Task7 Report

Overall Status: **Complete**

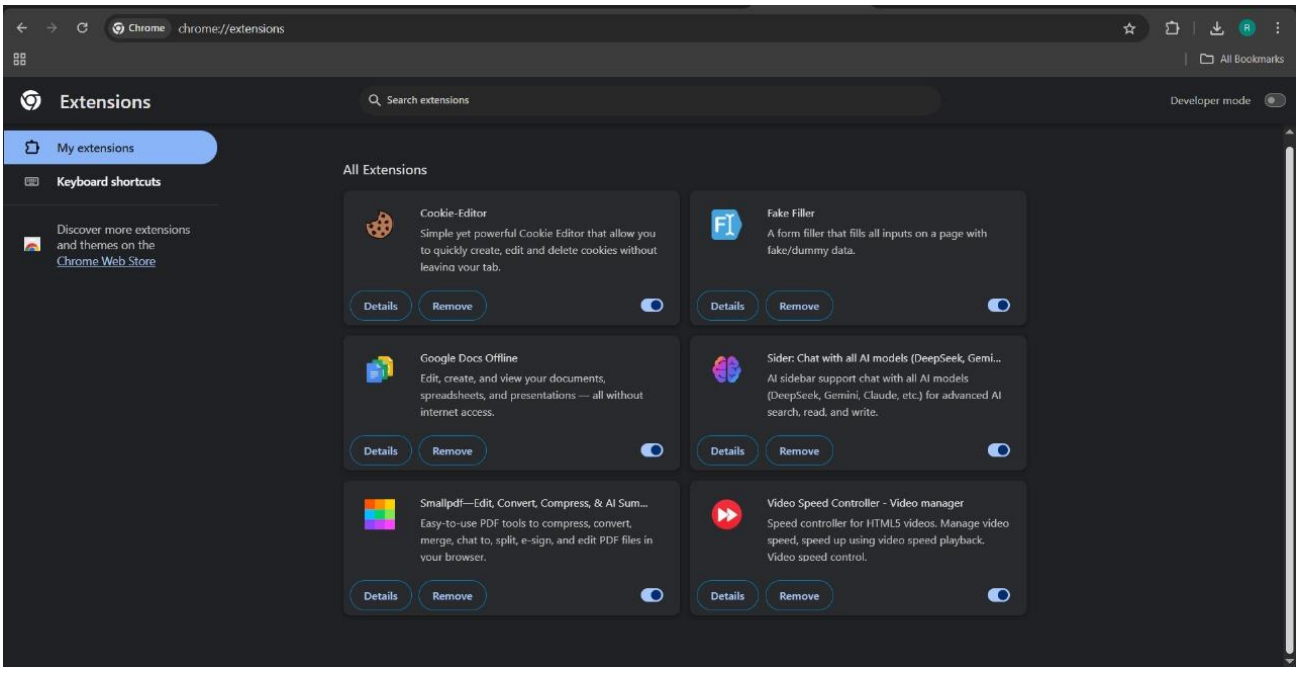
Project Name: Identify and Remove Suspicious Browser Extensions

