Forensic Analysis of Navman GPS Devices

D. Jones

e-mail: daniel.jameson.jones@gmail.com

Abstract

Navman devices can provide a wealth of information to forensic investigators and could prove to be vital to an investigation. In this paper we focus on one Navman device, including what information is left behind on the device and how that information can be interpreted into meaningful data that can be used by a forensic investigator.

Keywords

Navman, GPS

1. Introduction

Navman devices are some of the more common personal navigation devices around, and can be found on sale in most electronic stores and even in some supermarket chains.

With the availability of such devices, the chances of a forensic investigator encountering one of these devices as part of their investigation is likely. Therefore it pays that an investigator has an understanding of what these devices can store and how useful that information can be in an investigation.

In this paper we focus on the analysis of the Navman iCN320.

Each section of the paper will cover the details of the device, as well as the various files of interest and what information is contained within these files, followed by a conclusion.

2. Specifications of the Navman iCN320

The Navman iCN320 consists of the following hardware specifications outlined in table 1. Note that it appears that the data storage for the device is located on an SD memory card attached to the device; no other storage was identified on the device.

The operating system within the device does not appear to be a Windows CE OS (NavmanUnlocked Wiki (2011)), but may be a variation of a Linux OS as these devices have been modified to operate under a Linux operating system (duff.dk Website (2011)).

Processor:	Intel® PXA-255 300MHz Applications Processor
Memory:	32MB SDRAM
Screen:	2.83" (71.1mm) landscape TFT LCD colour display
Power:	5V DC, 1A
GPS Receiver:	SiRFstarII™
GPS update rate:	Typically every second once fix established
GPS accuracy:	Fix to 5 metres 95% of the time
Hard Drive:	No

Table 1: Technical Specifications of Navman iCN320 (Navman Website (2010))

3. Acquisition of the Navman iCN320

As the SD memory card contained the only known storage from the device it was the only component that could be acquired for further analysis.

The SD memory card was acquired with the use of a write blocked multimedia card adaptor (an Addonics AESDD12U2WP) and FTK Imager (v3.0.0.1443). The result of the acquisition produced a forensic copy (image) of the SD memory card in an EnCase E01 format.

Analysis of the forensic copy was conducted within EnCase v6.16.2.

4. Files of interest within the Navman iCN320

The following files of interest were identified within the 'root' directory of the SD memory card image; the information has been presented in a table containing the name of the file and its purpose.

File Name:	Purpose:
RECENT.DAT	Contains the recently entered destinations.
FAVVER4.DAT	Contains user saved favourite locations.
ROUTE.DAT	Contains the last recorded route entered from the device

Table 2: Details on files of interest from a Navman iCN320

The next sections of the paper cover the analysis of the data structure of each of the identified files.

5. Data analysis of the file 'RECENT.DAT'

The file 'RECENT.DAT' consists of record entries containing the address, latitude and longitude of that record entry. Examination of the file identified no file header or footer associated with the file. The record entries appear to begin at the start of the file.

Each record entry is 520 bytes in length; the first byte seems to be a marker that indicates the type of record entry (possibly how the record was entered into the device, such as a record that was saved from a point on the map or a point of interest (POI) or saved from a location that was manually entered by the user).

The record then contains the name and address of the location, which is stored as plain text, this location appears to be 431 bytes in length.

The record entry then contains some information for a length of 75 bytes; the purpose of this information is unknown.

The next portion of information is the longitude and latitude coordinates, which are 8 bytes in length within the record entry with 4 bytes allocated to the longitude and latitude coordinates respectively; the coordinates are stored as 32-bit signed integers.

Following on from the longitude and latitude coordinates are four bytes containing unknown information, followed by a byte denoting the end of the record entry.

