



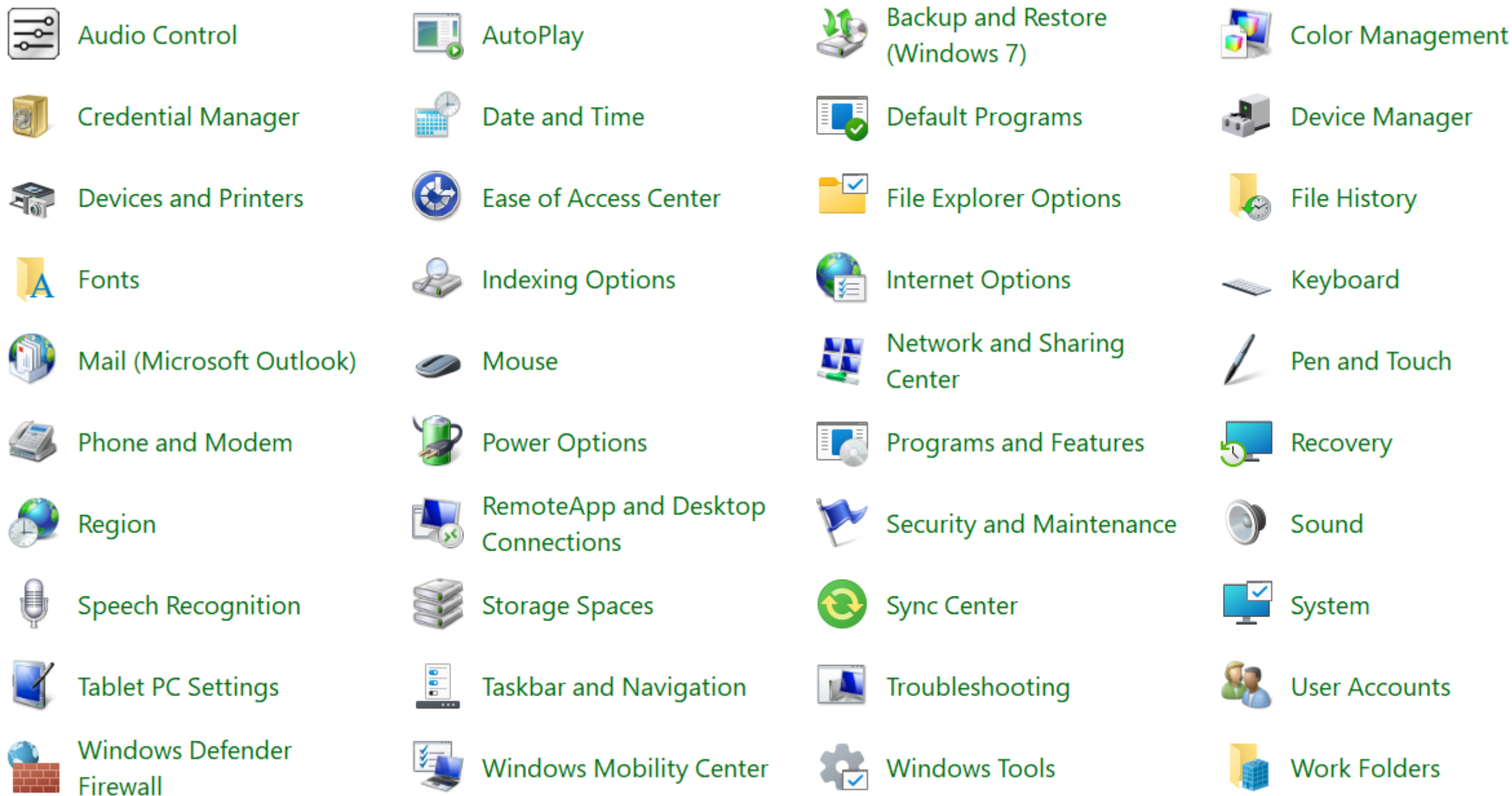
Registry Editor

By: Dana Mohammed Al-Mahrouk

Setting & Configuration of Application

Hello Here

- Where are application configuration settings saved?
- ✗ • font type and style in Word or character design for a game you play.
- ✓ • Application → (color, font size, screen size, path install program & setting, version ,update & upgrade)
- Your personality on the device, your preferences for design and organization.



