Evaluation of GPS EXIF Data Reporting for Digital Forensics Tools

Mohammad M. Mirza, Dr. Umit Karabiyik {mmmirza, ukarabiy}@purdue.edu
Department of Computer and Information Technology

Abstract

Recently there has been an increase in the number of smartphone devices that can capture additional data (e.g., GPS tags) when a photo is taken. In many cases, responders and digital forensic investigators consider photos as an important source of information, especially if they are dealing with mobile investigations as photos might be embedded with corresponding GPS data. Therefore, many of the advanced digital forensics tools, including open source (e.g., Autopsy) and proprietary (e.g., AXIOM) have incorporated extraction techniques for EXIF data from media files. However, these tools only present a limited EXIF data related to Geolocation (i.e., latitude, longitude, and altitude). Although general GPS information would be satisfactory in some cases, there are other EXIF data inducing GPS (image) direction and speed that might aid investigators and can be considered useful in many investigation settings. In this research, we focus on investigating and demonstrating missing GPS EXIF data in forensics tools such as Autopsy and AXIOM, where they lack identification, examination, and presentation of these data. Moreover, this has led us to the development of a simple functional extraction tool that parse and preserve relevant GPS EXIF data for further examination by digital forensic investigators.
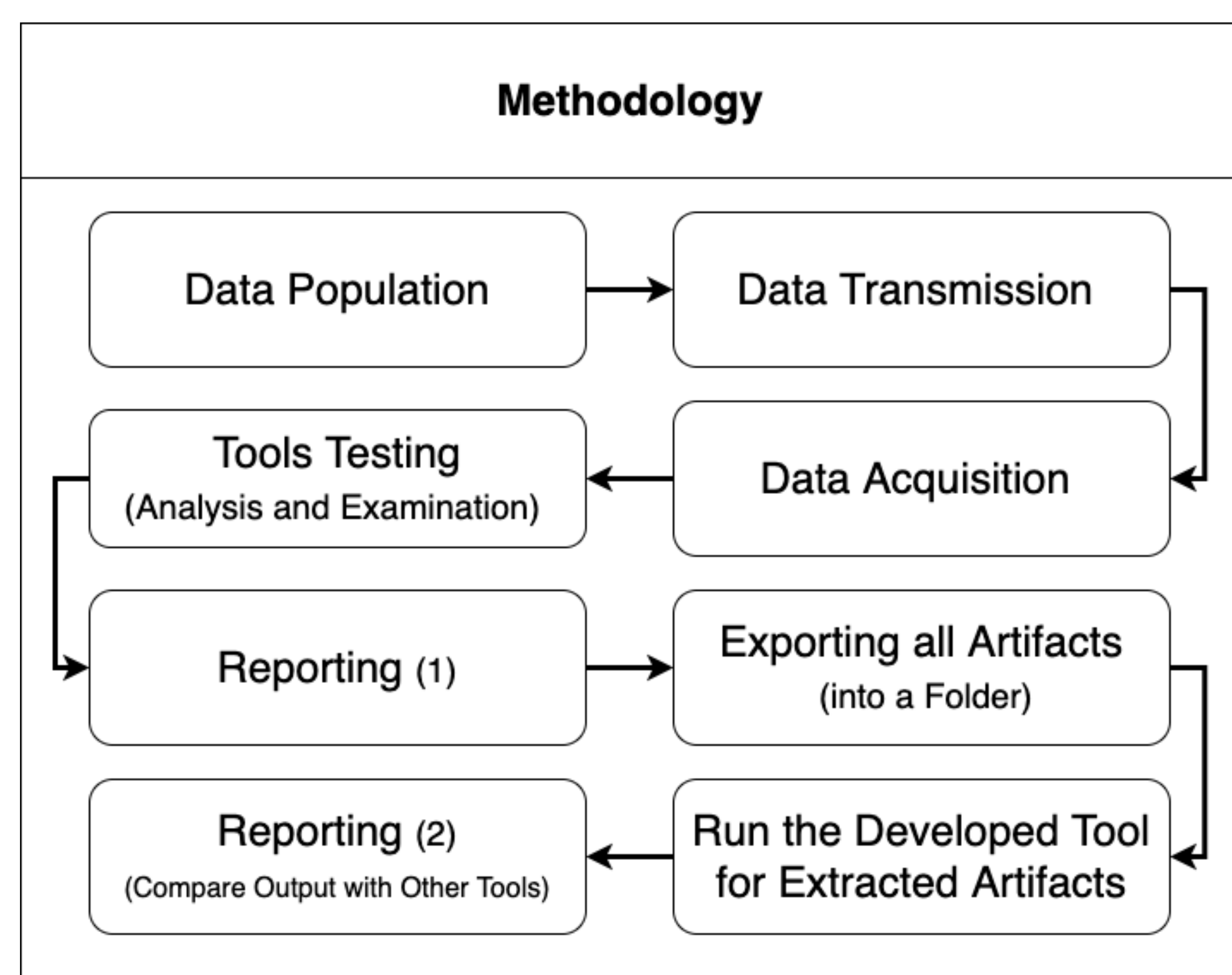
Methodology

Figure 1: Study Flowchart

Reporting (1)

Figure 2: AXIOM Output

Figure 3: Autopsy Output

Reporting (2)

Table 3 below shows the outcome of the developed tool that represent more GPS EXIF data from the given photo.

File Name	Date	Time	Lat	Log	Alt	Image Direction	Movement Speed
IMG_0133.JPG	2020:09:15	12:10:57	40.42413055555560	-86.9105138888890	189.01965923984300	57.60876468720230	0.11458577951728600

Table 3: Tool CSV Output Example

	AXIOM	Autopsy	Proposed Tool
GPS EXIF Data	Limited*	Limited*	More Information

Table 4: Comparison of Presented Information
* Only Latitude, Longitude, and Altitude

Experimental Setup

Device & Model	iPhone (Xs Max)	MacBook Pro	PC
OS version	iOS (v13.7)	macOS Catalina (v10.15.6)	Windows 10 Education (v2004)
Useage	Data population using default camera application (GPS on)	Copy transmitted files from Airdrop to USB	Used it for taking an image of the USB and analysis

Table 1: Devices Used in the Scenario

Tool	Autopsy	AXIOM	Proposed Tool
Version	4.15.0	4.4.0.21161	0.1

Table 2: Tools Used in the Scenario

Importance

Additional information extracted from EXIF tags can aid investigators to draw better conclusions and additional extracted data can help in:
1. Crime scene reconstruction and visualization.
2. Utilizing full positional EXIF data out of photos (if they can be recovered) and leave the choice to the investigator to determine what they need.
3. Enhance digital forensic technology to determine more information regarding the satiation and the surroundings.
4. Enhance investigators' spatial-awareness (e.g., determining the direction of the image inside buildings and determining movement speed when the photo was taken).

Proposed Tool Implementation

Figure 4: The Proposed Tool

Programming Language	Computing Library	Supporting Libraries	Graphical User Interface
Python	ExifRead	CSV and OS	PySimpleGUI

Table 5: Tool Development Environment and Libraries

Future Work

1. Expand the experiment setup on a larger sample size considering several possible scenarios.
2. Consider more EXIF tags tags that are missing from the digital forensics examined tools.