Scientific Working Group on Digital Evidence

SWGDE Best Practices for Portable GPS Device Examinations

Disclaimer:
As a condition to the use of this document and the information contained therein, the SWGDE requests notification by e-mail before or contemporaneous to the introduction of this document, or any portion thereof, as a marked exhibit offered for or moved into evidence in any judicial, administrative, legislative or adjudicatory hearing or other proceeding (including discovery proceedings) in the United States or any Foreign country. Such notification shall include: 1) The formal name of the proceeding, including docket number or similar identifier; 2) the name and location of the body conducting the hearing or proceeding; 3) subsequent to the use of this document in a formal proceeding please notify SWGDE as to its use and outcome; 4) the name, mailing address (if available) and contact information of the party offering or moving the document into evidence. Notifications should be sent to secretary@swgde.org.

It is the reader's responsibility to ensure they have the most current version of this document. It is recommended that previous versions be archived.

Redistribution Policy:
SWGDE grants permission for redistribution and use of all publicly posted documents created by SWGDE, provided that the following conditions are met:

1. Redistribution of documents or parts of documents must retain the SWGDE cover page containing the disclaimer.
2. Neither the name of SWGDE nor the names of contributors may be used to endorse or promote products derived from its documents.
3. Any reference or quote from a SWGDE document must include the version number (or create date) of the document and mention if the document is in a draft status.

Requests for Modification:
SWGDE encourages stakeholder participation in the preparation of documents. Suggestions for modifications are welcome and must be forwarded to the Secretary in writing at secretary@swgde.org. The following information is required as a part of the response:

a) Submitter's name
b) Affiliation (agency/organization)
c) Address
d) Telephone number and email address
e) Document title and version number
f) Change from (note document section number)
g) Change to (provide suggested text where appropriate; comments not including suggested text will not be considered)
h) Basis for change

Intellectual Property:
Unauthorized use of the SWGDE logo or documents without written permission from SWGDE is a violation of our intellectual property rights.

Individuals may not misstate and/or over represent duties and responsibilities of SWGDE work. This includes claiming oneself as a contributing member without actively participating in SWGDE meetings; claiming oneself as an officer of SWGDE without serving as such; claiming sole authorship of a document; use the SWGDE logo on any material and/or curriculum vitae.

Any mention of specific products within SWGDE documents is for informational purposes only; it does not imply a recommendation or endorsement by SWGDE.

SWGDE Best Practices for Portable GPS Device Examinations

Table of Contents

1. Purpose

The purpose of this document is to describe the best practices for portable global positioning system (GPS) device examinations.

2. Scope

This document provides basic information on the logical and physical acquisition of portable GPS devices.

3. Limitations

This document only addresses portable devices with GPS as its primary function. Some examinations are limited by the ability of the software used to extract the data. Manual examination may be needed if software is unsuccessful.

Some limitations encountered are as follows:

- **Cables** – Data Cables are often proprietary and difficult to obtain.
- **Condition of the Evidence** – Commercially available tools may not provide solutions to deal with physically damaged devices.
- **Equipment** – Equipment used during examinations may not be the most recent version due to agency verification requirements of hardware, firmware, and/or software.
- **Memory Cards** – Processing these cards inside the device pose risks (e.g., not obtaining all data including the deleted data, altering date/time stamps, etc.).
- **Passwords** – Some devices may be protected by user-applied passwords.
- **Training** – The individual copying data from a mobile device should be trained to ensure the integrity of the data.
- **Unallocated Data / Deleted Data** – Many forensic tools may only acquire a logical copy of the data. Deleted data may only be recoverable from a physical acquisition[1].

[1] Physical acquisition implies a bit-by-bit copy of an entire physical store (e.g., a memory chip)

4. Evidence Collection

4.1 Seizing Evidence

Immediately upon seizure of a GPS device, document the on screen data, power down the device and document the on-scene weather conditions. If available, document the GPS position with a secondary device. Disconnect all cables and antennas. Collect all power, data cables and memory cards directly connected to the device. If possible, acquire PIN or pass code information from user.