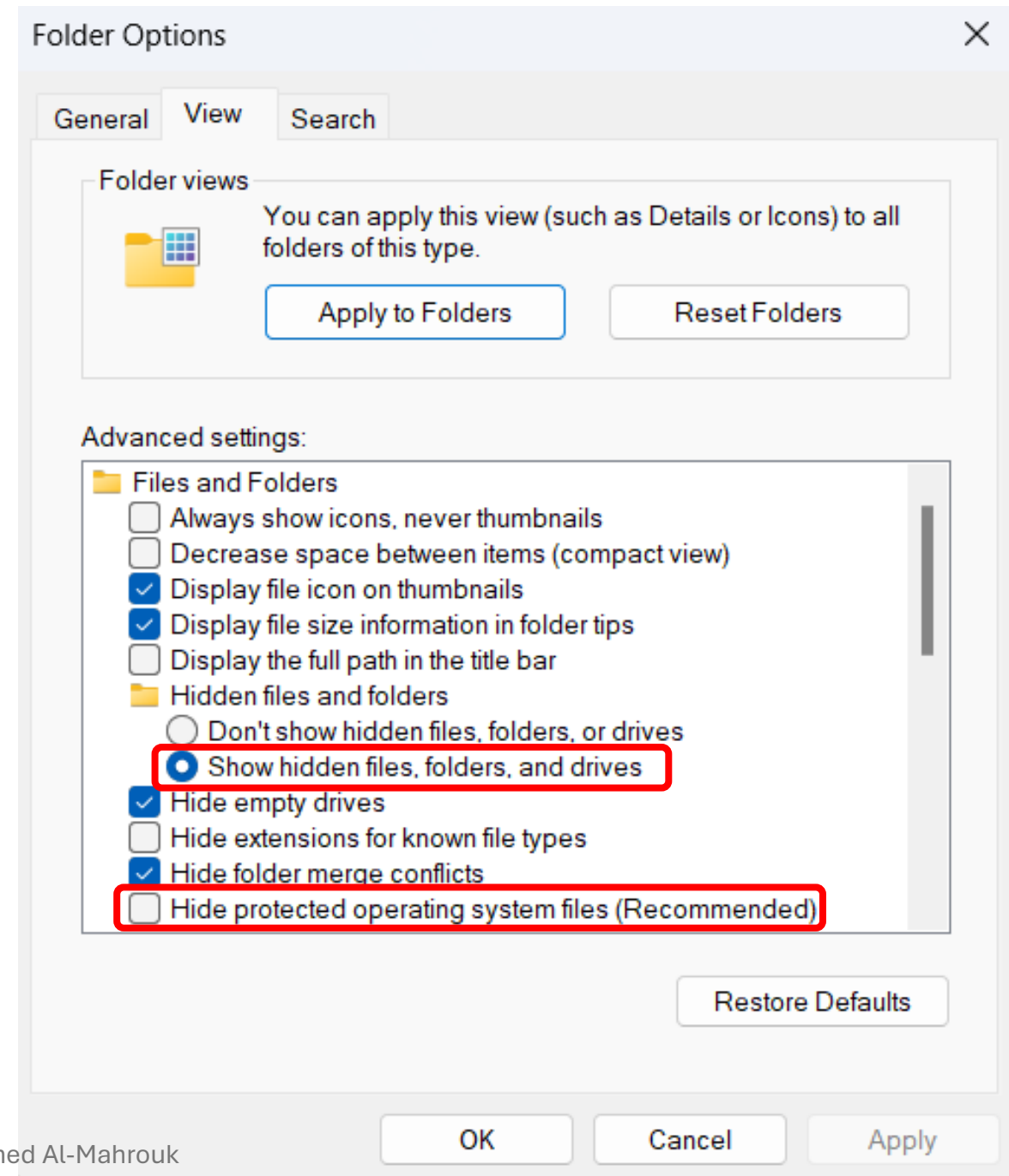
Past



- Program settings were stored in separate files distributed throughout the system.
- .ini → initialization file
- `attrib <+-[S | H | R]> <file-name>`
 - A → Read for archiving (default)
 - S → file system
 - H → Hidden file
 - R → read only

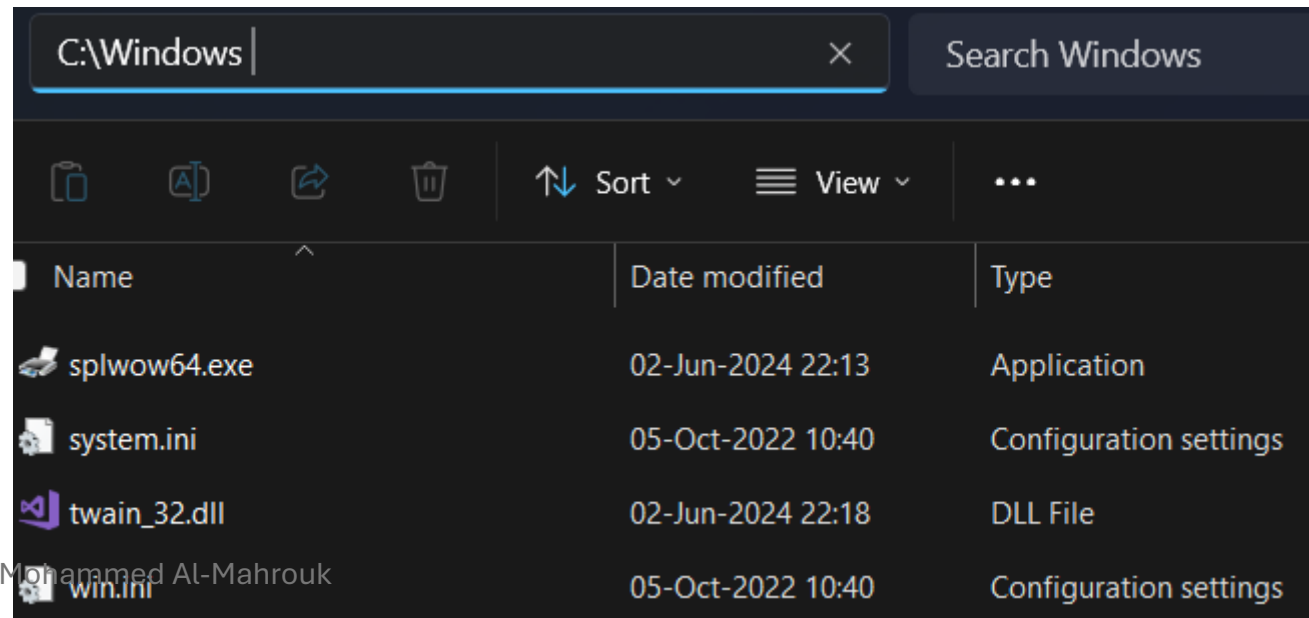
.ini Files

- **Show Hidden items.**
- **uncheck → Hide protected operating system files (Recommended)**



