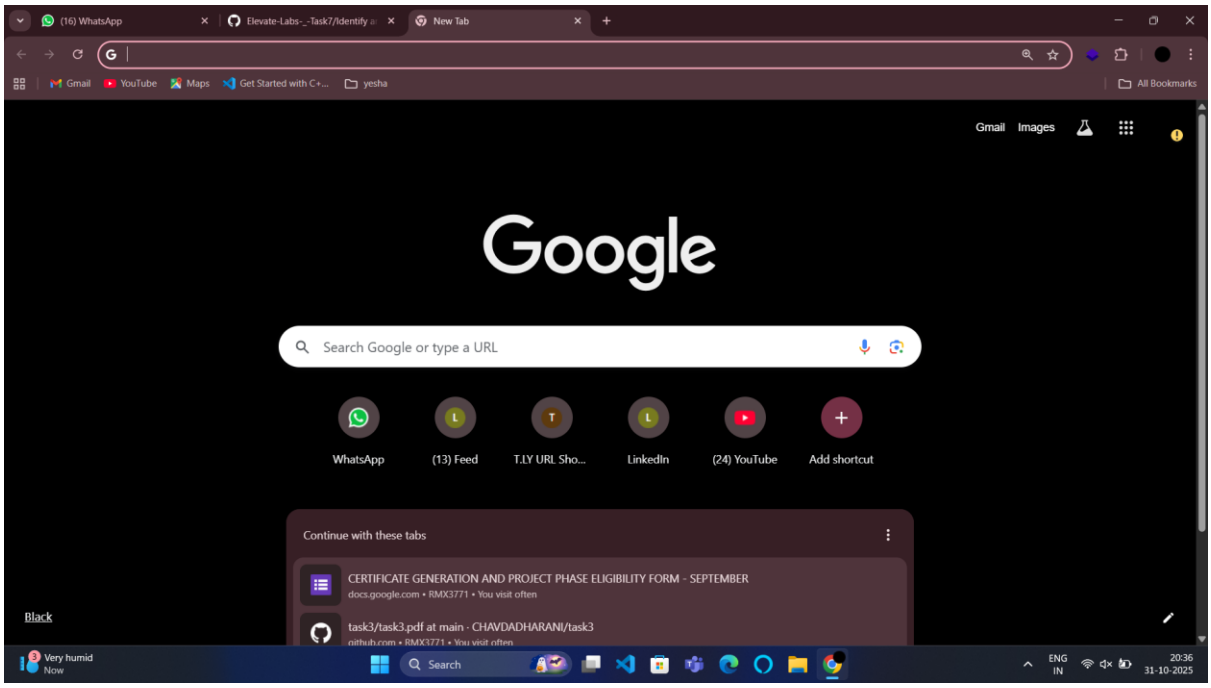
Task 7: Identify and Remove Suspicious Browser Extensions

Aim: Learn to spot and remove potentially harmful browser extensions.

