Forensic Science and Criminology

Case Report ISSN: 2513-8677

Forensic analysis of navigation system (GPS) – A case study

PN Ramakrishnan*

Central Forensic Science Laboratory, Directorate of Forensic Science Services, Ministry of Home Affairs, Government of India

Abstract

A navigation device which are presently commonly available providing the basic directions, maps, grocery shops, establishments, traffic movements, roads, vital institutions etc. based on the receipt of the signals received by the device i.e. Global Positioning System (GPS) signals in the formal of latitude and longitude data and same is converted into graphical representation or in the form of readable text mode. Present day smart phones are mostly provided with the GPS. Data retrieval from such GPS devices is a challenging in nature. This particular GPS device was of the make "GARMIN" model GPS-12 and GPS-128, 12-CHANNEL, Olanthe, KS, USA which was seized by the Indian Navy Patrol vehicles from the deep sea. Later, the case was transferred to National Investigation Agency (NIA). The laboratory with the help of GPSUtility Software version 5.11 could retrieve the vital data from the six (6) numbers of GPS devices. The paper envisages the methodology adopted in the data retrieval from an old model GPS navigation device which was illegally used by the fishermen in their fishing trawlers across the Indian Ocean.

Introduction

The fields of electronic evidences are no longer concentrated entirely on the conventional media but have to encounter various types of embedded devices out of which the GPS receiver is one among them. These GPS receiver devices consist of vital information if used by anti-social elements or terrorism etc. These handheld or vehicle mounted GPS devices have their own proprietary operating systems, file system formats and different techniques of communication. The analysis of such suspected GPS devices or receivers requires exclusive software and hard ware tools as well as knowledge of the principal, working mechanism and areas where digital data is stored. In view of the fact that the GPS devices have found to be omnipresent and more rampant in present scenario of commission of crimes. There are many types of GPS navigation in the world today but the most popular ones being TomTom, Garmin, Mio Technology, Navman, and Magellan. These embedded devices can provide valuable evidentiary digital data in the form of track logs, track points, routes stored about its location, call logs, received, and dialed numbers, videos, photos and audios depending upon the type of GPS receivers. All the modern GPS devices/receivers have slots for the external memory cards in addition to the built-in flash memory. All these forensic data retrievals can be used as unassailable evidence in the Court of Law.

It is evident that most of the earlier versions of the GPS receivers/devices use the flash memory technology in data storage. The history of the Global Positioning System and the different type of the GPS receiver/devices are explained elsewhere [1-6]. The GPS receiver uses satellites to pinpoint locations on the earth crust. Twenty four of these satellites are in operation and three extra satellites functions in case of any collapse of one or more of these. The orbits are arranged in such a way that at any time anywhere on Earth, there are at least four satellites visible in the sky. A GPS receiver device function is to locate four or more of these satellites, figure out the distance to each and use this information to deduce or calculate its own locations [7-9].

There are five (5) different types of GPS receivers they are (i) not self contain receiver – without screen or R232 receivers or GPS Mice, (ii) Self contained receivers or a computer is integrated in a GPS receiver, (iii) sophisticated receivers used by ONGC, military services, (iv) dedicated single purpose GPS systems like CAR GPS and (v) GPS incorporated in phones – modern smart phone systems etc. [2,9]. The Tom-Tom and Garmin model devices have the address to address routing feature along with optional mapping software. Voice prompt functions are available in Garmin Street Pilot, Nuvi models, Quest, Magellan, Tom-Tom Road Mate. Some of the devices also have built in road maps, routes, waypoint and Datums. They may also have a track back function which is designed to change the routes in case of a one-way route system [9].

The GPS receiver device as presently dealt with i.e. GARMIN make consists of different types of models available in the marked which can be divided into three main types – (1) Device with Secure Digital (SD) cards, (2) Device with only internal flash memory and (3) GPS devices with internal hard drive. Forensically the image of GPS devices can be acquired as bit stream image except for the device which has only the internal flash memory device. The GPS receivers normally accumulate the information in a file format of ".cfg" file. The analysis of the ".cfg" file indicates that the first destination in the '.cfg' file is the home location if entered, and the last two entries link to the start of the last calculated route and the last entered destination [8].