.ini

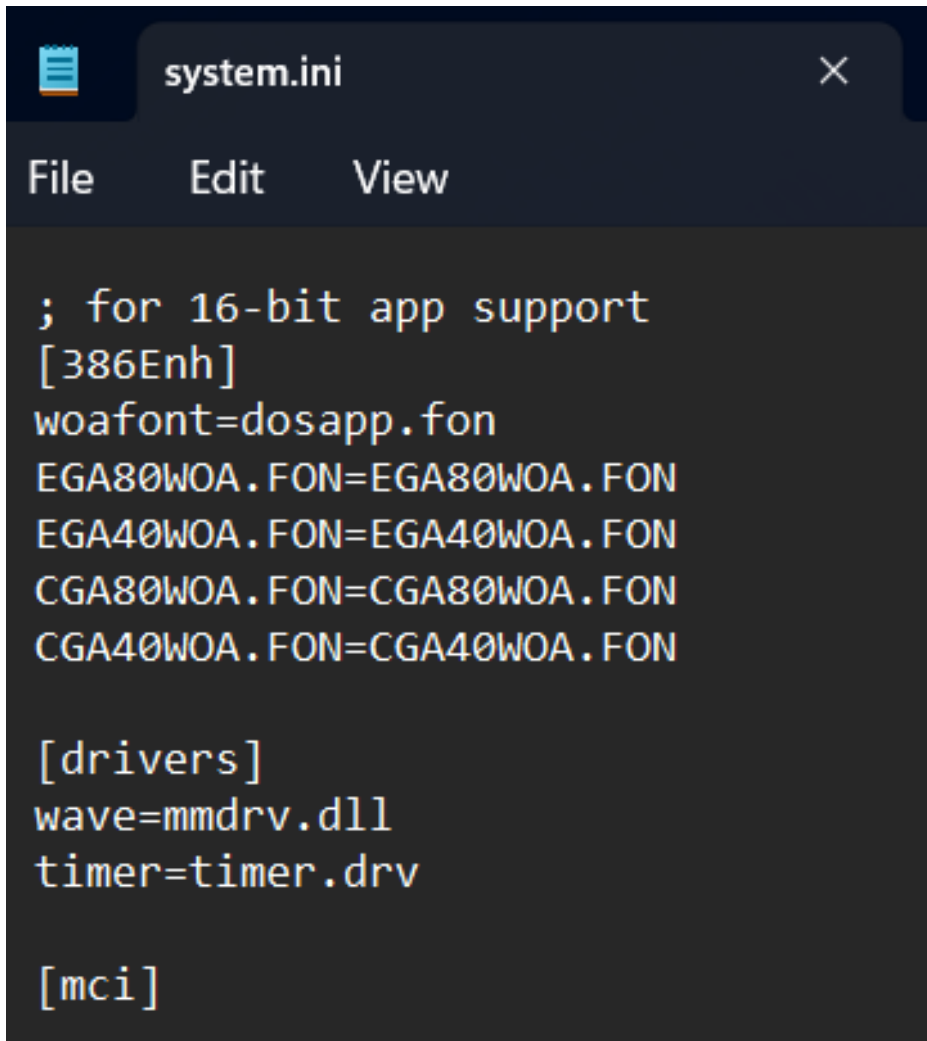
- Configuration files used by Windows operating systems.
- **System.ini**: is a legacy configuration file (older Windows), used to **configure system-level settings**, such as **device drivers, memory management**, and other **system components**.
- **Win.ini**: legacy configuration file (older Windows). store settings about **user interface and some application settings**, such as **fonts, colors**, and other **environment settings**.
- **Desktop.ini**



C:\Windows | Search Windows

Name	Date modified	Type
splwow64.exe	02-Jun-2024 22:13	Application
system.ini	05-Oct-2022 10:40	Configuration settings
twain_32.dll	02-Jun-2024 22:18	DLL File
win.ini	05-Oct-2022 10:40	Configuration settings

