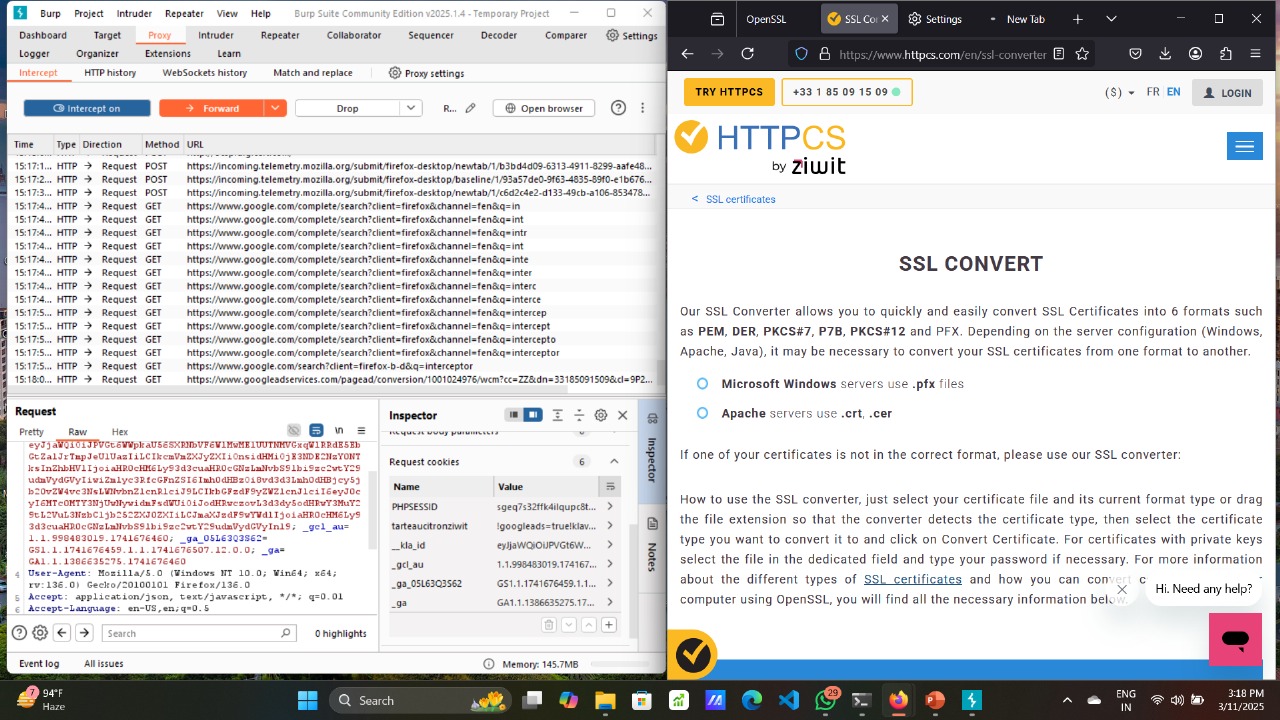
**HTTP Traffic Interceptor Project for Android devices**

This project captures, inspects, and modifies HTTP traffic using three different programming languages: **Python, Node.js, and Go**. Each implementation serves a different purpose but follows the same fundamental principles of HTTP interception.