Materials and methods

Embedded electronic evidence in the GPS devices are of evidentiary value and it is treated in the same manner as traditional forensic

Correspondence to: PN Ramakrishnan, Central Forensic Science Laboratory, Directorate of Forensic Science Services, Ministry of Home Affairs, Government Of India, E-mail: pnrkrishna@rediffmail.com

Keywords: *GPS, Navigation device, tracks, routes, way points, data & retrieval*

Received: January 14, 2018; **Accepted:** February 02, 2018; **Published:** February 06, 2018

evidence with same care and similar cardinal rules of computer forensics. The conventional procedure was followed in the analysis of GPS devices while collecting, preserving, analyzing, and presenting the digital data artifacts. In this paper the author had forensically analyzed the GARMIN-GPS-12 & 128 model device had been examined. This particular model consists of only the internal flash memory and entire digital data is stored in the built in flash memory. The device can be interfaced to a desktop forensic workstation through the Universal Serial Bus (USB) cable through a write protected USB Port.

In the present case study, the author had only attempted the LOGICAL analysis of the GPS device. The PHYSICAL analysis of built-in flash memory requires special hard ware tools for the bit stream acquisition, which is being procured separately and the study is being carried out separately. The GARMIN MAPSOURCE-WAYMANGER version 4.60 and GPS-Utility Software version 5.11 had been used for the LOGICAL extraction of the data from the GARMIN GPS12 & 128 device. The entire data was retrieved through the WRITE PROTECTED USB PORT as it protects one way data transfer and there is no probability of reverse data entry or modification of the vital data present in the GPS devices. The method of acquiring was found in many ways similar to conventional methods of data previewing and data transferring on a sterile media for further analysis (Figures 1-3).

Results and discussion

The data retrieved from the flash memory of the GPS device for this particular model of GARMIN i.e. model 12 and 128 were found in the ".gdb" format. The file extension relates to the 'GEO DATA BASE' which is the common form of storage and management framework for such geo data for the GPS systems. It actually combines the spatial data with the data repository to create a central data repository for spatial data storage and management. It can be control with the server or PC environments so as to allow one's GPS data into GIS data in a central location for easy access and management. This data called geodatabase offers ability to maintain the integrity of spatial data, topologies, network with consistent and accurate data base.

This 'gdb' data can be directly linked through the "GOOGLE EARTH" if there is an internet connection to view all the routes, maps and tracks of the vehicle which used this device to travel or its travelogue details.

All the tracks, way points and routes entered in the GARMIN model 12 and 128 devices can be viewed and stored forensically like any data in a secure way using the GPS Utility or GARMIN WAYPOINT+TRACK MANAGER. With help of these software's it is easy to identify the location with the data of latitude and longitude. It was observed that