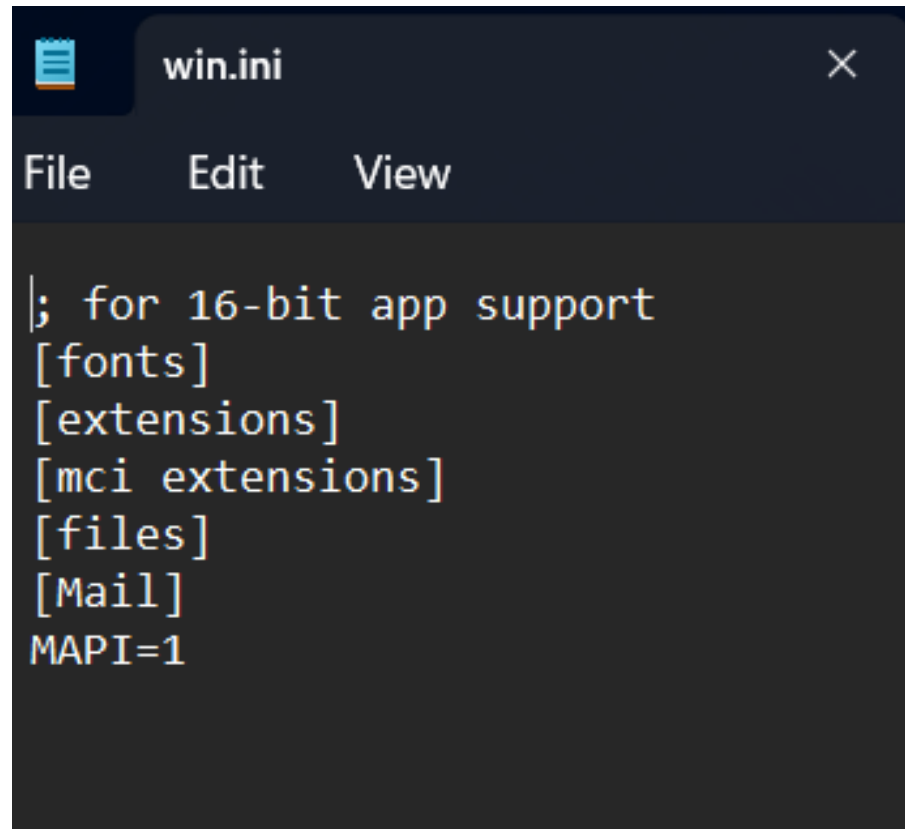
System.ini & Win.ini

A screenshot of a text editor window titled 'system.ini'. The window has a dark background and a menu bar with 'File', 'Edit', and 'View'. The text inside is as follows:

```
; for 16-bit app support
[386Enh]
woafont=dosapp.fon
EGA80WOA.FON=EGA80WOA.FON
EGA40WOA.FON=EGA40WOA.FON
CGA80WOA.FON=CGA80WOA.FON
CGA40WOA.FON=CGA40WOA.FON

[drivers]
wave=mmdrv.dll
timer=timer.drv

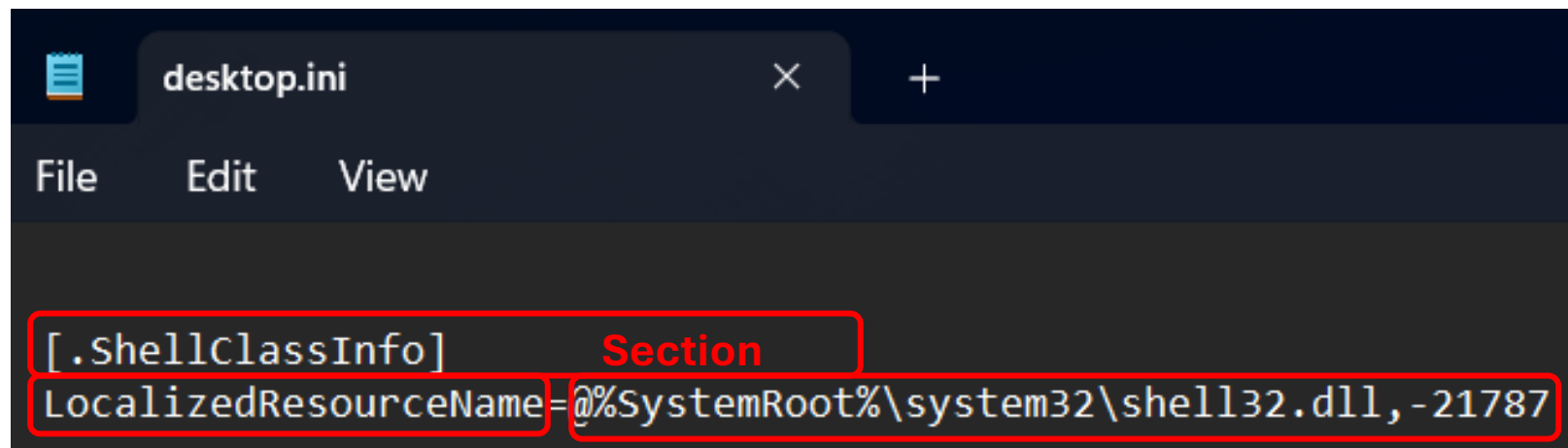
[mci]
```

A screenshot of a text editor window titled 'win.ini'. The window has a dark background and a menu bar with 'File', 'Edit', and 'View'. The text inside is as follows:

```
; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

Desktop.ini

- is used in modern versions of Windows to **store folder customization settings**. It allows users to assign a custom **icon** to a folder, change the folder's display **name**, ...etc.
- C:\Users\almah\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini

A screenshot of a Notepad window with a dark theme. The title bar shows 'desktop.ini'. The menu bar has 'File', 'Edit', and 'View'. The text area contains two lines: '[.ShellClassInfo]' and 'LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21787'. Red boxes highlight the first line and the second line. A red label 'Section' points to the first line, and a red label 'Key = Value' points to the second line.