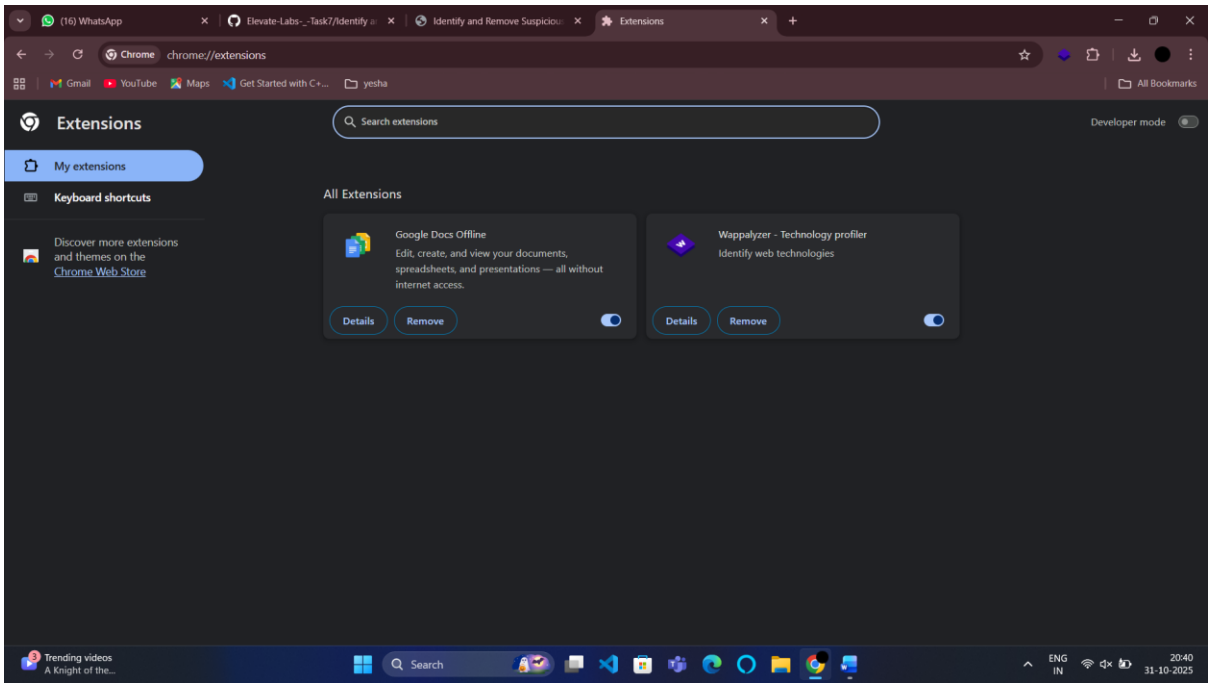
Requirements: Any web browser.

Steps:

1. Open the browser.

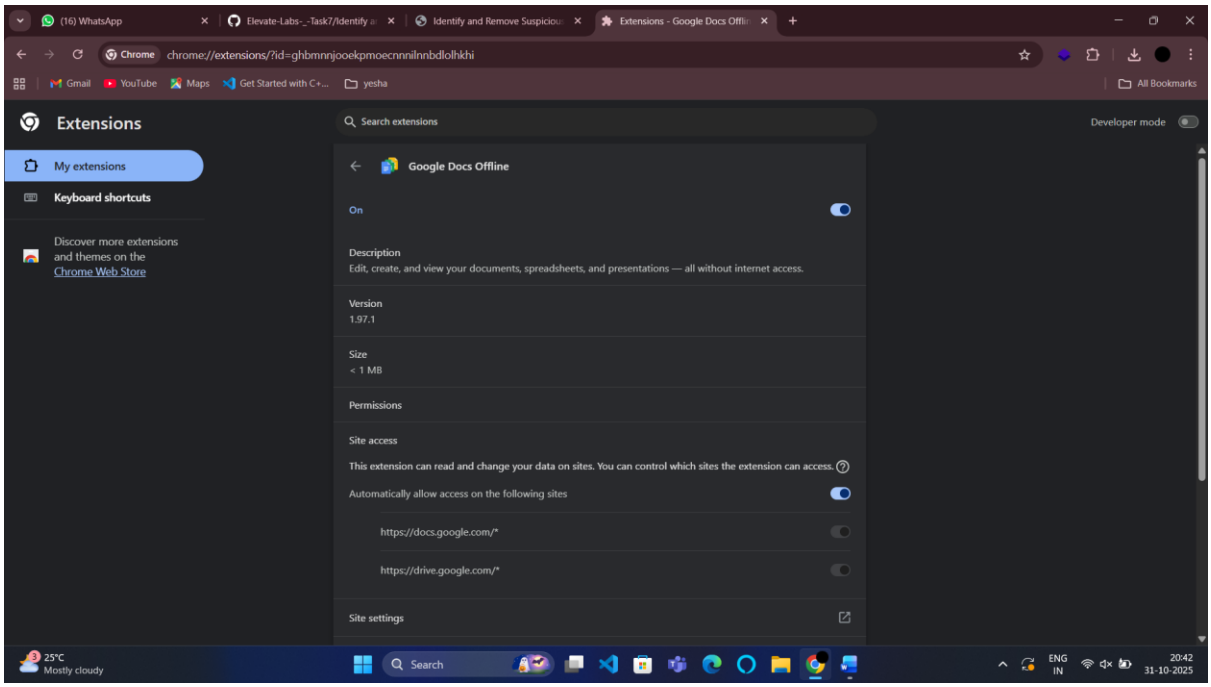


2. Then open the browser's Extensions/Add-ons Manager.

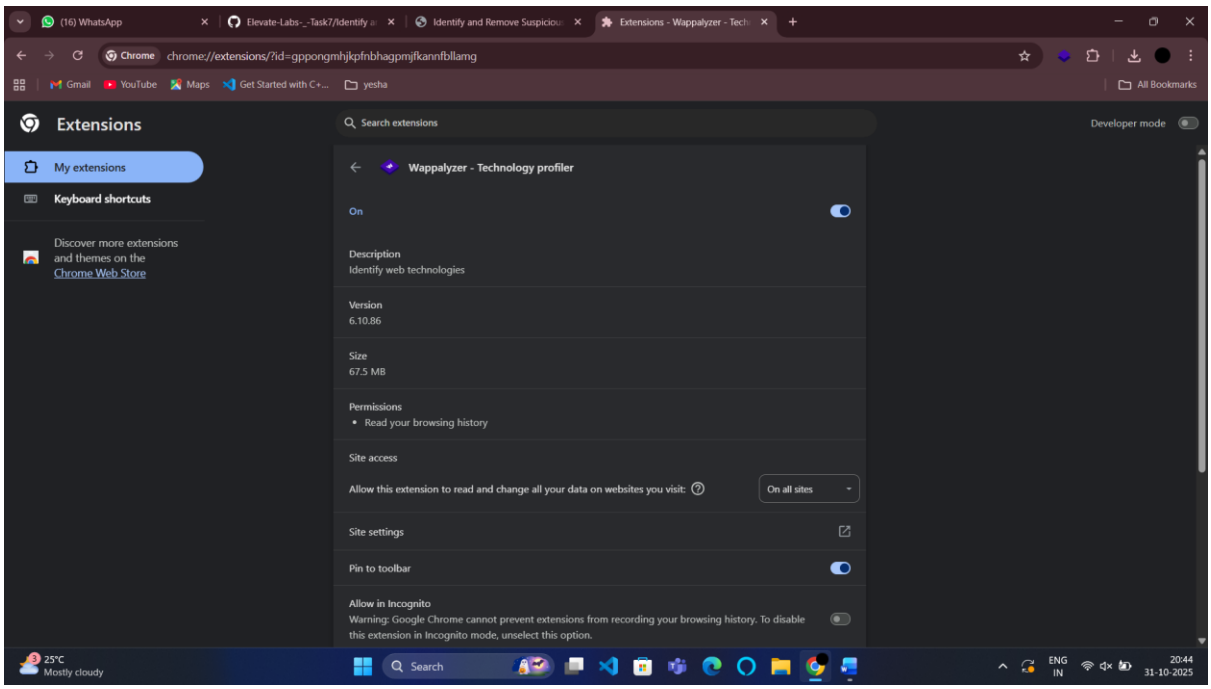


3. Review all installed extensions.

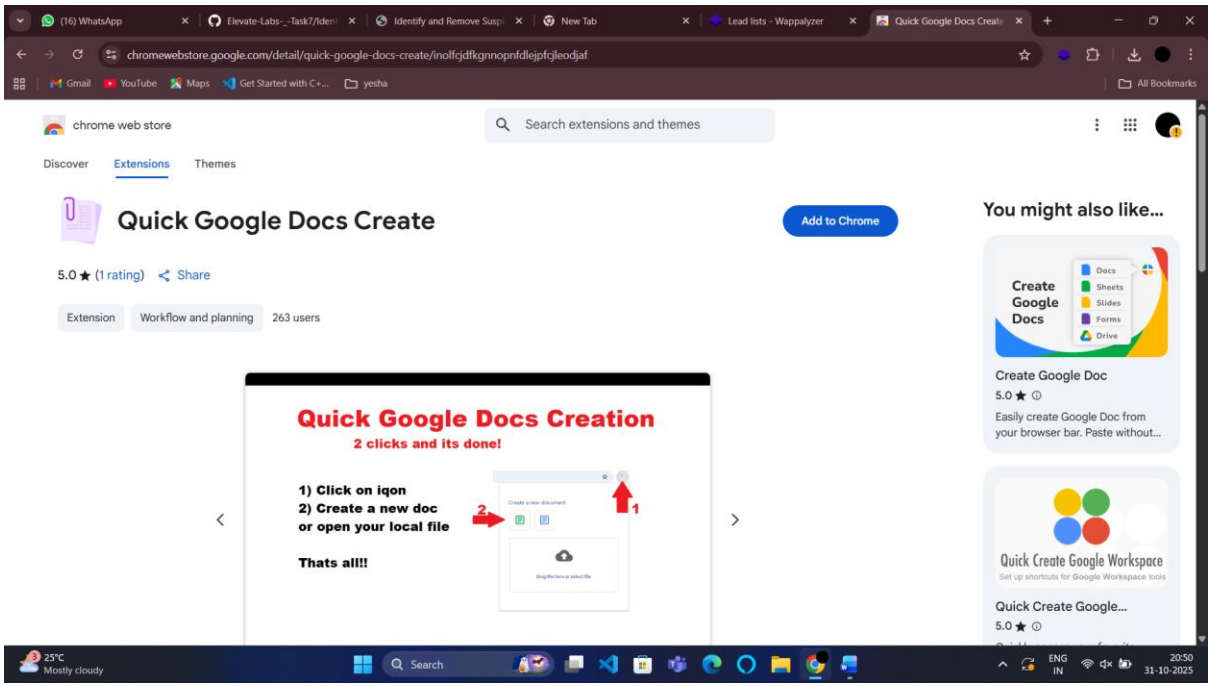
I. Add to Google Chrome

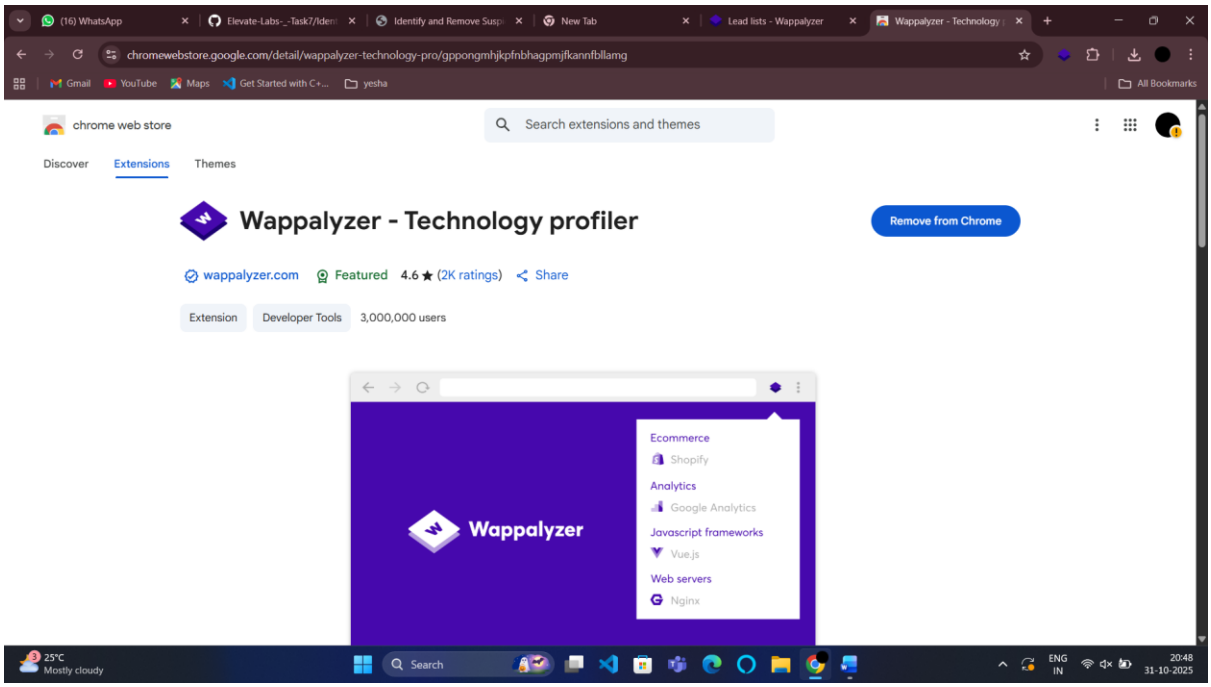


II. Wappalyzer– Technology profiler Identify web technologies



4. Check each one’s permissions and user reviews.





Name:- Wappalyzer - Technology profiler

Permission:- • Read your browsing history • This extension can read and change all your data on websites you visit