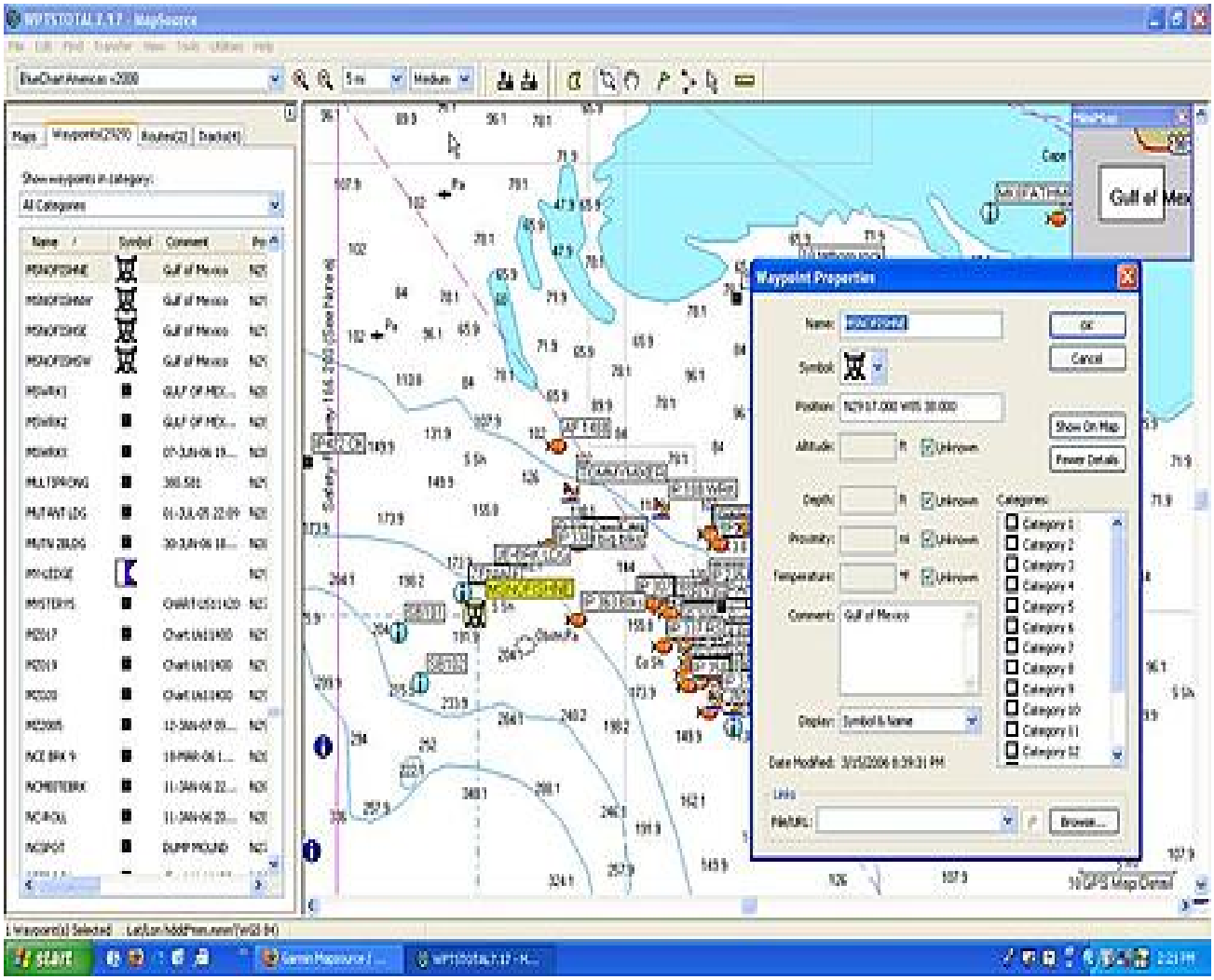


Figure 1. Screen shot of Garmin waypoint manager.

