Windows Memory Architecture and Registry Analysis

1.1 Memory Allocation and Handles

A computer operates by storing instructions temporarily in RAM until the CPU processes them. Each process on a system has access to a set of virtual addresses. These addresses aren't physical memory locations but are mapped through a page table to physical memory locations.

- **32-bit Windows**: Can address up to 4 GB of virtual memory.
- **64-bit Windows**: Can address up to 8 TB of virtual memory.

Each user process operates in its **own private virtual address space**. To access kernel resources, a user-mode process must use **process handles**. These handles serve as indirect references, ensuring security and isolation.

Tool: RAM_Map

- **Function**: Visualizes how Windows allocates system memory.
- **Source**: Part of the **Sysinternals Suite** by Microsoft.

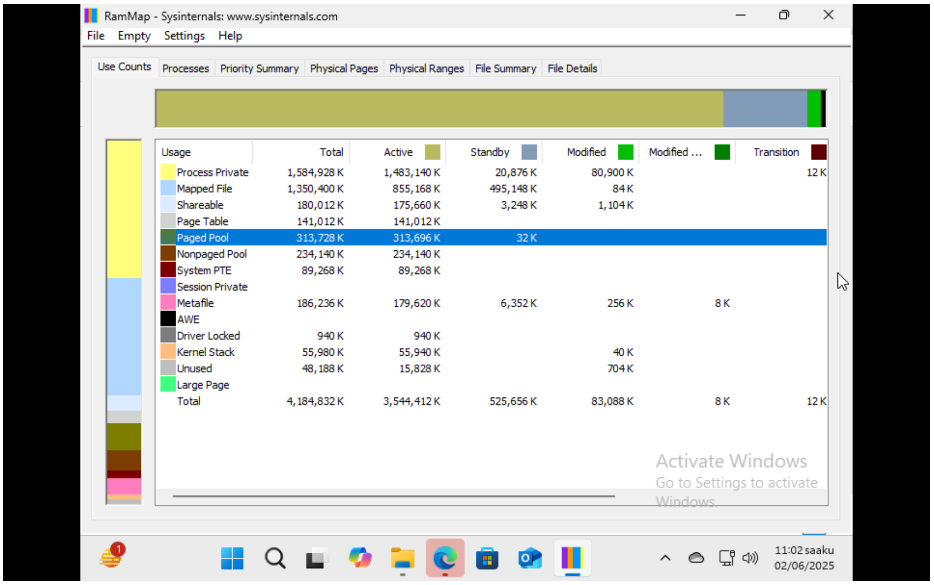

Fig: RAM_MAP

RAMMap gives detailed views on memory usage by processes, drivers, and the kernel. It's especially useful for memory forensic analysis

1.2The Windows Registry

The **Windows Registry** is a hierarchical database that stores configuration settings and options for the operating system and installed applications.

- Top-level containers are called **Hives**.
- Each hive contains **keys**, **subkeys**, and **values**.
- Registry editing can impact system stability, so changes should be made cautiously.

Main Registry Hives:

- **HKEY_CURRENT_USER (HKCU)** – Settings for the currently logged-in user.
- **HKEY_USERS (HKU)** – All user profiles.
- **HKEY_CLASSES_ROOT (HKCR)** – File type associations and OLE data.
- **HKEY_LOCAL_MACHINE (HKLM)** – Hardware, software, and system data.
- **HKEY_CURRENT_CONFIG (HKCC)** – Hardware profile used at boot.

Registry Value Types:

- **REG_BINARY** – Binary data.
- **REG_DWORD** – 32-bit numbers.
- **REG_SZ** – String data.

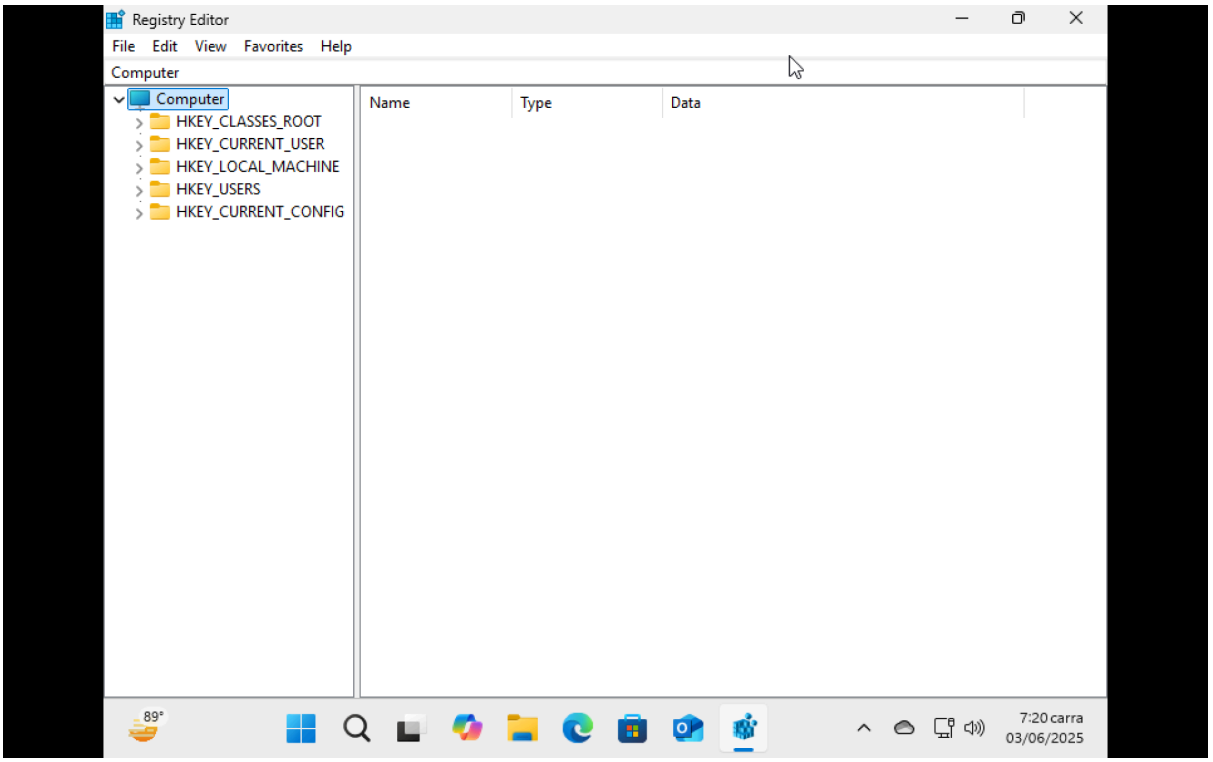

Fig: Windows Registry Hives

Tool: Regedit (regedit.exe)

Used to view and edit the registry. Shows hierarchical tree on the left and data on the right. Misuse can cause severe system issues.

Security Risks:

- Malware like **keyloggers** or **RATs** may hide startup entries in the registry.
- Tracks user activities, document access, and connected devices – valuable in **digital forensics**.

Note: The details related to **Windows Memory Architecture** and **Registry Analysis** in this report are referenced from **CISO Academy**'s cybersecurity training materials.

Reference Link:

https://www.netacad.com/courses/operating-systems-basics?courseLang=en-US