```
[.ShellClassInfo]
LocalizedResourceName=@%SystemRoot%\system32\shell32.dll,-21787
```

Key = Value

Done By: Dana Mohammed Al-Mahrouk

C:\Windows\System32\config

- containing files that are essential for the system's configuration and operation. This directory stores the Windows Registry's hive files, which hold the configuration settings for the operating system and installed applications.
 - **SYSTEM:** Contains system-related settings, including hardware configurations, device drivers, and services.
 - **SOFTWARE:** Stores settings for installed software and applications.
 - **SAM:** Stores the Security Accounts Manager (SAM) database, which includes information about user accounts and passwords.
 - **SECURITY:** Contains security settings, including policies and permissions.
 - **DEFAULT:** Stores settings for the default user profile.
- config\RegBack: backup copies recovery in case of corruption or failure.
- .LOG: changes to the registry are correctly recorded (system updates or changes)
- C:\Windows\System32\winevt\Logs: files related to event logs

Event Viewer

FileActionViewHelp

Event Viewer (Local)

Custom Views

Administrative Events

Device Manager - Synapt

Device Manager - Synapt

Windows Logs

Application

Security

Setup

System

Forwarded Events

Applications and Services Log

Hardware Events

Intel

Internet Explorer

Key Management Service

Microsoft

Microsoft Office Alerts

OneApp_IGCC

OpenSSH

Visual Studio

Windows PowerShell

Saved Logs

Application

Subscriptions

Application

Number of events: 39,822

Level	Date and Time	Source	Event ID	Task Ca...
Information	22-Aug-2024 13:41:12	Windo...	1001	None
Information	22-Aug-2024 13:06:34	MSSQL...	17890	Server
Information	22-Aug-2024 12:45:41	MSSQL...	25753	Server
Information	22-Aug-2024 12:45:41	MSSQL...	25754	Server
Information	22-Aug-2024 12:36:54	MSSQL...	17890	Server
Information	22-Aug-2024 12:31:25	MSSQL...	17890	Server
Information	22-Aug-2024 12:27:01	MSSQL...	17890	Server
Information	22-Aug-2024 12:21:32	MSSQL...	17890	Server
Information	22-Aug-2024 12:17:01	MSSQL...	17890	Server
Information	22-Aug-2024 12:11:30	MSSQL...	17890	Server
Error	22-Aug-2024 12:06:30	Univers...	1	None
Error	22-Aug-2024 12:06:30	Univers...	1	None
Information	22-Aug-2024 12:06:30	Univers...	1	None
Error	22-Aug-2024 12:06:28	Univers...	1	None
Error	22-Aug-2024 12:06:28	Univers...	1	None
Information	22-Aug-2024 12:06:28	Univers...	1	None

Event 1001, Windows Error Reporting

GeneralDetails

Analysis symbol:

Rechecking for solution: 0

Report Id: f15a3431-8d20-430d-a7db-4b6628d5275a

Report Status: 268435464

Hashed bucket: fb30d2b9a7acf0305d4da51668259751

Cab Guid: 153cd209-e14a-4105-803b-6d8d900eba6f

Log Name:

Source:

Event ID:

Level:

User:

OpCode:

More Information:

Application

Windows Error Reporting

1001

Information

ALMAHROUK\almah

Info

Event Log Online Help

Logged:

Task Category:

Keywords:

Computer:

22-Aug-2024 13:41:12

None

Almahrouk

Actions

Application

Open Saved Log...

Create Custom View...

Import Custom View...

Filter Current Log...

Properties

Find...

Save All Events As...

View

Delete

Rename

Refresh

Help

Event 1001, Windows Error Reporting

Event Properties

Copy

Save Selected Events...

Refresh

Help

Done By: Dana Mohammed Al-Mahrouk

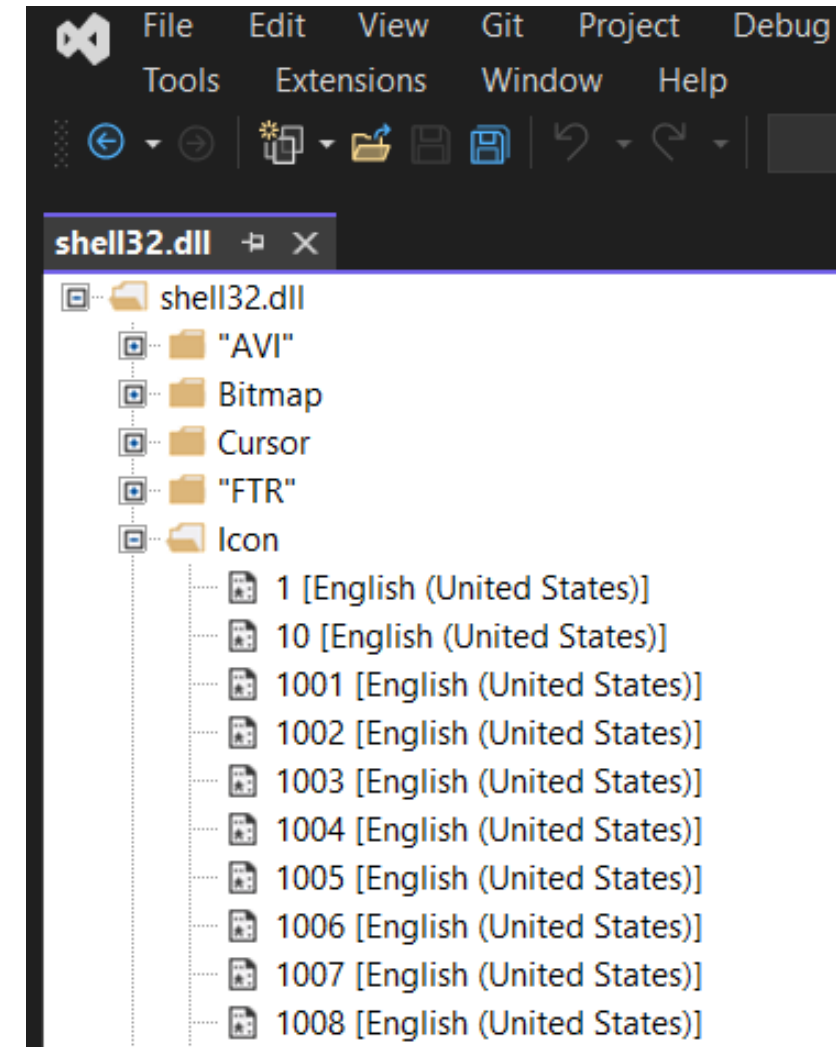
Search

13:41:58

22-Aug-2024

Ex 1: Change Folder Icon

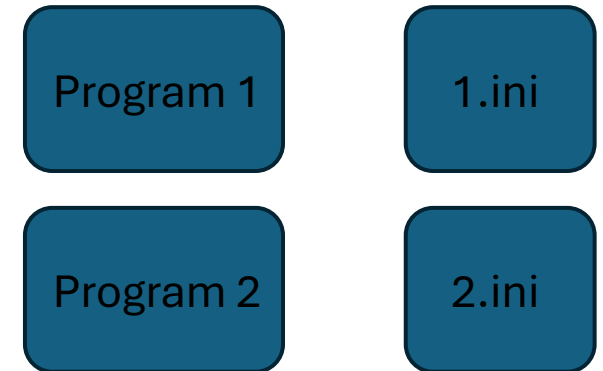
- Create folder → “My Folder” → Properties → Customize → Change Icon → Star
“C:\WINDOWS\System32\SHELL32.dll”
- Look Icons: %SystemRoot%\System32\SHELL32.dll
- Dll (Dynamic Link Library) file contain code, data, and resources that multiple programs can use to perform specific tasks, such as managing memory, displaying text, or interacting with hardware.



