SPOT FAKE LOCATIONS STORED INSIDE MOBILE PHONES WITH DATA VALIDATION: WHY ONLY USING AN APPLICATION TO TRACK USER MOVEMENTS IS SIMPLY NOT ENOUGH

EDITED BY
NICOLA CHEMELLO

AGENFOR
INTERNATIONAL

Geoposition is useful to **track** a cell phone user's movements, and today every enabled smartphone is capable of saving its exact GPS position with the high accuracy of a few meters.

This useful information is often used in **criminal cases** to prove or disprove alibis. In fact, there are several powerful digital forensics tools that allow data extraction from mobile phones, that are also capable of recovering some deleted contents.

The old school digital forensics examiner, focused on **evidence integrity** by preventing any change to a suspect's phone, tries to extract all it can, and then locks that information with what are called HASH functions to securely save it for the courtroom.

Another tool available to investigators nowadays is **Cloud Acquisition**, where content can be directly downloaded from third party services, for example Google timeline (formerly Google location history). Many software solutions such as Securcube Downloader are developed to achieve this goal.

Several apps, either gaming or related to social networks, and also ones developed by governments help the **tracking** of COVID-19 infected users, by using this GPS positioning to communicate with centralised servers and show where these subjects are moving in real time in order to prevent infections or to protect sensitive locations.

But there is an **issue**: new iOS and ANDROID applications like iMyFone AnyTo or Fake GPS Location are only two of many that allows users to "change location to anywhere, plan a route on the map to move along with customised speed, and work with location-based apps such as AR games, social platforms, etc." (IMyFone, undated).

These apps can **modify** the real information that is going to be saved in the smartphone of a suspect or an infected person and consequently allow the device to store fabricated **false positions**

[1] This article was previously published in the Newsletter of the High Technology Crime Investigation Association, Volume 2, Edition 1.

on remote locations (i.e. Google timeline). When a digital forensic extraction is performed, this will create a **fake alibi** for the user that would be therefore placed in a wrong position. In the same way, when an individual’s phone is feeding centralised servers its location, this data will be in fact useless since it is not the real one at all.

We need to see the real data and spot the fake one. We have an opportunity to do so: **Data Validation**.

This means **cross-checking** and correlating information extracted from **geoposition apps** with real third party ones such as Call Detail Records - CDRs - that are generated by cell phone providers to log the activities of all their customers for billing purposes. It is in fact **almost impossible** for a suspect to access, alter or spoof this type of data.

Data validation means using **multiple sources**, not just the easiest or fastest one, in order to not only find a single source of evidence but discover and connect multiple ones that confirm and validate each other, thus placing investigators in a position of certainty when connecting the dots of an examination.

The goal is to achieve **close cooperation** with all the information collected by the team of investigators working on the same case: as an example, a data validation process could be connecting cell tower data to the CCTV camera feeds retrieved from a gasoline station, or highway traffic logs and credit card ATM statements.

Taking into consideration the **need** for swift and precise systems to track the movements of persons infected with COVID-19 symptoms in order to limit the spread of the virus the most precise and detailed investigations must be performed.

Data validation and a **360-degree approach** to the issue as opposed to the simplest one is how preventive and control systems have to be designed and implemented.

AGENFOR
INTERNATIONAL

FOR MORE INFORMATION ON THIS TOPIC AND ON OUR PROJECTS PLEASE VISIT:

AGENFORMEDIA.COM