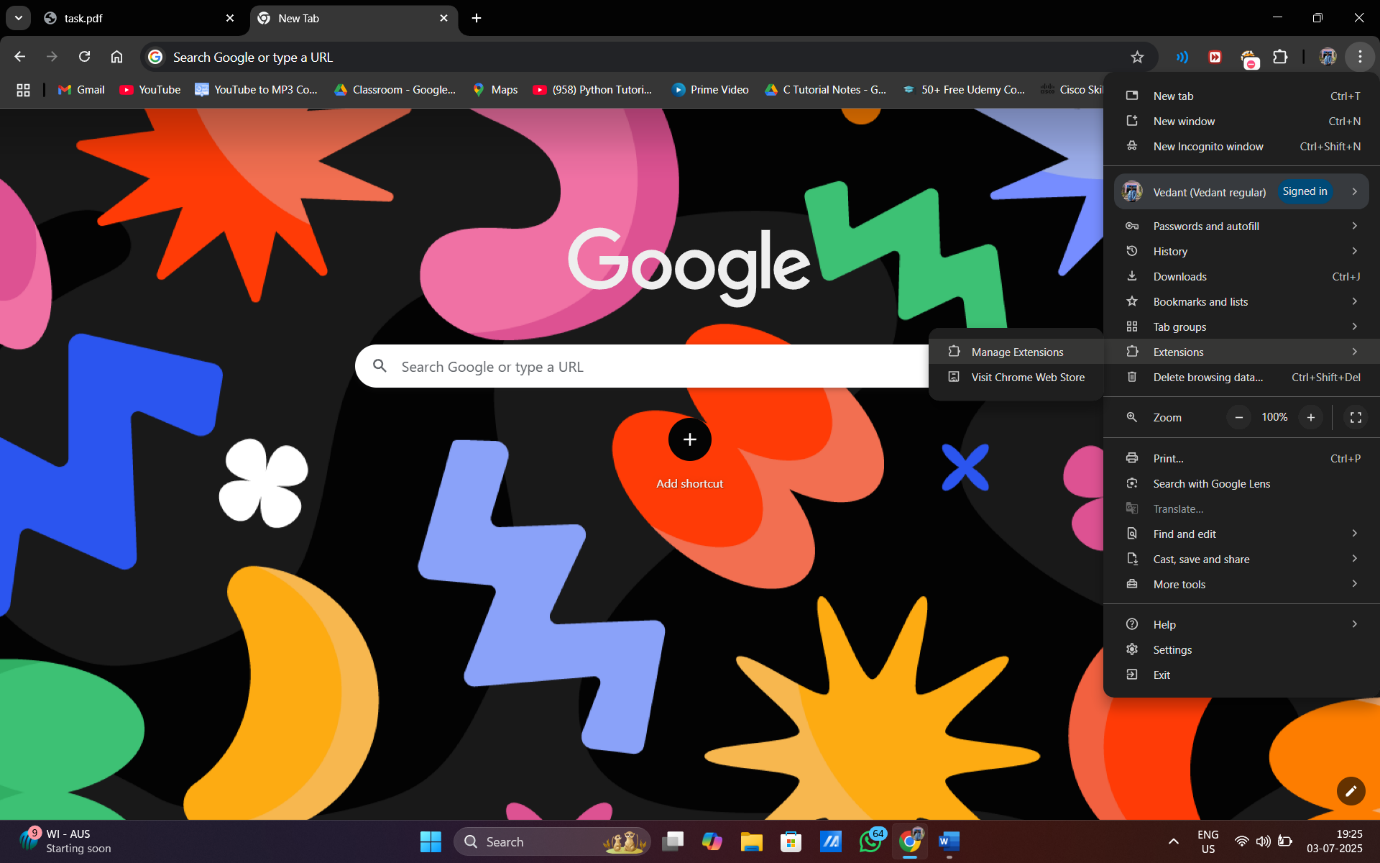
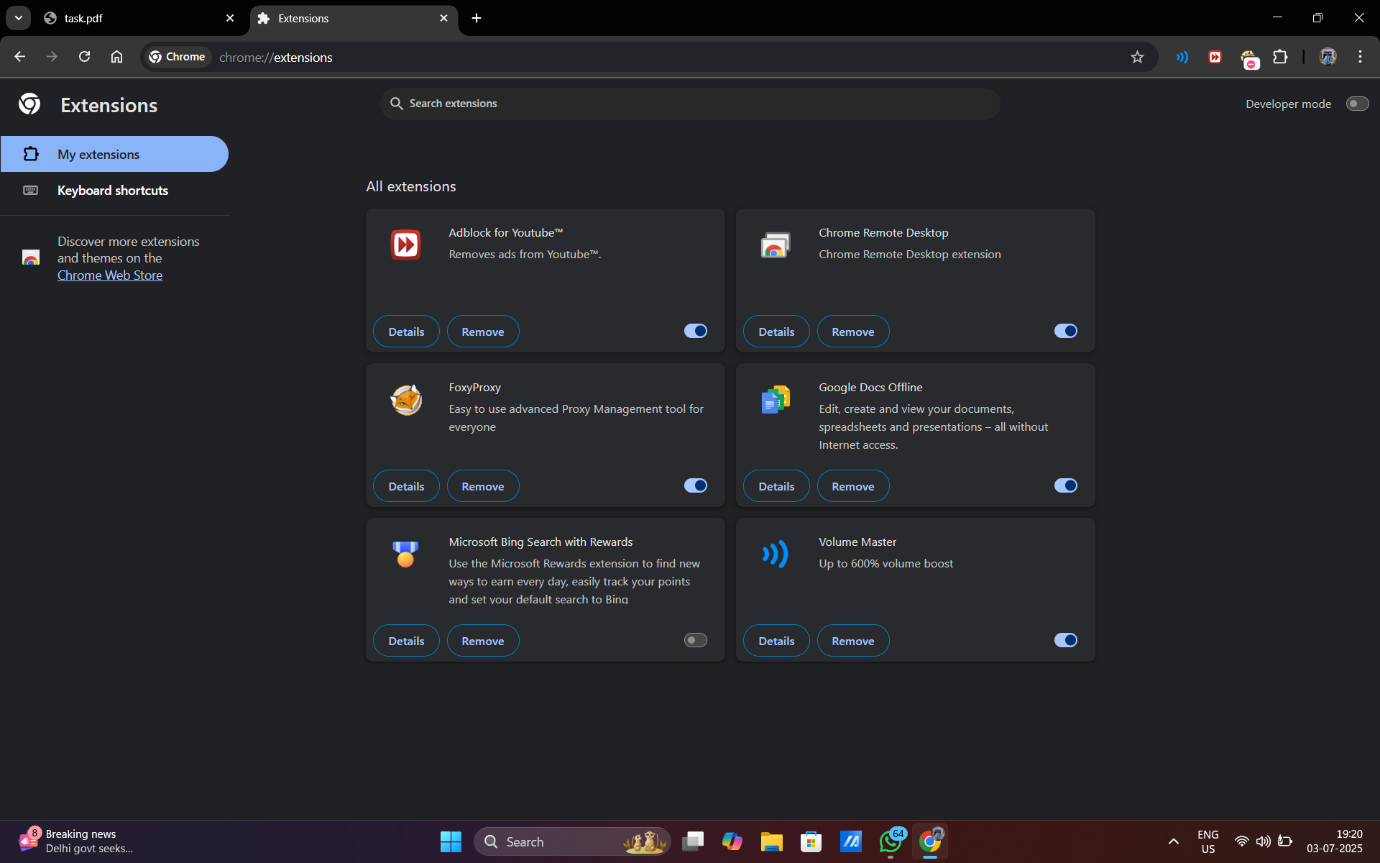
**Task 7 :Identify and Remove Suspicious Browser Extensions**

