CERIAS

The Center for Education and Research in Information Assurance and Security

iGEM: A Multi-Device Forensic Visualization Software for Geolocation and Digital Evidence Matching

Akif Ozer, Xiao Hu, Umit Karabiyik, Marcus K. Rogers

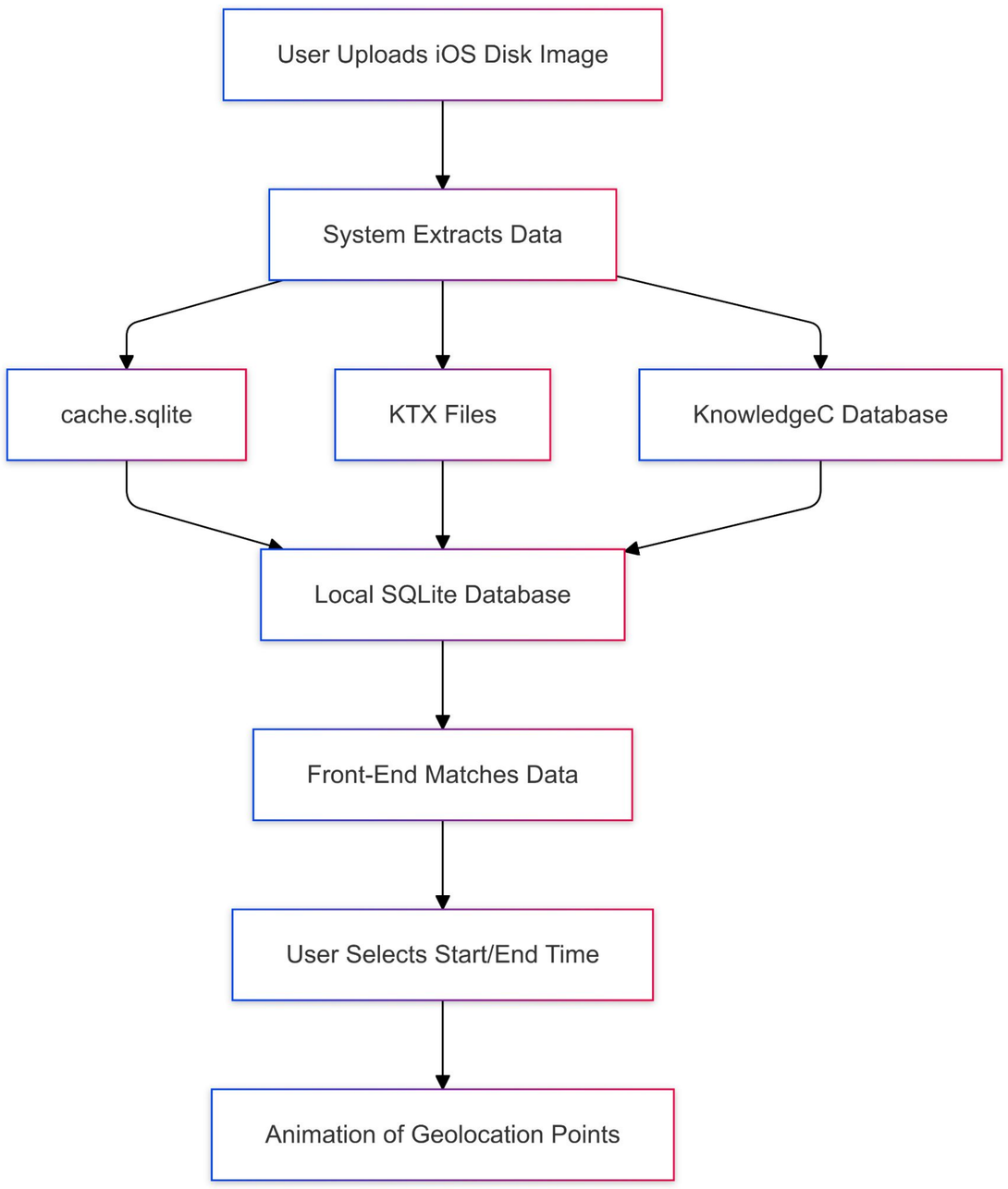
OVERVIEW

This research project was funded by Bureau of Justice Assistance (Award # 15PBJA-21-GK-03996-INTE)

Our project presents a forensic tool that combines data from iOS devices by linking geolocation, application logs, and visual artifacts. This unified approach uncovers hidden temporospatial patterns and improves both investigative research and court presentations.

