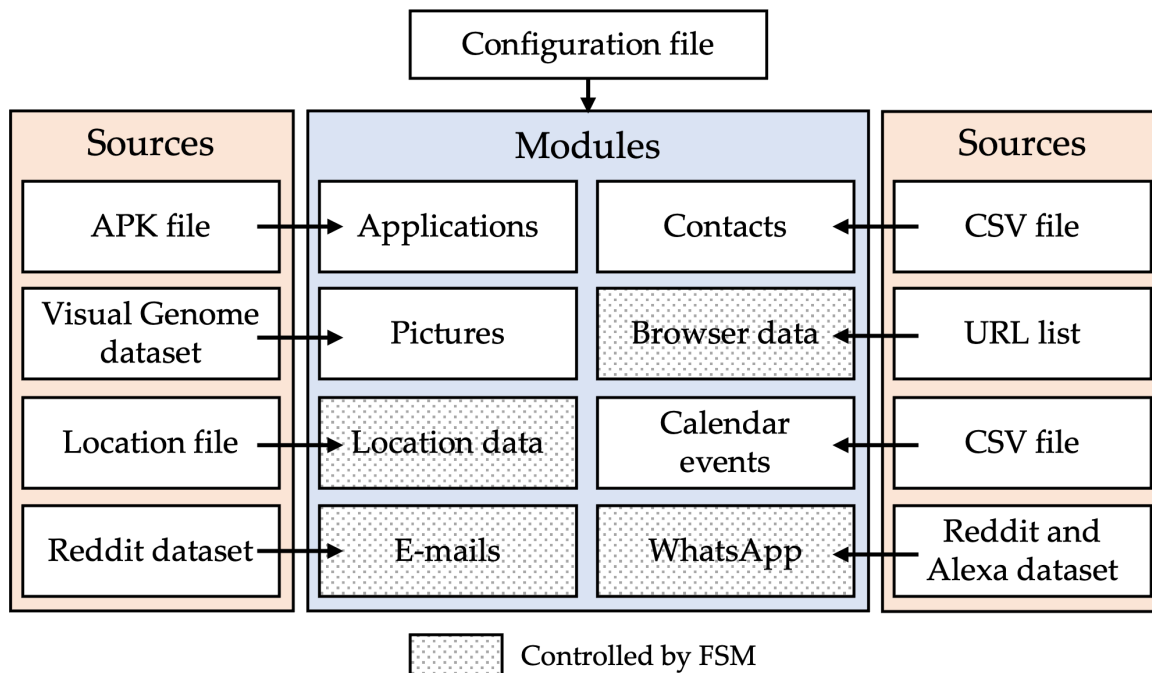


Short Documentation of framework from: “Automated data population using case-like scenarios for training and validation in mobile forensics”



Apps:

- You need 2 folders with APK files for:
 - o Standard apps: all smartphones receive these apps
 - o Individual apps: devices get random apps from this folder
- Connection via ADB → Smartphones must be connected to the PC
- APK files are pushed and installed automatically on the devices

Contacts:

- A CSV file with information about names, phone numbers and optional data (birthday, place of residence, ...) of their contacts is required for each person
- Connection via ADB → Smartphones must be connected to the PC
- A vCard is generated from the CSV file and loaded onto the smartphones

Token Setup:

- First, Google and WhatsApp accounts have to be created for everyone
- No connection to the smartphones required
- Script calls up the confirmation pages for Google Calendar, Gmail and WhatsApp for each person, one after the other. The respective person has to log in into Google and the QR code has to be scanned with the respective smartphone on WhatsApp. Tokens are saved automatically.

Reddit:

- A suitable subreddit must be selected
- No connection to the smartphones required
- Script starts to download the subreddit and prepares (filters + anonymizes) it automatically

Browser:

- A text file with web pages must be created for each person
- Connection via ADB → Smartphones must be connected to the PC
- In the Google Chrome browser, a certain number of random entries is called up from the text file

Photos:

- The number of photos, the period of the recordings and the naming style must be defined in the config file
- Connection via ADB → Smartphones must be connected to the PC
- Time stamps are chosen randomly, adapted to the naming style of the respective device and the photos are loaded onto the smartphones

GPS Spoofing:

- Places and times must be defined in the config file. Currently a total of 4 locations can be defined:
 - o Home
 - o Work
 - o Free time
 - o Weekend
- Connection via ADB → Smartphones must be connected to the PC
- Script automatically changes the GPS position according to the defined times. In order to log the location, Google Maps is called up after each change of location.

Google Calendar:

- A CSV file with information about the title, start and end time and optional dates (description, location, ...) of their calendar entries is required for each person
- No connection to the smartphones required
- Calendar is synchronized via Google API

Gmail:

- Reddit data needs to be downloaded
- No connection to the smartphones required
- Emails are sent through the Gmail API

WhatsApp:

- Reddit data needs to be downloaded
- No connection to the smartphones required
- Messages are sent/read through the WhatsApp Web client

FSM:

- Reddit and Amazon data needs to be downloaded and transition tables need to be created for each person
- Connection via ADB → Smartphones must be connected to the PC
- The FSM currently has 5 branches (WhatsApp, Gmail, GPS Spoofing, Browser, take photo).
-

Each branch contains states that cause certain actions:

- WhatsApp:
 - o idle
 - o read message
 - o start new chat
 - o send message
- Gmail:
 - o idle
 - o read

- write
- Browser:
 - browse
- GPS Spoofing:
 - mock location
- Take photo:
 - take photo