User Review out of 5 :- 4.6

Source:- Chrome Web Store

Assessment and Reason:-

Wappalyzer – Medium Risk (Keep if Needed):

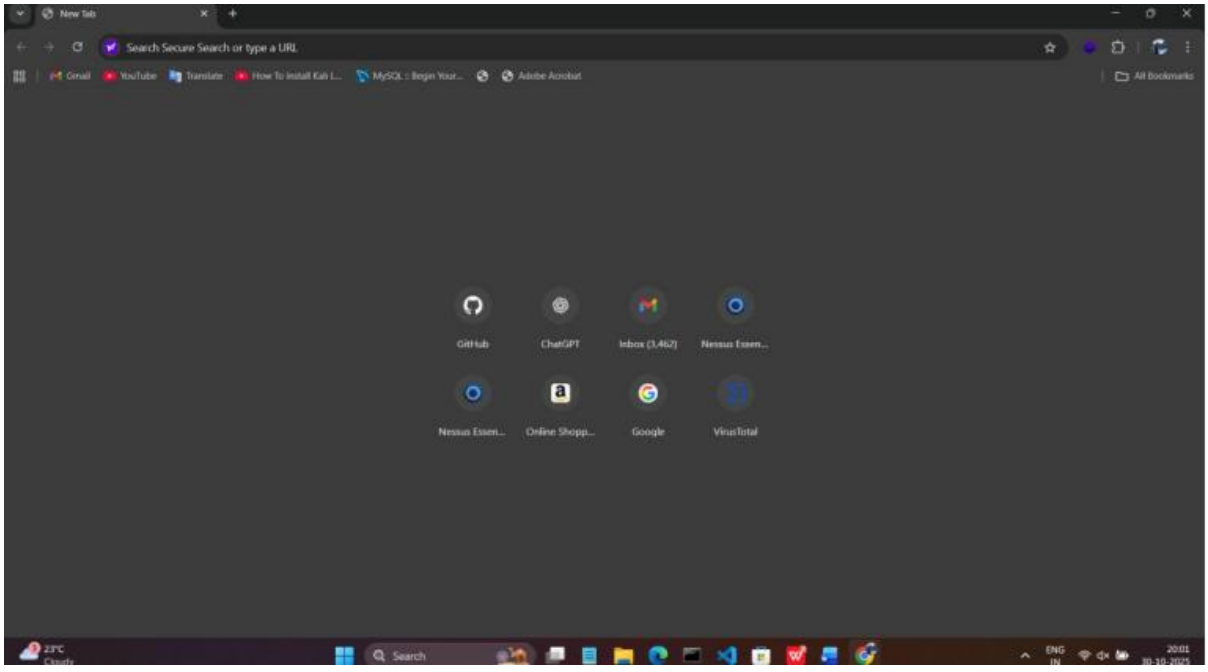
A legitimate developer tool that identifies technologies used on websites. However, it requests high-level permissions such as reading all website data. It should be kept only if required for development work and disabled otherwise.