```
C:\Users\almah\Desktop\My Folder>attrib desktop.ini
A SH C:\Users\almah\Desktop\My Folder\desktop.ini
```

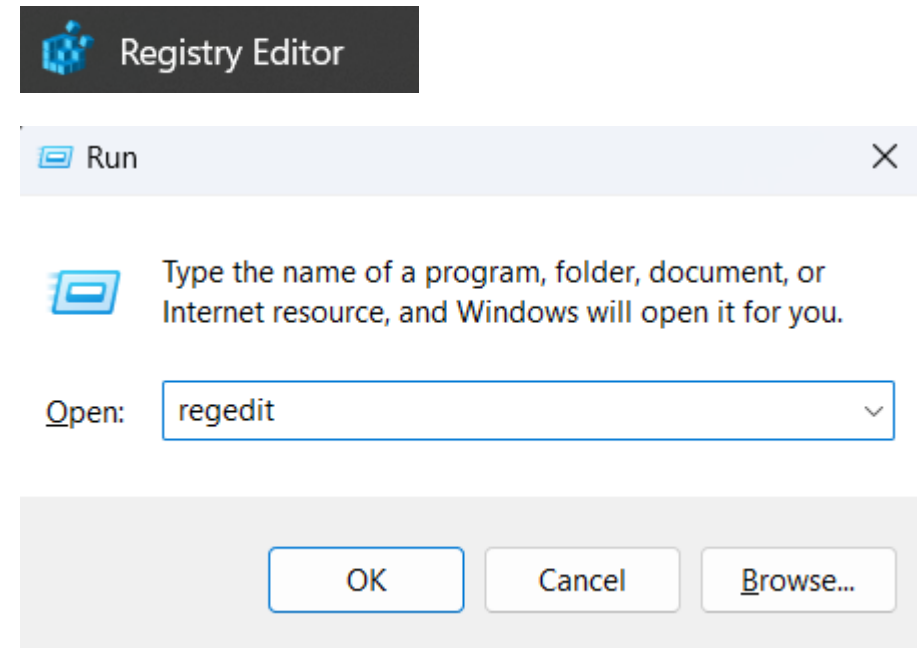
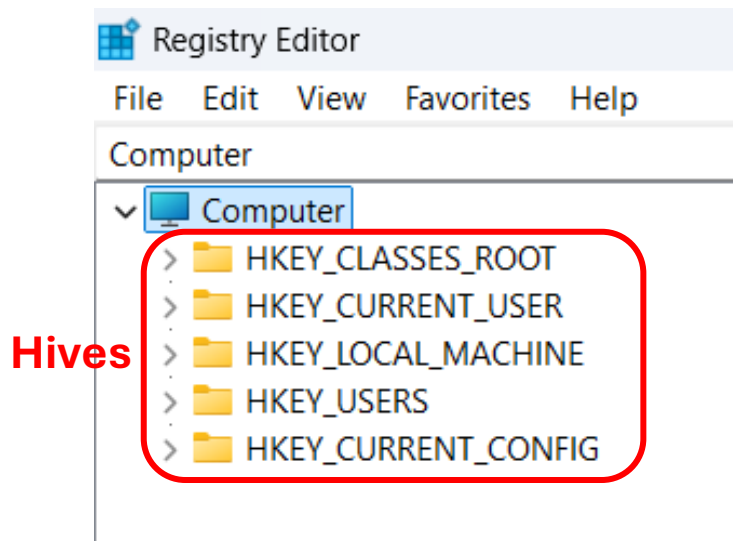
.ini Properties

- Properties of this file:
 - It can be **shared** with people & **easy editing**.
 - No **Windows permissions required** →
 - **Not registered on Windows**
 - **Problems dealing with firewall**
 - Several programs can take their settings from the same file and modify it (using the **key**) (the file is **locked**)
 - One program can take its settings from several configuration files
 - Available to **all users**
 - If the file is deleted or lost, the program will not be able to work



Windows Registry

- Started with Windows 95, Any problem with it, the operating system will not work, install a new Windows
- Open
 - Registry Editor
 - Win + R → regedit



Registry Editor

File Edit View Favorites Help

Computer\HKEY_CURRENT_USER\Console\%%Startup

Computer

HKEY_CLASSES_ROOT

HKEY_CURRENT_USER

AppEvents

Console

%%Startup

%SystemRoot%_System32_Win

%SystemRoot%_SysWOW64_W

C:_Users_almah_Downloads_cn

ConEmu

Hives

Keys

Sub-Keys

Name	Type	Data	Values
(Default)	REG_SZ	(value not set)	
DelegationConsole	REG_SZ	{00000000-0000-0000-0000-000000000000}	
DelegationTerminal	REG_SZ	{00000000-0000-0000-0000-000000000000}	

Value name

Value type

Value data

Windows Registry Editor



- Centralize place that save some application configuration setting.
- Is a hierarchical DB that store configuration setting & option on Microsoft OS it used to share information about the system, application & users.
- Application → (color, font size, screen size, path install program & setting, version ,update & upgrade)
- Device → (name, username, language, time zone, disktop background, keyboard – mouse – screen setting, power, ...etc)
- Windows + NIC + Firewall + ...
- You can backup Registry Editor.

Value Data Types

1. REG_SZ (String Value) → file paths, names
2. REG_MULTI_SZ (Multi-String Value) → list of values or multiple file paths (\0)
3. REG_EXPAND_SZ (Expandable String Value) → automatically expanded (dynamic) by the system. (environment variables like `%SystemRoot%` or `%ProgramFiles%`)
4. REG_DWORD (32-bit Number) → numeric values, such as flags, counters (`0x00000001`)
5. REG_QWORD (64-bit Number) → large numeric values (`0x0000000000000001`)

Value Name

- Default Value (Unnamed Value): `(Default)` or `@` → store the primary or most important setting for that key.
- Named Values: specific names that identify the type of data stored in them.
