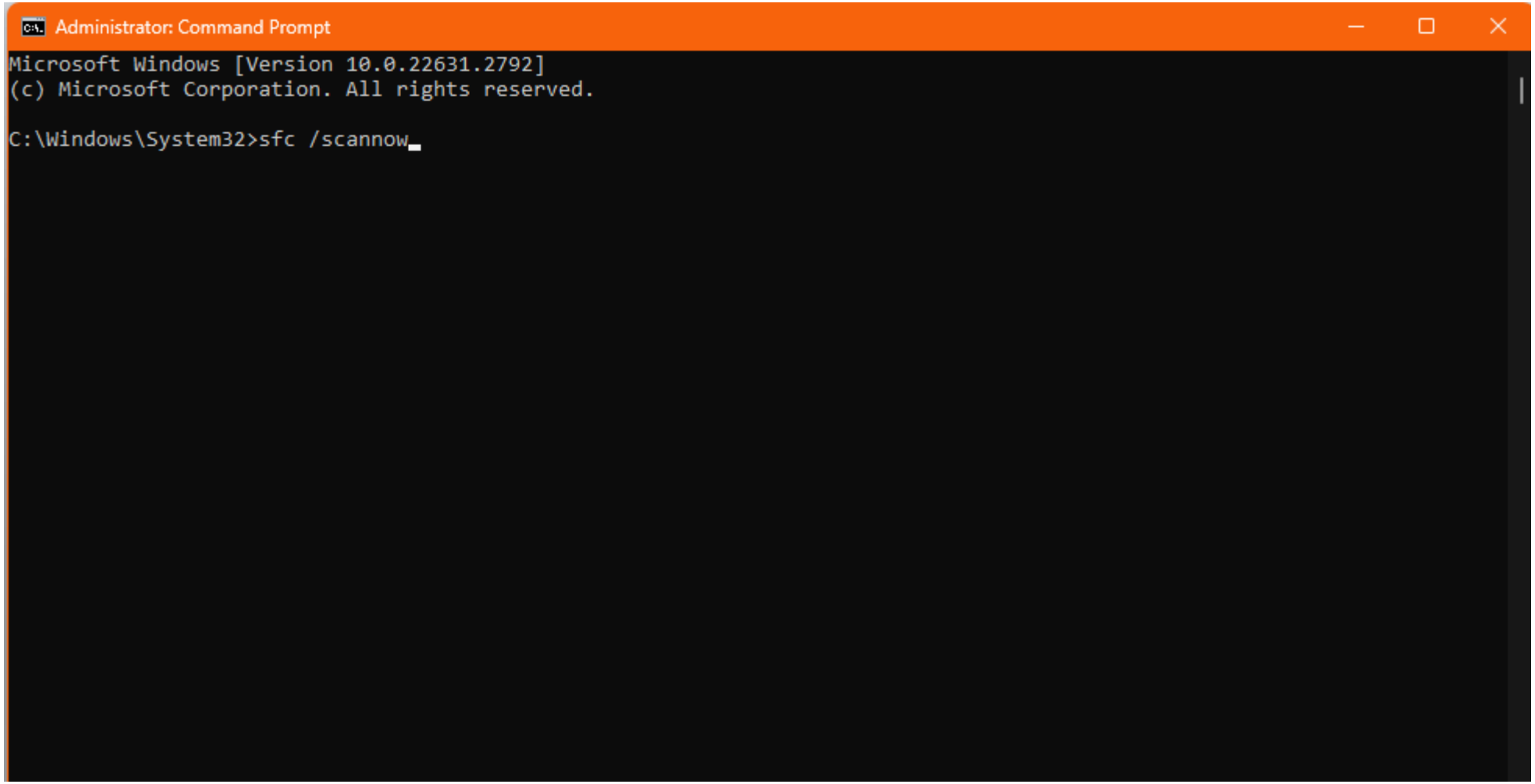

Registry Editor
File
Edit
View
Favorites
Help
Com
New
Permissions...
Delete
Del
Rename
Copy Key Name
Find...
Ctrl+F
Find Next
F3


Registry Editor
File Edit View Favorites Help
Computer\HKEY_USERS
Computer
Find
Find what:
Find Next
Look at
Cancel
Keys
Values
Data
Match whole string only

