**Task 7: Identify and Remove Suspicious Browser Extensions**

**Objective:**  
To learn how to spot and remove potentially harmful browser extensions that may compromise security or privacy.

**Tools Used:**

* Google Chrome Browser (latest version)

**Procedure:**

1. Opened Google Chrome.
2. Navigated to Menu (⋮) → More Tools → Extensions.
3. Carefully reviewed the list of installed extensions.
4. Checked for any:
   * Unknown or unrecognized extensions
   * Extensions with excessive permissions
   * Extensions with suspicious names or no publisher information
   * Disabled but still installed extensions
5. Verified that there were no extensions installed.

**Findings:**

* **Number of Extensions Found:** 0
* No browser extensions were present in the system, hence no suspicious or malicious extensions were detected.

**Action Taken:**

* No action required as there were no extensions installed.

**Security Notes:**

* Having no unnecessary extensions reduces the risk of data leaks, browser hijacking, and malicious script execution.
* Extensions can potentially capture browsing history, keystrokes, or login data if malicious. Regular checks are a good cybersecurity habit.

**Conclusion:**  
The browser is clean and free from any installed extensions, ensuring reduced attack surface and improved privacy.