Below is a table containing the details of the structure of a single record entry with the file 'RECENT.DAT':

Offset (Bytes):	**Length (Bytes):**	**Description:**
0	1	Marker (possibly identifying the entry type).
1	431	Free text – containing the name and address of the record entry.
432	75	Unknown
507	4	Longitude Coordinate stored as a 32bit signed integer.
511	4	Latitude Coordinate stored as a 32bit signed integer.
515	4	Unknown
519	1	End of record marker (denoted by 0x00)

Table 3: Table containing layout of a single record entry within the file 'RECENT.DAT'

6. Data analysis of the file 'FAVVER4.DAT'

The file 'FAVVER4.DAT' consists of record entries containing the address, latitude and longitude of that record entry. Examination of the file identified no file header or footer associated with the file the record entries appear to begin at the start of the file.

Each record entry is 1508 bytes in length; with the name of the location stored as plain text starting at the beginning of the record and continuing for 280 bytes in length.

The record entry then contains some information for a length of 72 bytes; the purpose of this information is unknown.

The next portion of information is the longitude and latitude coordinates, which are 8 bytes in length within the record entry with 4 bytes allocated to the longitude and latitude coordinates respectively; the coordinates are stored as 32-bit signed integers. These are stored in the same manner as with the file 'RECENT.DAT'.

Following on from the longitude and latitude coordinates are some mixed data that is unknown and null bytes for 1148 bytes to denoted record length of 1508 bytes.

Below is a table containing the details of the structure of a single record entry with the file 'FAVVER4.DAT':

Offset (Bytes):	**Length (Bytes):**	**Description:**
0	280	Free text – containing the name and address of the record entry.
280	72	Unknown
352	4	Longitude Coordinate stored as a 32bit signed integer.
356	4	Latitude Coordinate stored as a 32bit signed integer.
360	1148	Unknown

Table 4: Table containing layout of a single record entry within the file 'FAVVER4.DAT'

7. Data analysis of the file 'ROUTE.DAT'

The file 'ROUTE.DAT' consists of only one record entry containing the address, latitude and longitude of that record entry.

Examination of the file identified a file header consisting of 5 null bytes (0x00). No file footer was identified.

Each record entry is 532 bytes in length; with the name of the location stored as plain text starting at the beginning of the record and continuing for 432 bytes in length.

The record entry then contains some information for a length of 75 bytes; the purpose of this information is unknown.

The next portion of information is the longitude and latitude coordinates, which are 8 bytes in length within the record entry with 4 bytes allocated to the longitude and latitude coordinates respectively; the coordinates are stored as 32-bit signed integers. These are stored in the same manner as with the file 'RECENT.DAT' and 'FAVVER4.DAT'.

Following on from the longitude and latitude coordinates are sixteen (16) bytes containing unknown information, followed by a byte denoting the end of the record entry.

Below is a table containing the details of the structure of the single record entry with the file 'ROUTE.DAT':

Offset (Bytes):	Length (Bytes):	Description:
5	432	Free text – containing the name and address of the record entry.
437	75	Unknown
512	4	Longitude Coordinate stored as a 32bit signed integer.
516	4	Latitude Coordinate stored as a 32bit signed integer.
520	16	Unknown
536	1	End of record marker (denoted by 0xFF)

Table 5: Table containing layout of a single record entry within the file 'ROUTE.DAT'

8. Conclusion

The basic principles and understandings of the information that can be retrieved from these devices can allow an investigator to enhance their investigation and provide a much greater depth of detail in any investigation involving these types of devices.

Further research can be made into identifying some of the unknown sections of the files identified by the author. From further work tools can be developed to automate the process of analysing these types of devices and better equip an investigator when dealing with such devices and make the process of analysing and reporting these devices that much easier.

9. References

Navman Website (2010), "iCN 320 - Tech Specs", http://www.navman.com/in-car/europe/uk/Products/66739/3431/3435/, (Accessed 30 May 2011)

NavmanUnlocked Wiki (2011), "NavmanUnlocked Wiki - Unlock", http://navmanunlocked.wikispaces.com/Unlock, (Accessed 30 May 2011)

duff.dk Website (2011), "Navman iCN 330 - now with linux", http://duff.dk/navman/, (Accessed 30 May 2011)