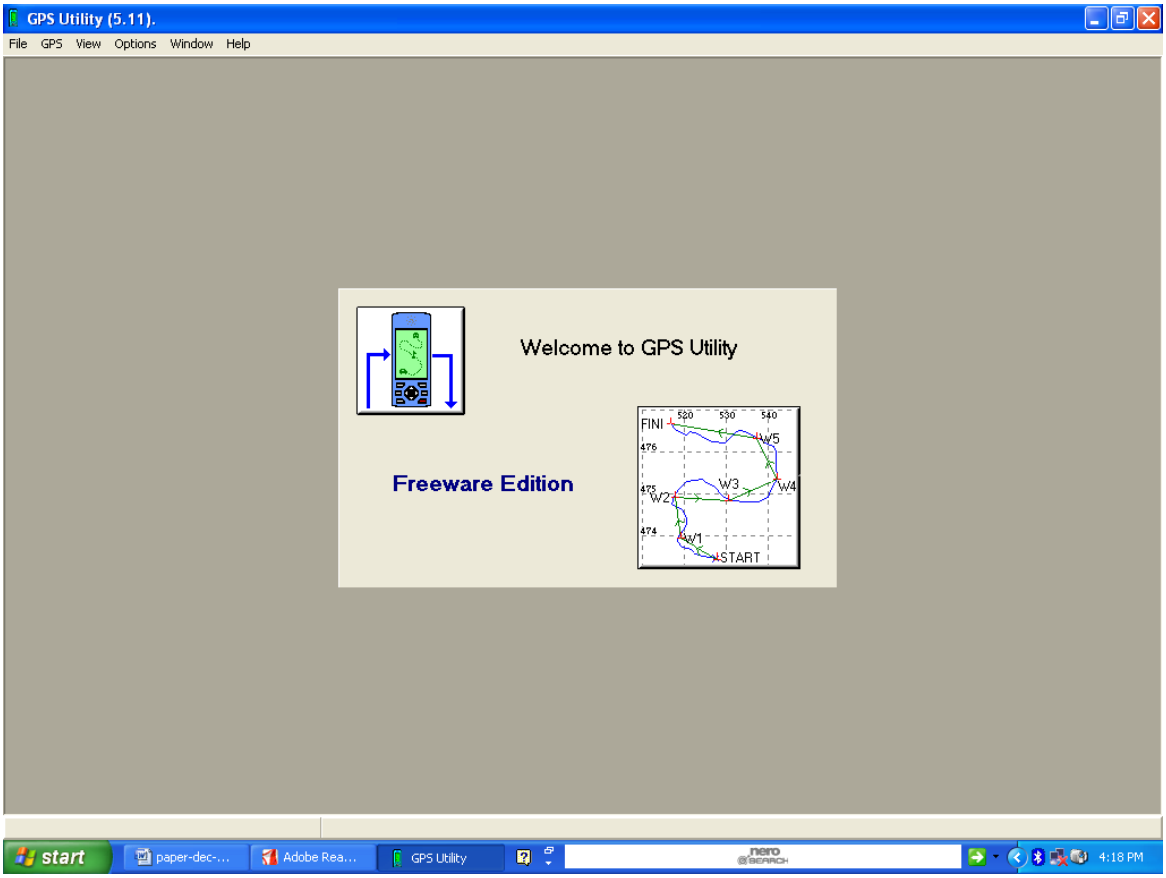


Figure 2. Screen shot of GPSU ver.5.11.

Figure 3. GPS receiver/device- Garmin -12.

the latitude and longitude are in datum map system. These latitude and longitude will give us a precision of location as found on the map and moreover it can also be used to calculate the distance between two addresses or location when subjected under investigation. The track details, the way point details and the route details as viewed through the software are given in the Figures 4-6 as screen shots.