****

Here we go to settings and in settings we find extensions and then go to manage extension

****

**Here is the list of extension installed in my computer**

**Ad block for youtube**

**Chrome remote desktop**

**Foxyproxy**

**Google docs offline**

**Microsoft bing search**

**Volume master**

**Ad block for youtube:- block youtube ads**

**Permissions**

* **Read your browsing history**
* **Block content on any page**

**Chrome remote desktop:- Chrome Remote Desktop extension help to use pc chrome using phone**

**Permissions**

* **Manage your downloads**
* **Communicate with cooperating native applications**

**Foxyproxy:-** **Easy to use advanced Proxy Management tool for everyone**

**Permissions**

* **Read and change all your data on all websites**
* **Display notifications**
* **Manage your downloads**

**Google docs offline:-** **Edit, create and view your documents, spreadsheets and presentations – all without Internet access.**

**Permissions**

**Not available**

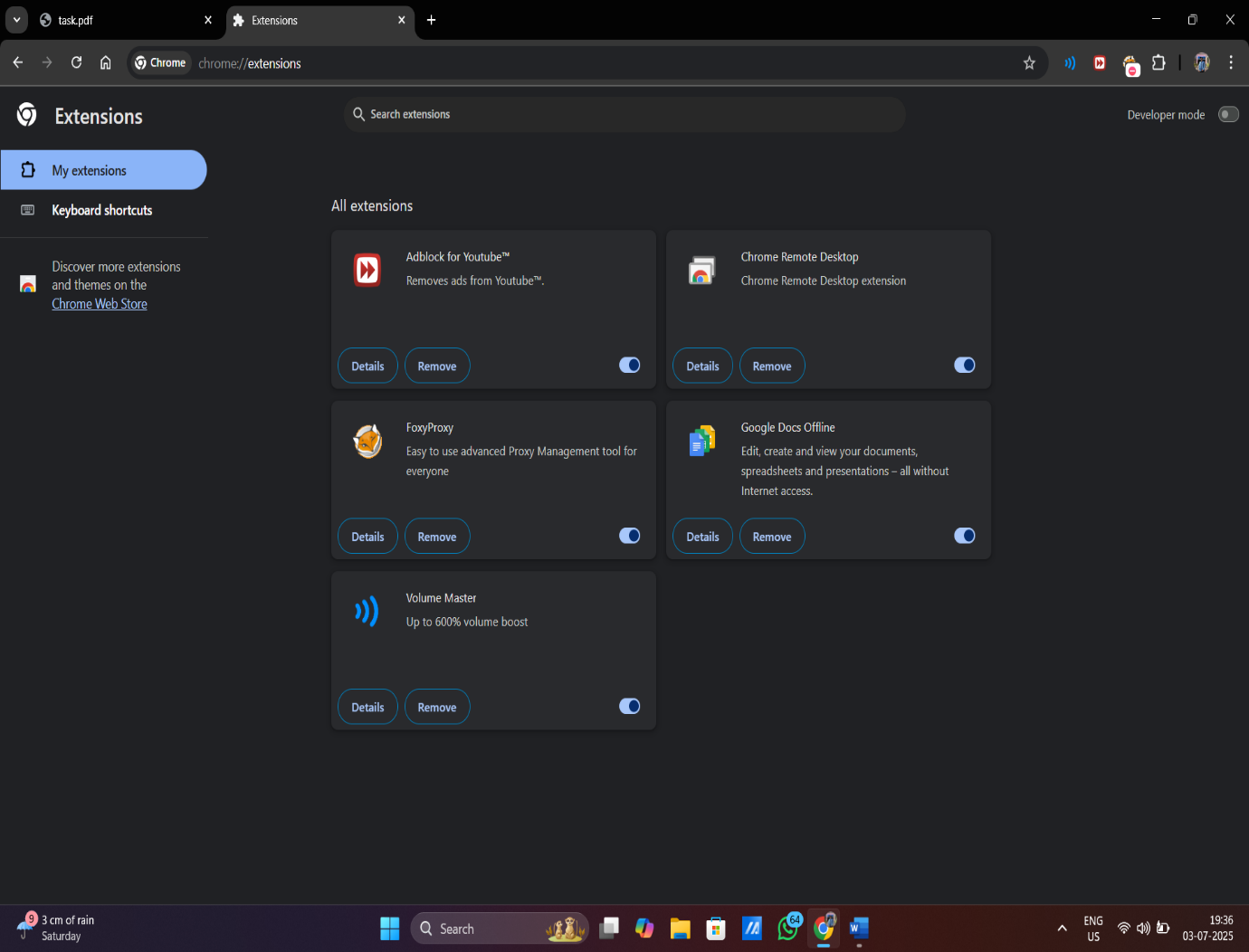
**Microsoft bing search**

**Here I remove it as it is unnecessary**

**Volume Master:-** **Up to 600% volume boost**

**Permissions**

* **Read and change all your data on all website**

**Here is the final screen shot of item being removed **

**how malicious extensions can harm users**

**Malicious browser extensions can cause significant harm to users by stealing sensitive information, hijacking accounts, injecting ads, and even installing malware. They can compromise personal data like browsing history, passwords, payment details, and session cookies. Attackers can also use them to manipulate search results, redirect traffic, and steal cryptocurrency.**