4.1.1 Handling Evidence

- Evidence should be handled according to agency policy while maintaining a chain of custody.
- Network isolation of the GPS device should be maintained by keeping the device turned off until processing in the laboratory setting. This isolation should include GPS, Wi-Fi, cellular, and Bluetooth networks.
- Additional forensic analysis – Occasionally, there may be a need to conduct traditional forensic processes on a GPS device (DNA, latent prints, etc.). These are case dependent and should be discussed with the investigator about the need for such evidence as well as the order in which they should be performed. Contact appropriate crime lab personnel for guidance on processing order to avoid the destruction of forensic evidence.
- Biological contaminants and physical destruction provide unique challenges to the recovery of data. Universal precautions should be utilized to protect the health and safety of the examiner.

4.2 Equipment Preparation

"Equipment" in this section refers to the non-evidentiary hardware and software the examiner utilizes to conduct data extraction and analysis of the evidence.

- Equipment and software applications should be verified[2] to ensure proper performance.
- Current information (e.g. user's manual) describing the manufacturer's software/hardware and other relevant documentation should be recently reviewed and accessible.
- Data Cables are often proprietary and difficult to obtain. Some cables are specific to a single device while others support multiple models.

[2] The validation process is discussed in the document titled "*SWGDE Recommended Guidelines for Validation Testing*."

4.3 Data Acquisition

Prior to data acquisition, the examiner should conduct a thorough review of the device's features/functions related to the storage of user data as outlined in user manual and remove any connected antennas. Obtain appropriate power/data cables and memory cards.

During data acquisition, isolate the GPS device from Wi-Fi, GPS, cellular and Bluetooth networks.

GPS devices and their media cards should be protected with some form of hardware or software write-protection.

A GPS device and any associated media cards should be forensically imaged using an acquisition tool.

4.4 Data Analysis

Analysis of data can be conducted using various tools. Data of importance may include:

> Device configuration settings (Bluetooth pairing), maps, tracks/archived tracks, waypoints, routes/journey, saved locations, favorites, owner information, "Home" location, recent destinations, city and state history, contacts/addresses, Points of interest (POI), last GPS fix, pictures (including Geotags), text messages, text files, call logs (incoming, outgoing, missed calls).

4.5 Documentation

Documentation should meet the requirements of the examiner's agency and applicable policies.

Evidence handling documentation should include, but not limited to:

- Copy of legal authority
- Chain of custody
- Detailed description and/or photographs of the device (make, model, condition, etc.)
- Photographs or documentation of any visible damage
- Information regarding the packaging and condition of the device

Examination documentation should:

- Contain sufficient detail to allow another examiner, competent in the same area of expertise, to identify what has been done and to access the findings independently
- Include communication notes regarding the case
- Be preserved according to the examiner's agency policy

4.6 Archive

Depending on agency policy, acquisition case files should be archived.

- Maintain archives according to departmental policy and applicable laws.
- GPS device acquisitions may capture data using proprietary formats and archiving the tool version used may be required.

5. Report

Reports should:

- Contain a graphical representation of the data acquired
- Seek to address case specific requests from the investigator
- Provide the reader with all the relevant information in a clear and concise manner
- Be reviewed according to agency policy

6. Reference Sites and Publications

The below listed resources provide information that may prove helpful to the examiner:

- **Garmin** - http://www.garmin.com
- **PC Planner** - pcplanner.c-map.it
- **GPS Utility** - www.gpsu.co.uk
- **Magellan** - http://www.magellangps.com
- **TomTology** - www.forensicnavigation.com
- **Google Earth** - http://www.avmap.it/index.php?swt=12
- **GPS Visualizer** – www.gpsvisualizer.com
- **GPSBabel** - http://www.gpsbabel.com/
- **AVMAP GPX Converter** - http://www.avmap.it/index.php?swt=12
- **EasyGPS** - http://www.easygps.com/
- **Free GPS Software** - http://www.maps-gps-info.com/fgpfw.html
- **GPSForensics.org** – http://www.GPSForensics.org

Scientific Working Group on Digital Evidence

SWGDE Best Practices for Portable GPS Device Examinations

History

Revision	Issue Date	Section	History
1.0	06/04/2012	All	Release for Public Comment
1.1	09/12/2012	All	Incorporated general edits and voted to release as an Approved document
1.1	--	--	Updated document per current SWGDE Policy with: new disclaimer, removed Definitions section, and corrected SWGDE hyperlinks. No changes to content and no version/publication date change. (9/27/2014)