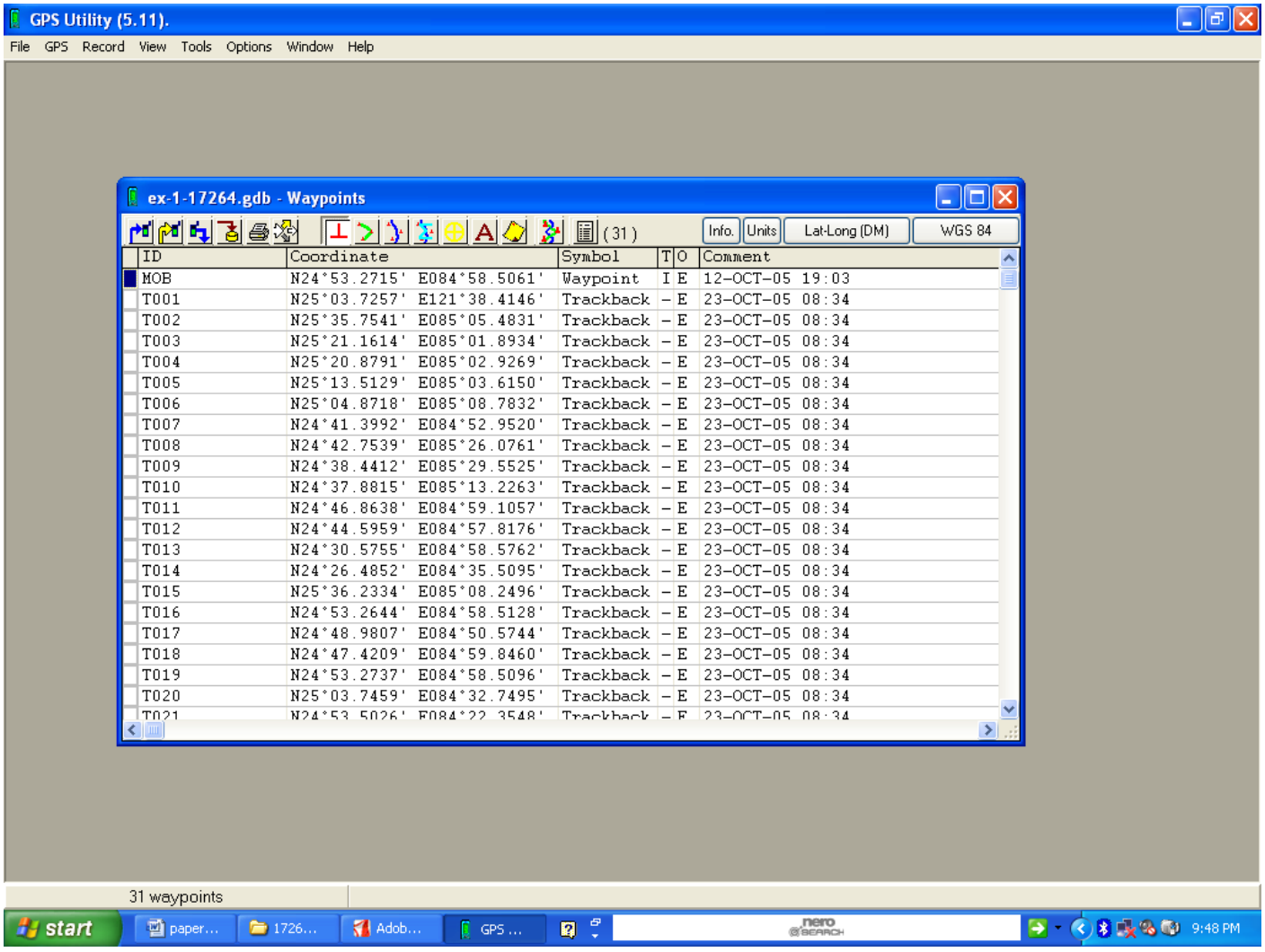
Conclusion

The forensic examination of an embedded device such as GPS receiver was examined thorough with the tools required for such devices and circumspectly experimented with one of the product from one of the largest manufacturer of GPS receiver namely GARMIN with the model no.s 12 and 128 respectively. There are much different types of GPS receivers but the chosen one was done on the basis of its popularity and being used by the offshore fishermen community. The reason of forensically carry out an investigation on a GPS device was to test the feasibility of the forensic investigation of GPS devices as opposed to our standard forensic investigation of digital devices such as computer hard drive. Due to the ubiquity of the GPS device in our contemporary world, the forensics examination of such a device can be used to as a part of indisputable evidence in a court of law which can be used as an indispensable tool to know the terrorism from our sea/ocean coasts.

The determination of position may be described as the process of triangulation using the measured range between the user and four or more satellites.

Acknowledgments

The author will remain grateful to Shri. V Venugopal, Director-in-charge, CFSL, Hyderabad for his moral support and the scientific temperament in bringing out this research article and for giving an opportunity to present the same in a scientific summit. The author also sincerely thanks Dr. C N Bhattacharyya, Chief Forensic Scientist cum Director, Directorate of Forensic Science Services, MHA, New Delhi for the constant encouragement research activity. Finally, the author also takes this opportunity to thank Shri. A K Ganjoo, (former Director, CFSL, Hyderabad) present Director, CFSL, Chandigarh who had given the full opportunity and support during the examination of the case during his tenure as Director at Hyderabad, which could presently transform into an interesting case work study.



ID	Coordinate	Symbol	T	O	Comment
MOB	N24°53.2715' E084°58.5061'	Waypoint	I	E	12-OCT-05 19:03
T001	N25°03.7257' E121°38.4146'	Trackback	-	E	23-OCT-05 08:34
T002	N25°35.7541' E085°05.4831'	Trackback	-	E	23-OCT-05 08:34
T003	N25°21.1614' E085°01.8934'	Trackback	-	E	23-OCT-05 08:34
T004	N25°20.8791' E085°02.9269'	Trackback	-	E	23-OCT-05 08:34
T005	N25°13.5129' E085°03.6150'	Trackback	-	E	23-OCT-05 08:34
T006	N25°04.8718' E085°08.7832'	Trackback	-	E	23-OCT-05 08:34
T007	N24°41.3992' E084°52.9520'	Trackback	-	E	23-OCT-05 08:34
T008	N24°42.7539' E085°26.0761'	Trackback	-	E	23-OCT-05 08:34
T009	N24°38.4412' E085°29.5525'	Trackback	-	E	23-OCT-05 08:34
T010	N24°37.8815' E085°13.2263'	Trackback	-	E	23-OCT-05 08:34
T011	N24°46.8638' E084°59.1057'	Trackback	-	E	23-OCT-05 08:34
T012	N24°44.5959' E084°57.8176'	Trackback	-	E	23-OCT-05 08:34
T013	N24°30.5755' E084°58.5762'	Trackback	-	E	23-OCT-05 08:34
T014	N24°26.4852' E084°35.5095'	Trackback	-	E	23-OCT-05 08:34
T015	N25°36.2334' E085°08.2496'	Trackback	-	E	23-OCT-05 08:34
T016	N24°53.2644' E084°58.5128'	Trackback	-	E	23-OCT-05 08:34
T017	N24°48.9807' E084°50.5744'	Trackback	-	E	23-OCT-05 08:34
T018	N24°47.4209' E084°59.8460'	Trackback	-	E	23-OCT-05 08:34
T019	N24°53.2737' E084°58.5096'	Trackback	-	E	23-OCT-05 08:34
T020	N25°03.7459' E084°32.7495'	Trackback	-	E	23-OCT-05 08:34
T021	N24°53.5026' E084°22.3548'	Trackback	-	E	23-OCT-05 08:34