METHODOLOGY

Our methodology uses modern software frameworks to extract forensic data from iOS devices. We analyze disk images to locate key artifacts—such as Cache.Sqlite for GPS data, KnowledgeC.db for app usage logs, and KTX files for visual evidence—which are then combined into a single SQLite database. An interactive interface with timeline controls and map-based views allows us to link spatial, temporal, and usage data. This approach supports thorough research and improves court presentations by offering fresh insights into temporospatial relationships.

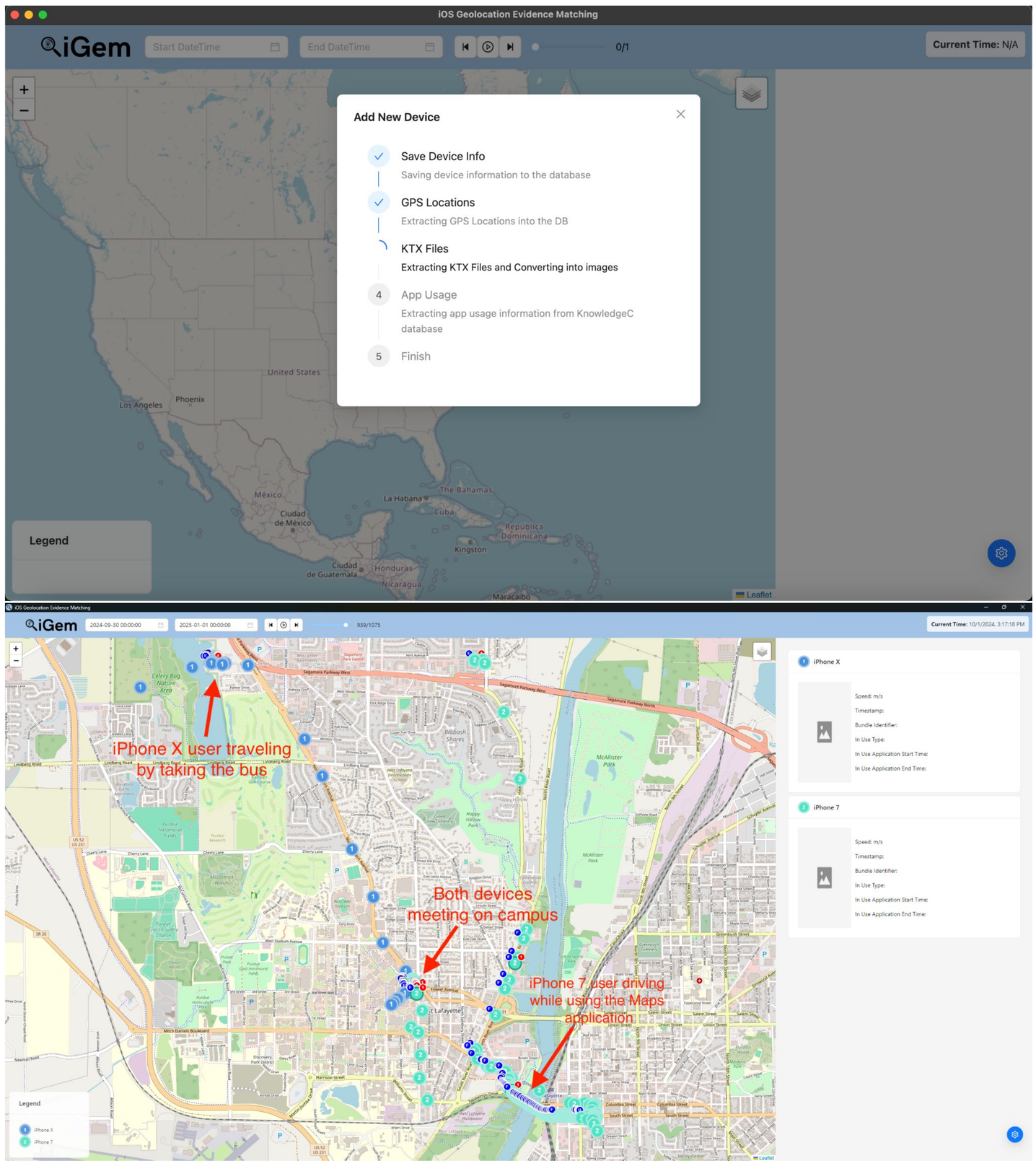


GOALS

The main goals of our project included:

- Streamlining the extraction, linking, and display of key forensic data, such as location details, timestamps, and app usage logs, to enhance court presentations and support novel visualization of temporospatial data.
- Developing an integrated tool that merges diverse data sources into a single interactive interface, enabling investigators to correlate artifacts without inherent location data with those that include accurate spatial and temporal details.

FINDINGS



PURDUE UNIVERSITY

{ozer, hu961, umit, rogersmk}@purdue.edu

CERIAS