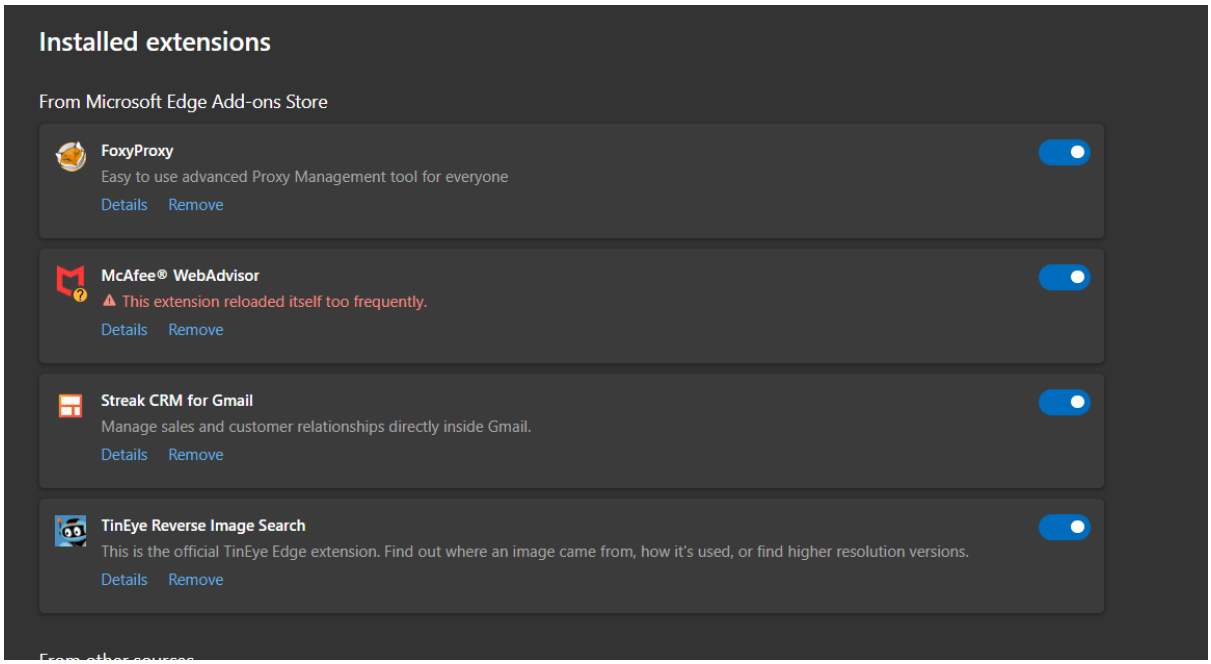
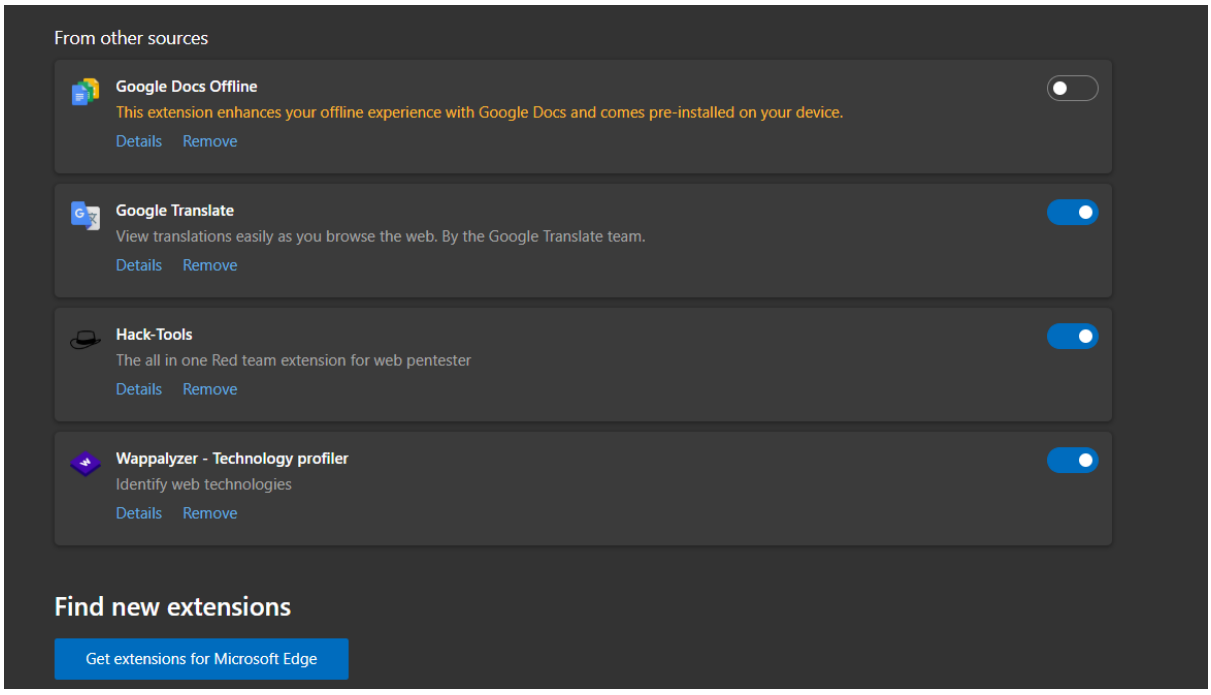
Task 7

Installed Extensions:-



From Other Sources:-



How Malicious Browser Extensions Can Harm Users:-

Malicious or compromised browser extensions can pose serious security and privacy threats because they often have extensive permissions within the browser. Common ways they can harm users include:

1. **Data Theft**
    - Can read and capture sensitive data from websites, including login credentials, banking information, and personal details.
2. **Browsing Hijacking**
    - Changes default search engine, homepage, and new tab settings to redirect users to malicious or ad-filled websites.
3. **Privacy Invasion & Tracking**
    - Monitors every website visited and creates detailed browsing profiles, which can be sold to advertisers or threat actors.
4. **Malware Delivery**
    - Downloads and runs malicious scripts or files, potentially infecting the system with viruses or ransomware.
5. **Security Setting Manipulation**
    - Alters browser security configurations, allowing harmful scripts to run and bypass security warnings.
6. **Cryptojacking**
    - Uses the user's CPU/GPU to mine cryptocurrency without consent, causing slow performance and high power usage.
7. **Phishing Assistance**
    - Injects fake login forms or modifies site content to trick users into entering credentials on phishing pages.

Steps Taken

1. Opened the Extension Manager in Microsoft Edge by typing edge://extensions/ in the address bar.
2. Reviewed all installed extensions from both the Microsoft Edge Add-ons Store and “From Other Sources.”
3. Checked details and permissions for each extension:
    - Verified developer/publisher authenticity.
    - Checked permission scope (site access, data access).
    - Reviewed any warnings (e.g., McAfee WebAdvisor reload issue).
4. Flagged suspicious or unnecessary extensions:
    - Not in active use.
    - Showing unusual behavior (frequent reloads, high permissions without need).
5. Removed flagged extensions to reduce security risks:
    - Clicked **Remove** and confirmed removal.
    - Avoided disabling only — performed full removal for suspicious items.
6. Restarted the browser to apply changes and check performance improvements.
7. Verified that no unusual redirects, pop-ups, or performance issues persisted.

Extensions Removed

Extension Name	**Reason for Removal**
Streak CRM for Gmail	Not actively used; unnecessary permissions for current needs.
TinEye Reverse Image Search	Rarely used; removed to minimize extension footprint and potential risks.