his is the missing piece you forgot:  
✅ winload.efi is the one who loads:

* ntoskrnl.exe
* system32\drivers\\*.sys
* \Windows\System32\Config\SYSTEM → (registry hive)

1. PSU turns on → BIOS/UEFI starts → POST

2. BIOS/UEFI loads bootloader (bootmgr or bootmgfw.efi)

3. Bootloader loads winload.efi

4. winload.efi:

- Loads ntoskrnl.exe

- Loads hal.dll

- Loads SYSTEM registry hive

- Loads boot-critical drivers

5. winload.efi passes control to ntoskrnl.exe

6. Kernel initializes memory, process scheduler, device manager

7. Loads SMSS.exe → starts session 0 (boot session)

8. Loads csrss.exe, wininit.exe, services.exe

9. Starts user login process (winlogon, lsass)

10. GUI boots up

Network stack is the main point which creates and sends the packets in the internet

|  |  |
| --- | --- |
| C:\Windows | The **heart** of the OS, where Windows lives |
| C:\Program Files | Default location for **64-bit apps** |
| C:\Program Files (x86) | For **32-bit apps** on 64-bit Windows |
| C:\Users | Stores user profiles, documents, downloads |
| C:\Users\Shadow | Your home directory (/home/shadow in Linux) |
| C:\ProgramData | Shared data between applications (like /var in Linux) |
| C:\System Volume Information | Stores **system restore** data and volume info |
| C:\$Recycle.Bin | Hidden folder that stores deleted files (Recycle Bin) |
| C:\pagefile.sys | Virtual memory (paging file) |
| C:\hiberfil.sys | Used when system hibernates |
| C:\bootmgr | Boot manager file, part of the bootloader |
| C:\Recovery | Contains recovery environment tools |

**C:\Windows Folder — Where the OS Lives**

This is like /etc, /bin, /lib, /boot, /var **all in one** for Windows.

| **Subfolder** | **Purpose** |
| --- | --- |
| System32 | Core OS binaries, drivers, services, DLLs (like /bin + /lib) |
| SysWOW64 | For 32-bit DLLs and apps on 64-bit systems |
| WinSxS | Component Store (like version control of OS DLLs) |
| Temp | Temp files used by Windows |
| Logs | Logs of updates and system events |
| assembly | Stores Global Assembly Cache (GAC) for .NET |
| Fonts | Fonts installed on the system |
| explorer.exe | GUI shell of Windows (taskbar, start menu) |

C:\

├── Windows\

│ ├── System32\

│ ├── SysWOW64\

│ ├── WinSxS\

│ └── Temp

├── Program Files\

├── Program Files (x86)\

├── Users\

│ └── Shadow\

│ └── AppData\

│ ├── Roaming\

│ ├── Local\

│ └── LocalLow\

├── ProgramData\

├── bootmgr

└── pagefile.sys

**1. 📁 C:\Windows**

**📌 What it is:**

This is the **main OS directory**, like /etc or /lib in Linux.

**🎯 When it's used:**

Every time the system boots or you run any system-level task, this folder gets involved.

**🧪 Example:**

* When you log in, explorer.exe from C:\Windows launches your desktop and taskbar.
* When you run commands like ipconfig, it’s using ipconfig.exe from System32.
* **📁 C:\Windows\System32**
* **📌 What it is:**
* This folder contains all the **core system executables, drivers, and DLLs**.
* **🎯 When it's used:**
* Every time you run something like:

ping google.com

It runs ping.exe from this folder.

**💡 Real-world:**

* services.exe → Manages background services
* lsass.exe → Handles authentication (can be dumped for password hashes)
* taskmgr.exe → Task Manager GUI
* regedit.exe → Registry Editor

**C:\Program Files & C:\Program Files (x86)**

**📌 What it is:**

Default folder for installed applications:

* Program Files = 64-bit apps
* Program Files (x86) = 32-bit apps

**🎯 When it's used:**

Every time you launch a third-party app like **Chrome**, **Wireshark**, or **Notepad++**, it’s pulled from here.

**💡 Real-world:**

* C:\Program Files\Wireshark\wireshark.exe → launches the network capture tool.

**C:\Users\Shadow**

**📌 What it is:**

Your user profile — contains documents, desktop, downloads, settings.

**🎯 When it's used:**

Every time you log in, Windows loads your profile from here.

**💡 Real-world:**

* C:\Users\Shadow\Downloads\payload.exe ← User runs a file from here.
* C:\Users\Shadow\Desktop\report.docx ← Daily files live here

**📁 C:\Users\Shadow\AppData\Roaming**

**📌 What it is:**

Stores **user-specific app settings** that roam with you (useful in domain environments).

**🎯 When it's used:**

Apps like Discord, Python, Firefox, or VSCode store settings here.

**💡 Example:**

* C:\Users\Shadow\AppData\Roaming\Python\Python310\Scripts\ ← Python scripts live here

**C:\Users\Shadow\AppData\Local**

**📌 What it is:**

Non-roaming, machine-specific settings.

**🎯 When used:**

Apps like Chrome, Edge, and Windows store cache and local files here.

**💡 Example:**

* Local\Google\Chrome\User Data ← Your saved passwords, cookies, sessions

**📁 C:\ProgramData**

**📌 What it is:**

Shared folder between all users, used by installers, antivirus, and services.

**🎯 When it's used:**

* Antivirus definitions
* App licensing
* Shared logs

**💡 Example:**

* C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup ← Startup shortcut for all user

**C:\Windows\Temp and %TEMP%**

**📌 What it is:**

Temporary files, installer cache, etc.

**🎯 When used:**

During software install, extract zip files, or browsing.

**💡 Example:**

* C:\Users\Shadow\AppData\Local\Temp\setup.msi

**📁 C:\Windows\System32\config**

**📌 What it is:**

Stores the **Registry hives** (SAM, SYSTEM, SECURITY, etc.)

**🎯 When used:**

Every time the system boots, or an app runs — this is your **Windows brain**

**💡 Real-world:**

* SAM = Has user hashes (can be dumped via reg save + hashcat or John)
* SYSTEM = Decryption key for SAM
* SECURITY = Local security policy

**💣 bootmgr, BCD, winload.efi**

**📌 What it is:**

Part of the **bootloader**

**🎯 When used:**

On system startup

**💡 Example:**

* bootmgr = Boot manager
* BCD = Boot configuration database
* winload.efi = Loads kernel + drivers