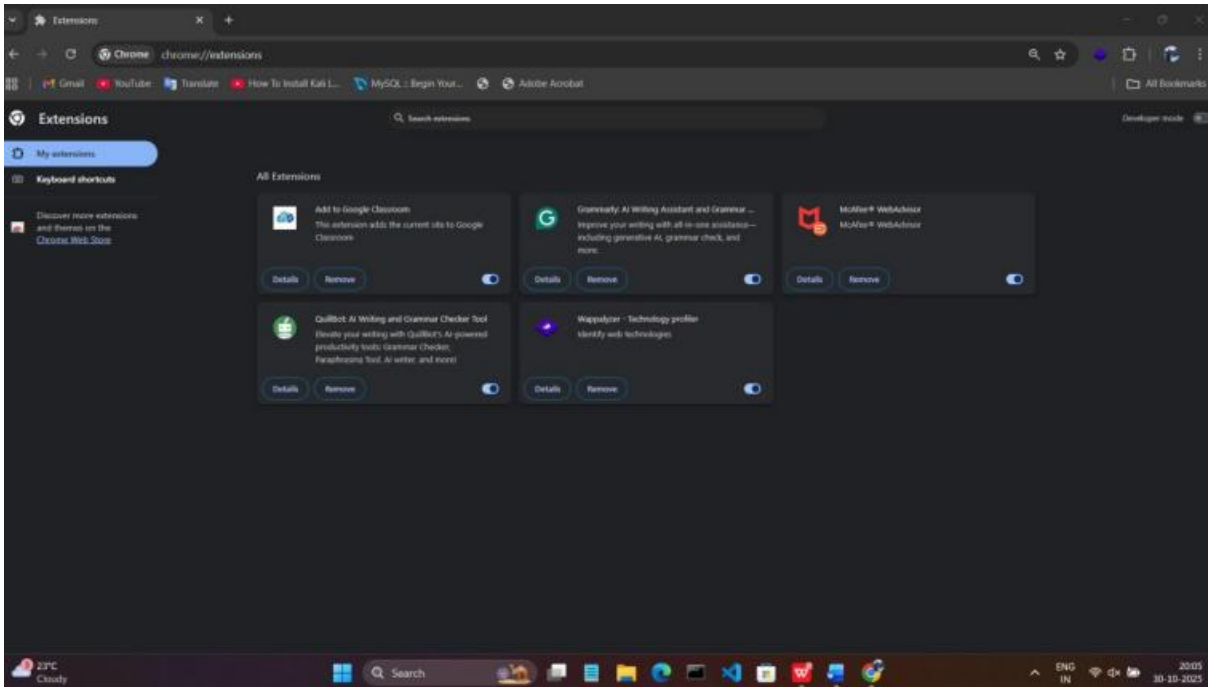
6. Remove suspicious or unnecessary extensions.

- It’s from a third-party and can modify copied data. That’s a privacy risk.

1. Keeping - Wappalyzer

7. Restart browser and check performance.





After removing the suspicious extension - AnyDoc Translator and reviewing the remaining ones, the browser was restarted to observe any changes in performance and stability.

Post-restart, the browser showed noticeable improvement in responsiveness. Web pages loaded faster, and there were no unexpected pop-ups or background activity. The overall browsing experience felt smoother and more secure.

This step confirmed that removing unverified or unnecessary extensions can positively impact browser performance and reduce potential security risks. Regular monitoring of installed extensions helps maintain both speed and safety.

8. Research how malicious extensions can harm users.

• During research, it was found that malicious browser extensions can pose serious security and privacy threats to users. These extensions often disguise themselves as useful tools but secretly collect sensitive data or interfere with normal browsing activity.

• Some of the key ways in which malicious extensions can harm users include:

1. Data Theft:

They can access browsing history, saved passwords, cookies, and even clipboard data,

leading to unauthorized access or identity theft.

2. Tracking and Privacy Invasion:

Malicious extensions can continuously monitor a user's online activities and sell the collected data to advertisers or third parties without consent.

3. Ad Injections and Redirects:

They may insert unwanted advertisements, pop-ups, or redirect users to phishing or infected websites to generate revenue or install more malware.

4. Browser Hijacking:

Some extensions modify browser settings like the homepage, default search engine, or new tab page, forcing users into unwanted sites.

5. System Slowdown:

Running in the background, they consume unnecessary resources and cause noticeable lag, making the browser unstable.

• This research highlights the importance of installing extensions only from trusted sources, reviewing permissions carefully, and regularly auditing all browser add-ons to maintain a secure browsing environment.

Conclusion:

After completing the review and removal process, it was observed that not all extensions are equally trustworthy, even if they seem useful. Among the installed extensions,

The remaining extensions — Add to Google Classroom, Grammarly, Quill Bot, McAfee Web Advisor, and Wappalyzer — were found to be legitimate, with most originating from the official Chrome Web Store. However, McAfee Web Advisor and Wappalyzer were categorized as medium risk because of their high-level permissions and third-party installation.

After removing the unverified extension and restarting the browser, overall performance improved slightly, with faster loading times and smoother tab management. This confirms that removing unnecessary or malicious extensions can enhance both browser performance and user security.

The task provided practical experience in analysing permissions, understanding risks associated with browser extensions, and maintaining a secure browser environment.