Figure 4. Screenshots of way point details from GPSU software v.5.11.

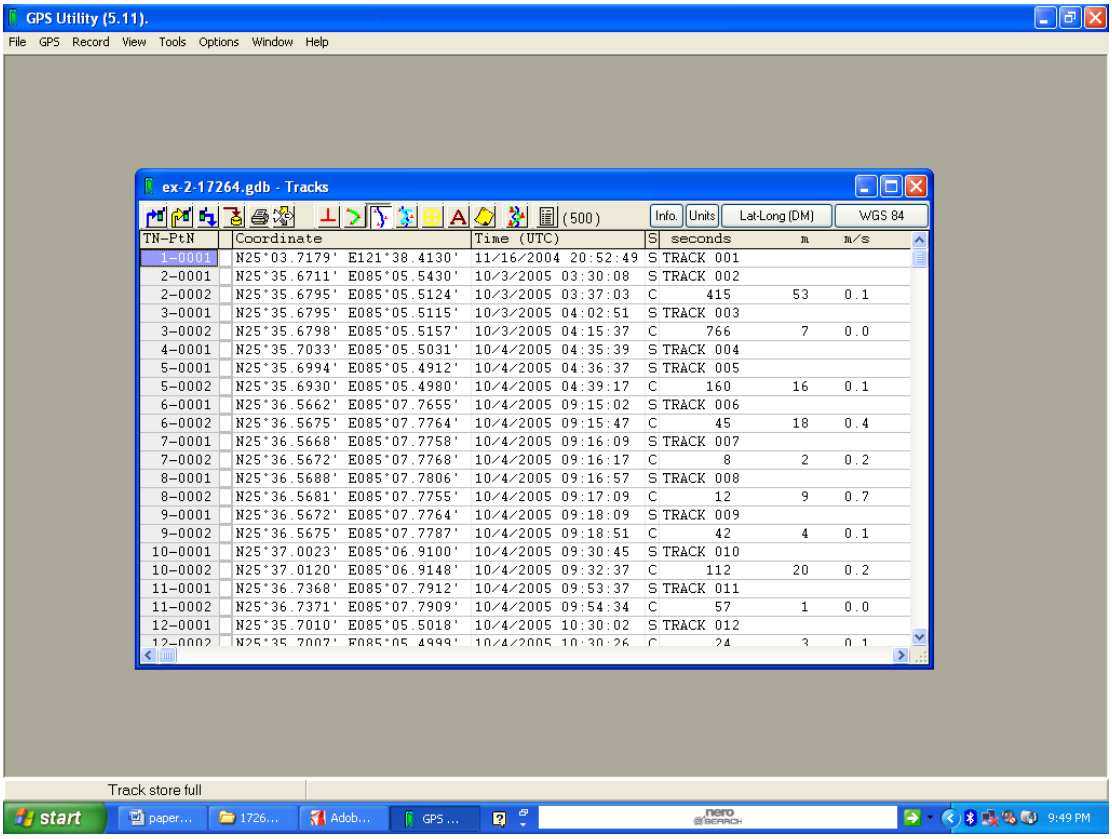


Figure 5. Screenshots of track details obtained from GPS utility ver.5.11 software.