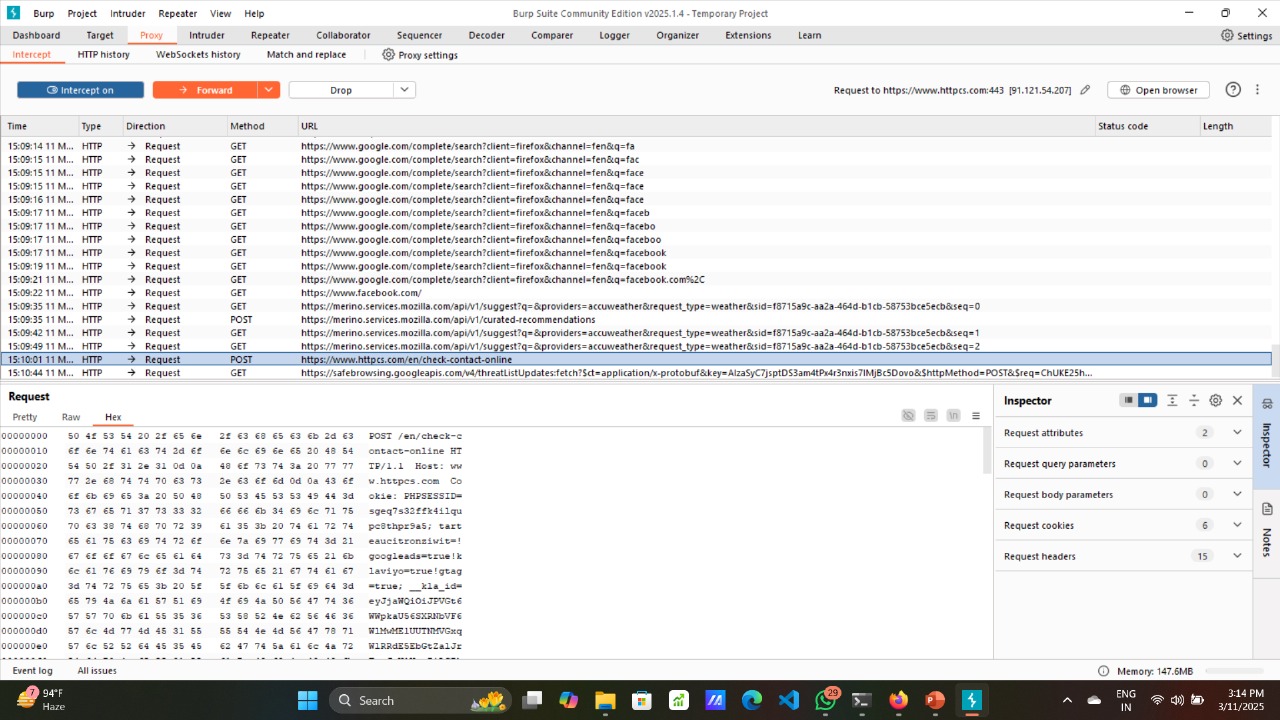
An HTTP Traffic Interceptor works by intercepting HTTP communication between a client (browser, API, or device) and a server. It allows **monitoring, logging, modifying, or blocking** network requests and responses. This is useful for:  
✅ **Security Testing** – Detecting vulnerabilities in network communication  
✅ **Debugging & Development** – Observing how requests and responses flow  
✅ **Traffic Analysis** – Logging and analyzing network activity

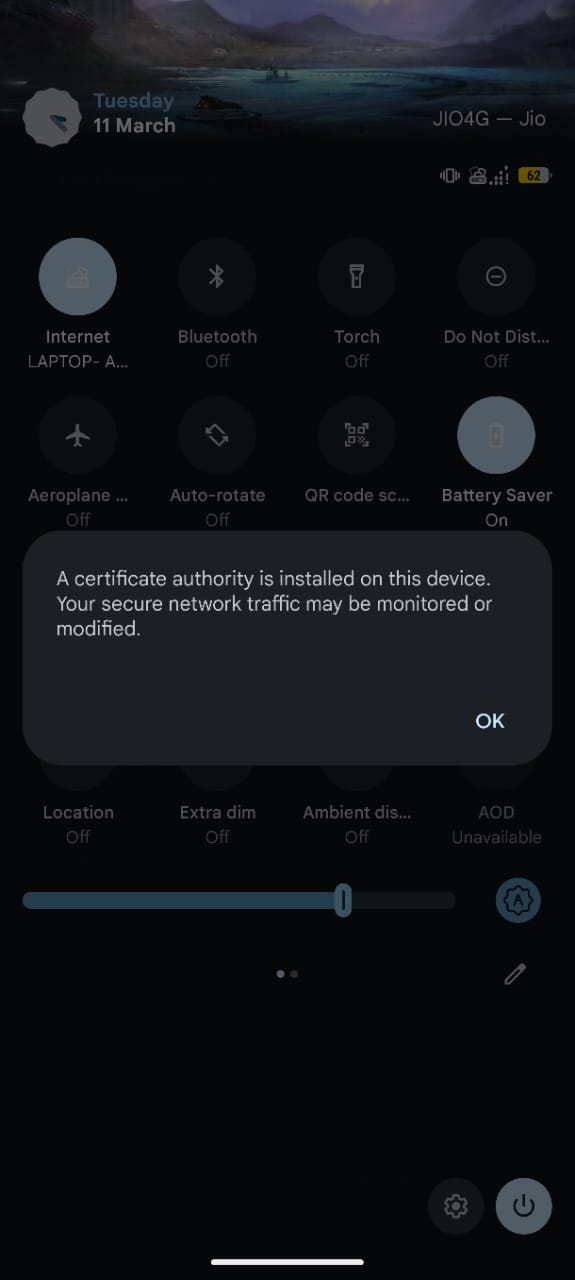
**Key Concepts:**

1. **Packet Sniffing** – Capturing raw network packets to analyze HTTP traffic (Python implementation).
2. **Proxy Interception** – Acting as an intermediary between client and server to inspect/modify requests (Node.js implementation).
3. **Reverse Proxy** – Redirecting traffic through an intermediate server to capture and log data (Go implementation).



Basically we have used a software called BURP SUITE for the configuration and to establish the connection between the PC and android device. After setting up the connection user can see the data packets being exchanged between the user and the server that he/she is trying to fetch on the BURP SUITE dashboard.





After configuring the proxy and port we would have to install the certificate provided in the BURP SUITE software in your android device and work accordingly.