 - `Path` : Stores file paths or directory locations.
 - `Version` : Indicates the version of an application or component.
 - `Enabled` : A flag, often stored as a `REG_DWORD`, indicating whether a feature is enabled (`1`) or disabled (`0`).
 - `(Default)` : The unnamed default value, often used for primary settings.
 - `DisplayName` : Stores the name of an application or service as it should appear in the user interface.
 - `ServiceDll` : Specifies the DLL used by a service

Hives



1. HKEY_CLASSES_ROOT (HKCR):

Contains file associations and OLE (Object Linking and Embedding) object classes. It links file extensions to the applications that handle them and defines the COM (Component Object Model) objects used by applications.

Usage: When you double-click a file in Windows Explorer, the settings in this hive determine which application is launched to open the file.

HKEY_CURRENT_USER\SOFTWARE\CLASSES

HKEY_LOCAL_MACHINE → Software → Classes → .docx → Word.Document.12 → ShellNew
→ File Name

16-bit programmer

Hives



2. HKEY_CURRENT_USER (HKCU): (User Level)

configuration settings for the currently logged-in user. It includes settings like desktop configurations, user-specific software configurations, and user preferences.

The hive is stored in the `**Ntuser.dat**` file located in the user's profile directory (`C:\Users\Username`).

Ex: Run App Automatically when device Run

HKEY_CURRENT_USER → Software → Microsoft → Windows → CurrentVersion → Run

To Add: right click → new → String Value → [Name], → modify → Value Data → [path.exe]

Ex: HKEY_CURRENT_USER → Software → Adobe → Photoshop → 160.0

Ex: HKEY_CURRENT_USER → Software → Python → PythonCore → 3.10

Hives



3. HKEY_LOCAL_MACHINE (HKLM): (Device Level)

Stores settings and configurations that apply to all users on the computer.

Contains system-wide settings such as hardware configurations, installed software, system services, and more.

- Subkeys:
 - A. **SAM**: Security Accounts Manager database, which stores user account information.
 - B. **SECURITY**: Security-related settings, policies, and audit settings.
 - C. **SYSTEM**: System configuration, including services and drivers.
 - D. **SOFTWARE**: Installed software information and their settings.

Hives

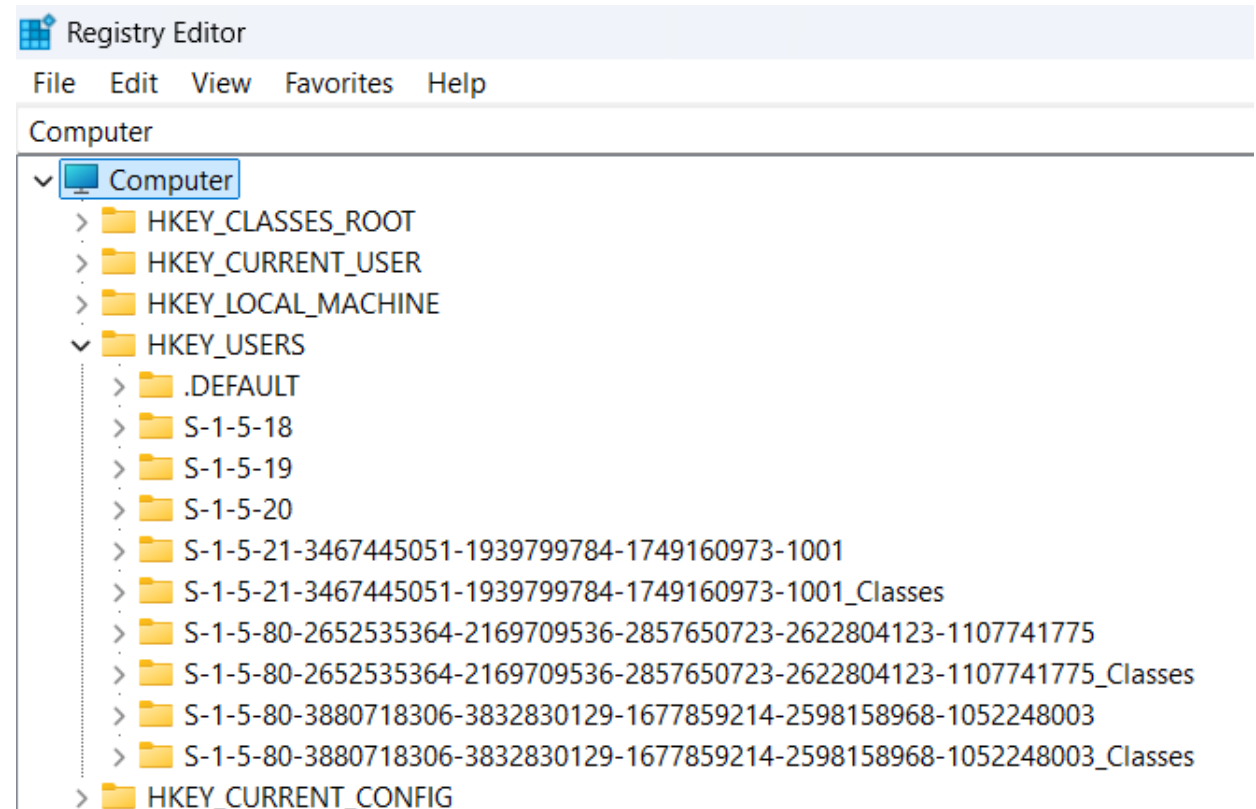
4. HKEY_USERS (HKU):

Contains settings for all user profiles on the computer.

including the default profile and the currently logged-in user's settings.

- SID (Security identifier)
- User ID

HKEY_CURRENT_USER &&
HKEY_USERS



Hives