How to Fix Registry Errors in Windows

- Back Up Your Registry
- Create a System Restore Point
- Command Prompt

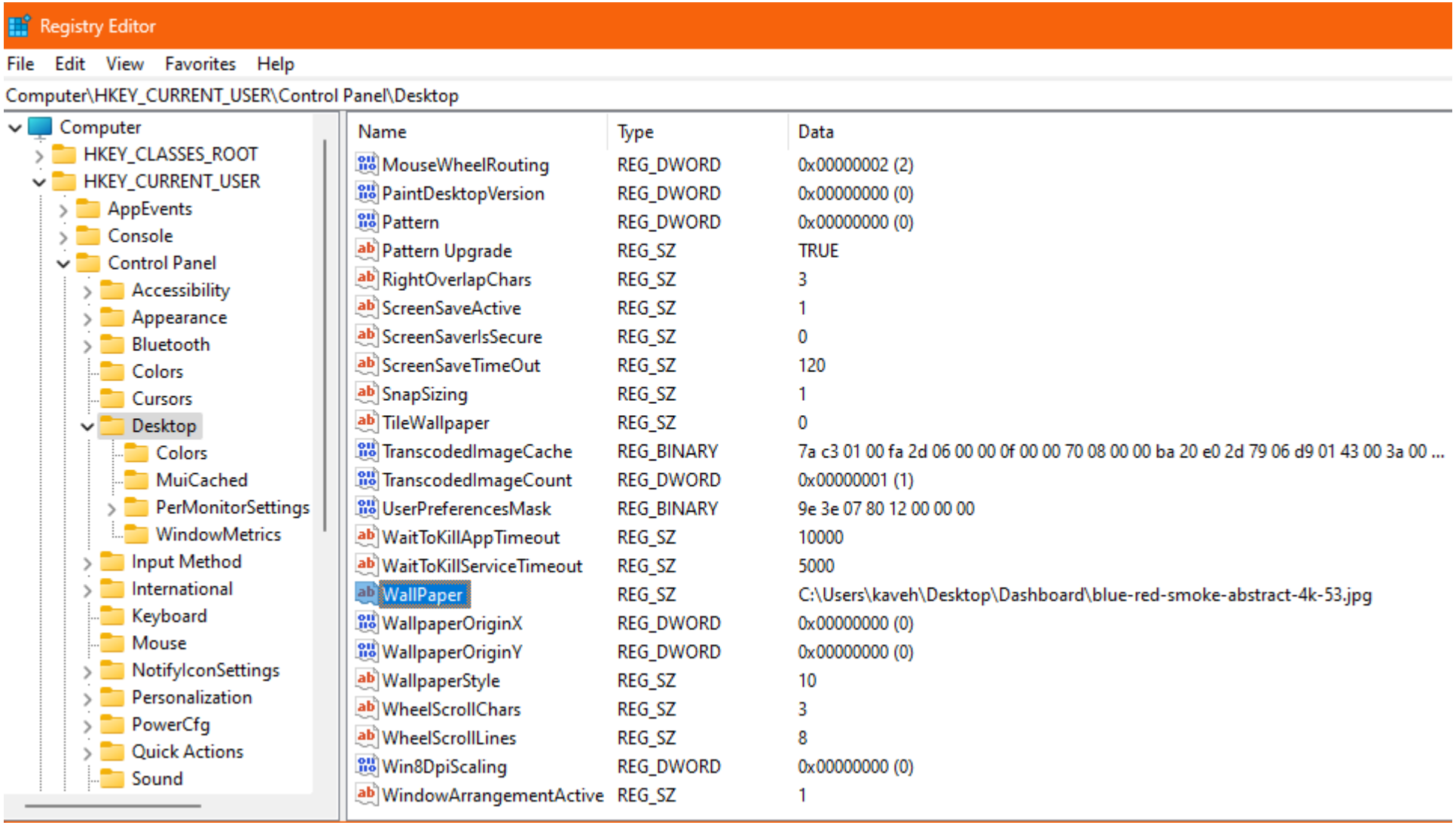

command Prompt
Chat
All
Apps
Documents
Web
Settings
Best match
Command Prompt
System