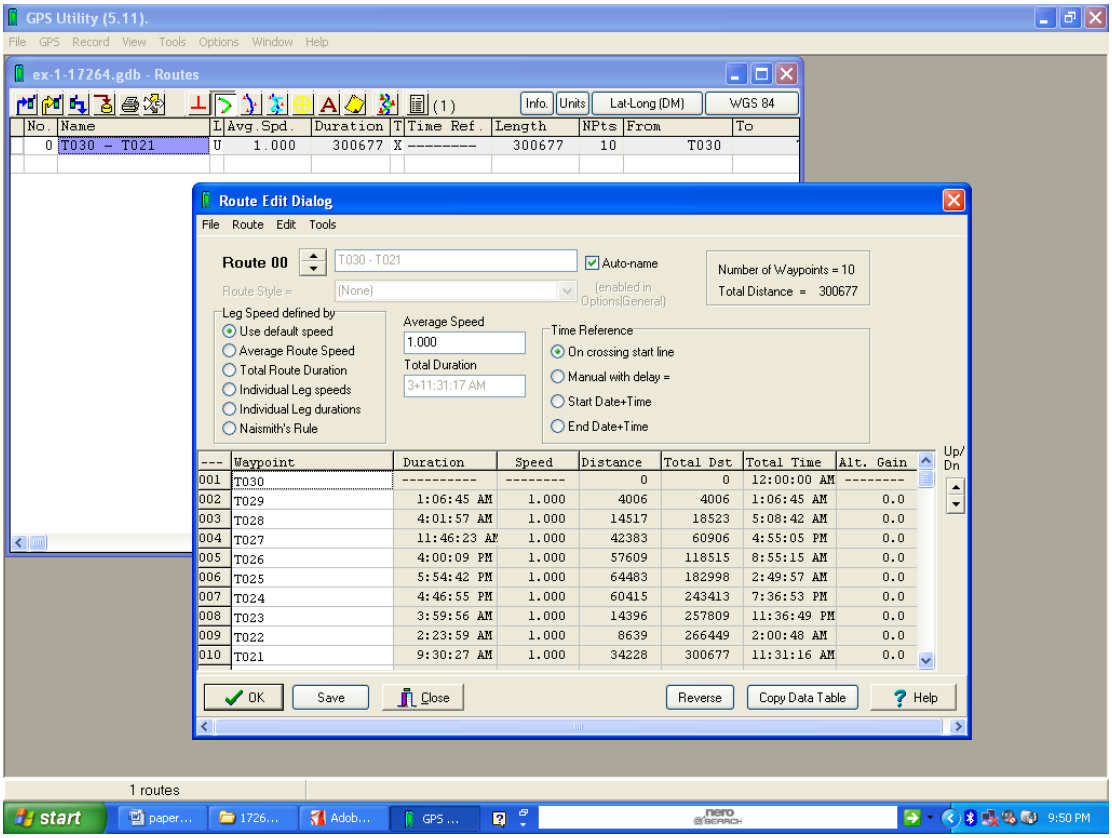


Figure 6. Screenshots of route details-GPS utility ver. 5.11 software.

References

1. B. Nutter (2007) Pinpointing TomTom location records: A forensic analysis. 2008 Elsevier Ltd Peter Hannay, A Methodology for the forensic acquisition of the TomTom One satellite navigation System – A research in progress, Edith Cowan University.
2. Theiss AK, Yen DDCC, Ku CY (2005) Global positioning systems: an analysis of applications, current development and future implementations. Computer Standards & Interfaces 27: 88-100.
3. ACPO (2003) *Good Practice Guide for Computer based Electronic Evidence 3.0*. Retrieved 16 Oct, 2007.
4. Hannay P (2007) A Methodology for the Forensic Acquisition of the TomTom One Satellite Navigation System–A Research in Progress. Paper presented at the 5th Australian Digital Forensics Conference.
5. http://ww.tomtom.com
6. http://www.GPSforensics.org
7. Andy S (2008) The user manual of TomTology software.
8. Nutter B (2008) Pinpointing TomTom location records: A forensic analysis. Science Direct.
9. (CANALYS, 2007) The trend of GPS navigation system http://www.gpsforensics.org/downloads/canalys_20aug07.pdf.