POC - HOMOGRAPHY DETECTOR TOOL

NAME :- MISHTHI NILESH CHAVAN

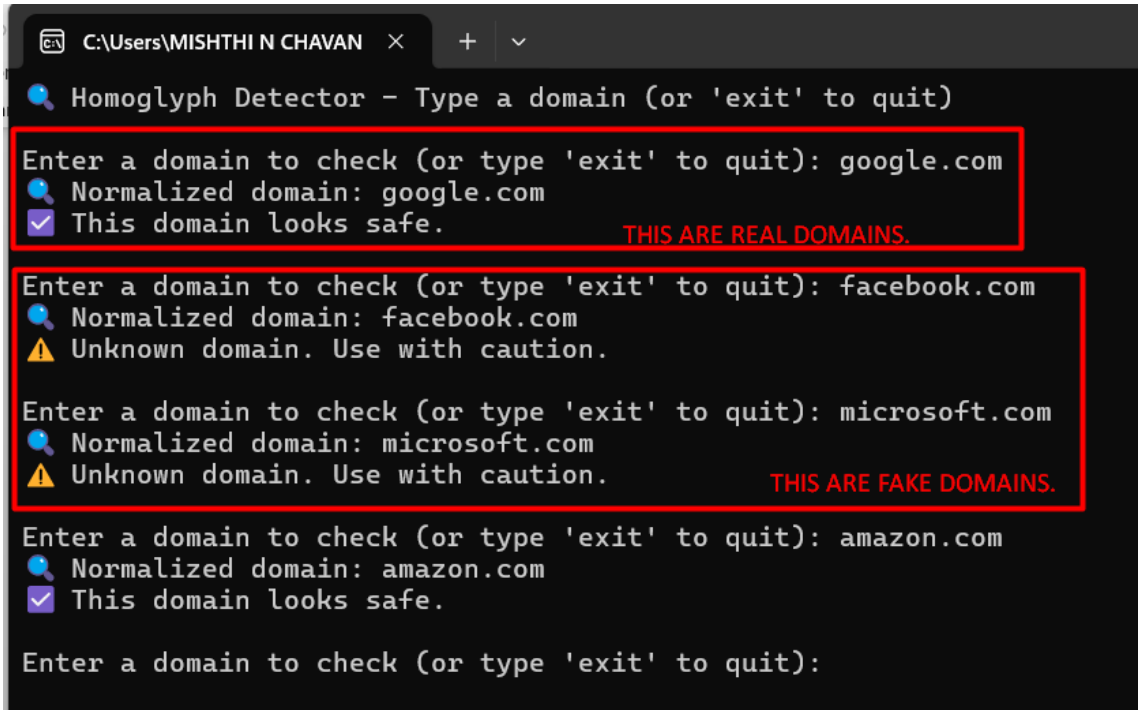
INTERN ID :- 368

- OBJECTIVE :-
  The goal of this project is to create a tool that can detect fake domain names that look like real ones but are actually made using tricky Unicode characters. This helps protect users from phishing attacks by warning them when a domain might be trying to pretend to be a trusted website like google.com or amazon.com.

- TOOL DESCRIPTION :-
  This tool checks if a website name (domain) is trying to look like a real one by using fake look-alike letters from other languages (called homoglyphs). It compares the typed domain with real ones like google.com or amazon.com, and warns the user if the domain is suspicious.

- FILE USED :- homography_detector.py

- SCREENSHOTS :- Running the tool , Entering a fake domain , Output showing warning for suspicious domain, View of test_domains.txt



- REAL VS FAKE DOMAIN EXAMPLES :-

  ➔ Real domains are official and trusted website names like `google.com` or `amazon.com`. The tool checks and says "This domain looks safe."

  ➔ Fake domains try to look like real ones but may be slightly different or suspicious. The tool warns "Unknown domain. Use with caution."

- CONCLUSION :-

  This tool helps us spot fake website names that look like real ones but are slightly different. These fake names can be used in scams or phishing attacks. By checking domains before clicking, we can stay safe online and avoid getting tricked by lookalike websites.