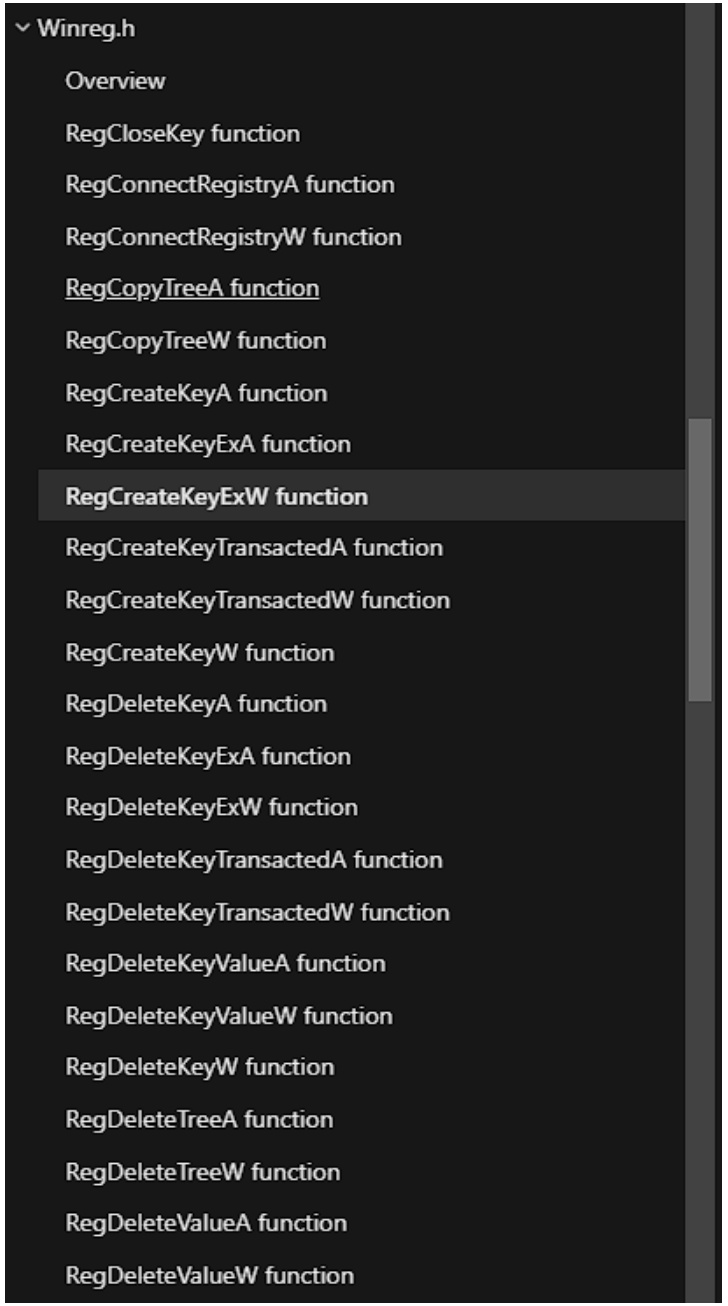

Administrator: Command Prompt
Microsoft Windows [Version 10.0.22631.2792]
(c) Microsoft Corporation. All rights reserved.
C:\Windows\System32>sfc /scannow

```
Dism /Online /Cleanup-Image /CheckHealth

Dism /Online /Cleanup-Image /ScanHealth

Dism /Online /Cleanup-Image /RestoreHealth
```


Registry Editor
File Edit View Favorites Help
Computer\HKEY_CURRENT_USER\Control Panel\Desktop
Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
AppEvents
Console
Control Panel
Accessibility
Appearance
Bluetooth
Colors
Cursors
Desktop
Colors
MuiCached
PerMonitorSettings
WindowMetrics
Input Method
International
Keyboard
Mouse
NotifyIconSettings
Personalization
PowerCfg
Quick Actions
Sound
Name Type Data
MouseWheelRouting REG_DWORD 0x00000002 (2)
PaintDesktopVersion REG_DWORD 0x00000000 (0)
Pattern REG_DWORD 0x00000000 (0)
Pattern Upgrade REG_SZ TRUE
RightOverlapChars REG_SZ 3
ScreenSaveActive REG_SZ 1
ScreenSaverIsSecure REG_SZ 0
ScreenSaveTimeOut REG_SZ 120
SnapSizing REG_SZ 1
TileWallpaper REG_SZ 0
TranscodedImageCache REG_BINARY 7a c3 01 00 fa 2d 06 00 00 0f 00 00 70 08 00 00 ba 20 e0 2d 79 06 d9 01 43 00 3a 00 ...
TranscodedImageCount REG_DWORD 0x00000001 (1)
UserPreferencesMask REG_BINARY 9e 3e 07 80 12 00 00 00
WaitToKillAppTimeout REG_SZ 10000
WaitToKillServiceTimeout REG_SZ 5000
WallPaper REG_SZ C:\Users\kaveh\Desktop\Dashboard\blue-red-smoke-abstract-4k-53.jpg
WallpaperOriginX REG_DWORD 0x00000000 (0)
WallpaperOriginY REG_DWORD 0x00000000 (0)
WallpaperStyle REG_SZ 10
WheelScrollChars REG_SZ 3
WheelScrollLines REG_SZ 8
Win8DpiScaling REG_DWORD 0x00000000 (0)
WindowArrangementActive REG_SZ 1


Winreg.h
Overview
RegCloseKey function
RegConnectRegistryA function
RegConnectRegistryW function
RegCopyTreeA function
RegCopyTreeW function
RegCreateKeyA function
RegCreateKeyExA function
RegCreateKeyExW function
RegCreateKeyTransactedA function
RegCreateKeyTransactedW function
RegCreateKeyW function
RegDeleteKeyA function
RegDeleteKeyExA function
RegDeleteKeyExW function
RegDeleteKeyTransactedA function
RegDeleteKeyTransactedW function
RegDeleteKeyValueA function
RegDeleteKeyValueW function
RegDeleteKeyW function
RegDeleteTreeA function
RegDeleteTreeW function
RegDeleteValueA function
RegDeleteValueW function

Syntax

C++ Copy

```
LSTATUS RegCreateKeyExW(
  [in]            HKEY                        hKey,
  [in]            LPCWSTR                     lpSubKey,
                  DWORD                       Reserved,
  [in, optional]  LPWSTR                      lpClass,
  [in]            DWORD                       dwOptions,
  [in]            REGSAM                      samDesired,
  [in, optional]  const LPSECURITY_ATTRIBUTES lpSecurityAttributes,
  [out]           PHKEY                       phkResult,
  [out, optional] LPDWORD                     lpdwDisposition
);
```