5. **HKEY_CURRENT_CONFIG (HKCC):**

Provides a snapshot of the current hardware configuration, including settings that are dynamic and change depending on the hardware state.

Add & Remove program



- program's GUID (Globally Unique Identifier)
- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NlaSvc\Parameters\Internet
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile

Control Panel → Mouse

- Mouse:
- Computer\HKEY_CURRENT_USER\Control Panel\Mouse
- MouseSensitivity → change
- SwapMouseButton = 1
- Key Name
- Data Type

Value name:

SwapMouseButton

Value data:

1



Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveWindowTracking	REG_DWORD	0x00000000 (0)
Beep	REG_SZ	No
DoubleClickHeight	REG_SZ	4
DoubleClickSpeed	REG_SZ	340
DoubleClickWidth	REG_SZ	4
ExtendedSounds	REG_SZ	No
MouseHoverHeight	REG_SZ	4
MouseHoverTime	REG_SZ	400
MouseHoverWidth	REG_SZ	4
MouseSensitivity	REG_SZ	12
MouseSpeed	REG_SZ	1
MouseThreshold1	REG_SZ	6
MouseThreshold2	REG_SZ	10
MouseTrails	REG_SZ	0
SmoothMouseXCurve	REG_BINARY	00 00 00 00 00 00
SmoothMouseYCurve	REG_BINARY	00 00 00 00 00 00
SnapToDefaultButton	REG_SZ	1
SwapMouseButton	REG_SZ	0

Control Panel → Desktop

- Computer\HKEY_CURRENT_USER\Control Panel\Desktop
- Wallpaper



Value name:
WallPaper
Value data:
<u>C:\WINDOWS\web\wallpaper\Windows\img19.jpg</u>

Disk Space Message



- Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies
- → right click → new key → Explorer → right click → new Dword → “NoLowDiskSpaceChecks” = 1
- **Message Confirm Delete File of Folder**
- Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies
- right click → new Dword → “ConfirmFileDelete” = 0

Login as a Guest

- No password
- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa



Value name:

forceguest

Value data:

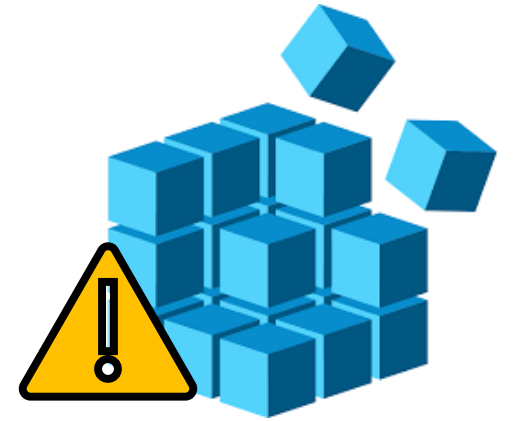
1

Add Item to right click menu






- Computer\HKEY_CLASSES_ROOT\Directory\Background\shell
- Then right click → New → key → <put name> → right click → key → “command” → data value of default name “Program path.exe”

Turn Off Firewall



- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile
- DisableNotifications = 0
- EnableFirewall = 0

Name	Type	Data
 (Default)	REG_SZ	(value not set)
 DisableNotifications	REG_DWORD	0x00000001 (1)
 EnableFirewall	REG_DWORD	0x00000001 (1)

Open Port



- Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules

Virus/Program Run when Windows Open



- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- New string → Data Value = “program path”



Thank You

Done By: Dana Mohammed Al-Mahrourk