Date: 05/06/25

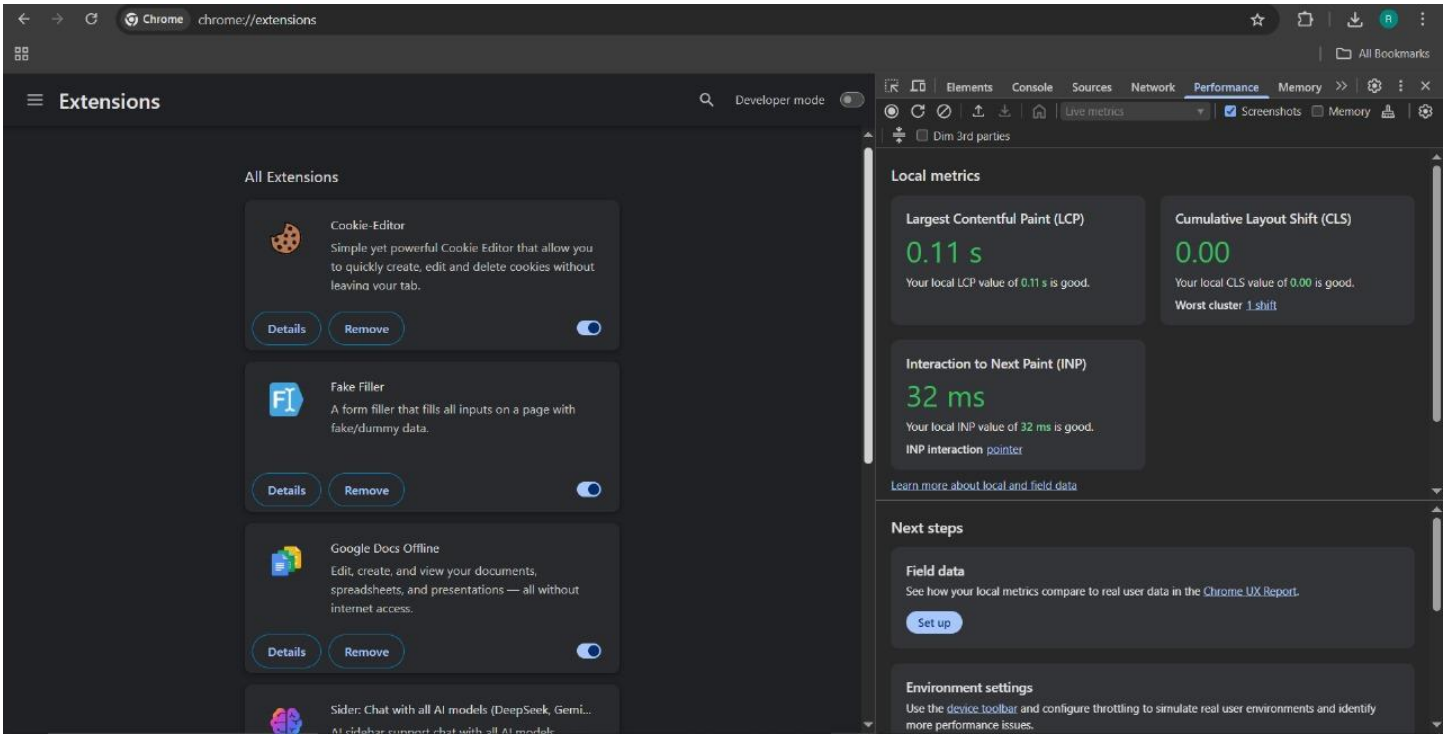
- **Objective: Learn to spot and remove potentially harmful browser extensions.**
- **Tools:Any web browser (Chrome, Firefox)**
- **Deliverables: List of suspicious extensions found and removed (if any)**

Steps:

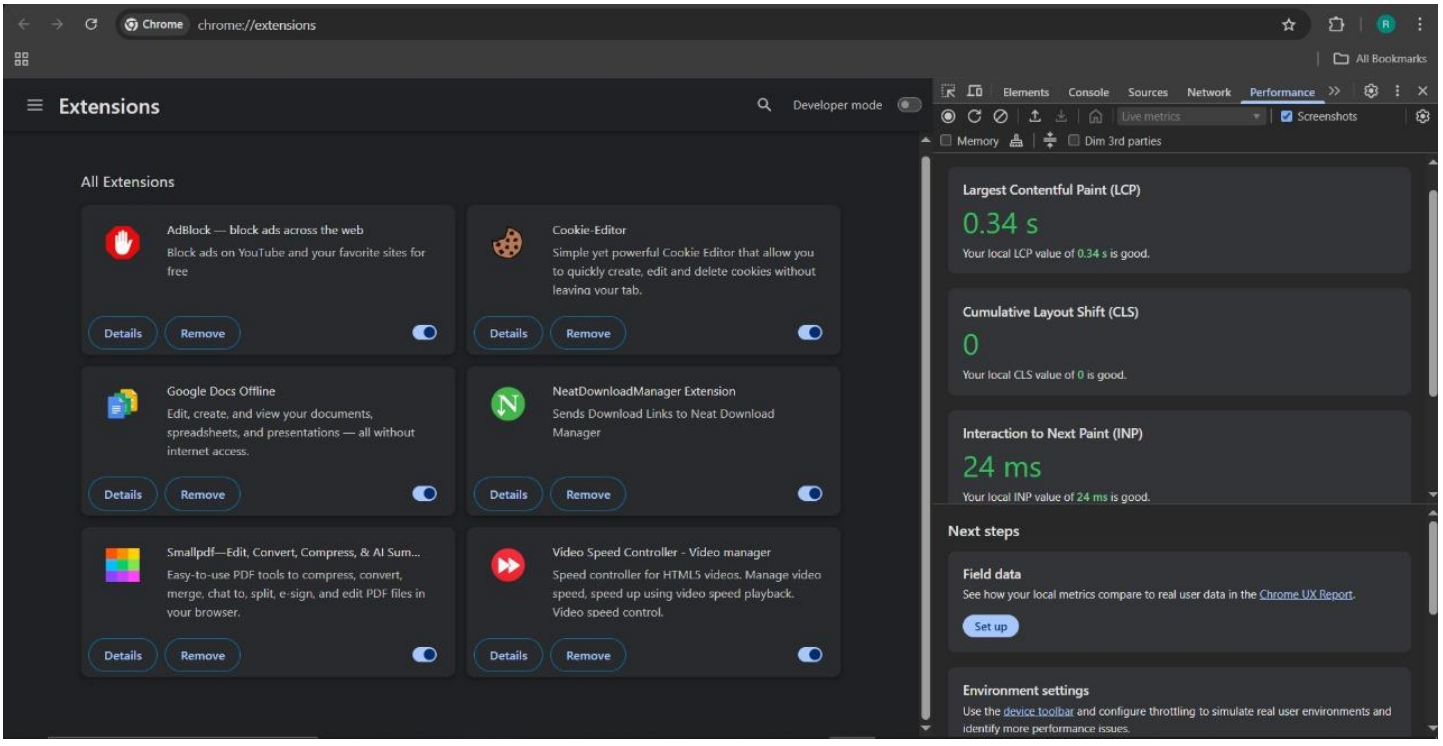
Currently I am using Google Chrome browser , so to navigate to extensions you need to open extensions manager which can be done by :
Menu (⋮) > Extensions > Manage Extensions Or go to ***chrome://extensions/***
This is the list of extensions I currently use in my browser.



The current performance of Chrome with all existing extensions is as follows:



After removing the extensions:



Malicious browser extensions can pose **serious risks** to users' privacy, data, and system performance. Here's how they can harm users:

🔐 1. Data Theft

- **Credential Harvesting:** Steal usernames, passwords, and credit card numbers by logging keystrokes or reading input fields.
- **Cookie Theft:** Access browser cookies to hijack sessions or steal login tokens.
- **Autofill Exploitation:** Extract saved data from autofill (e.g., names, addresses, payment info).

🌐 2. Browser Hijacking

- **Redirects to Phishing Sites:** Change your homepage, search engine, or redirect links to malicious/phishing domains.
- **Injecting Fake Updates:** Trick users into downloading malware disguised as browser updates or plugins.
- **Manipulating Search Results:** Modify results to show sponsored or dangerous links.

📈 3. Ad Injection & Click Fraud

- **Unwanted Ads/Pop-ups:** Display ads on websites where they shouldn't exist.
- **Invisible Clicks:** Simulate clicks on ads in the background to earn fraudulent revenue.
- **Affiliate Hijacking:** Replace legitimate affiliate links with their own to steal commissions.

⚙️ 4. Abusing Permissions

- **Excessive Access:** Many malicious extensions ask for permissions like:
  - "Read and change all your data on the websites you visit"
  - "Manage your downloads"
  - "Capture content of your screen"
- **Silent Surveillance:** Monitor your browsing habits and behavior without your knowledge.

🐢 5. Performance Degradation

- **High CPU & RAM Usage:** Run hidden scripts (e.g., cryptominers) in the background.
- **Browser Crashes:** Poorly written or malicious code can make your browser unstable.
- **Bandwidth Drain:** Background communication with external servers slows down browsing.

🚨 6. Propagation of Malware

- **Dropper Behavior:** Install additional malware or extensions.
- **Command & Control (C2):** Communicate with malicious servers to receive updated instructions.
- **Spying:** Use webcams, microphones, or screen capture APIs in stealth.

✅ How to Stay Safe

- Only install extensions from **trusted sources** (e.g., Chrome Web Store, Mozilla Add-ons).
- **Check permissions** before installing. If they seem excessive, avoid it.
- **Review regularly** and remove unused or unknown extensions.
- Use **security software** that can monitor browser add-ons.
- Keep your **browser updated** to avoid known extension exploits.