Binärfomate cracken

Dennis Keitzel

Universität Hamburg

22. Juni 2010

Inhalt

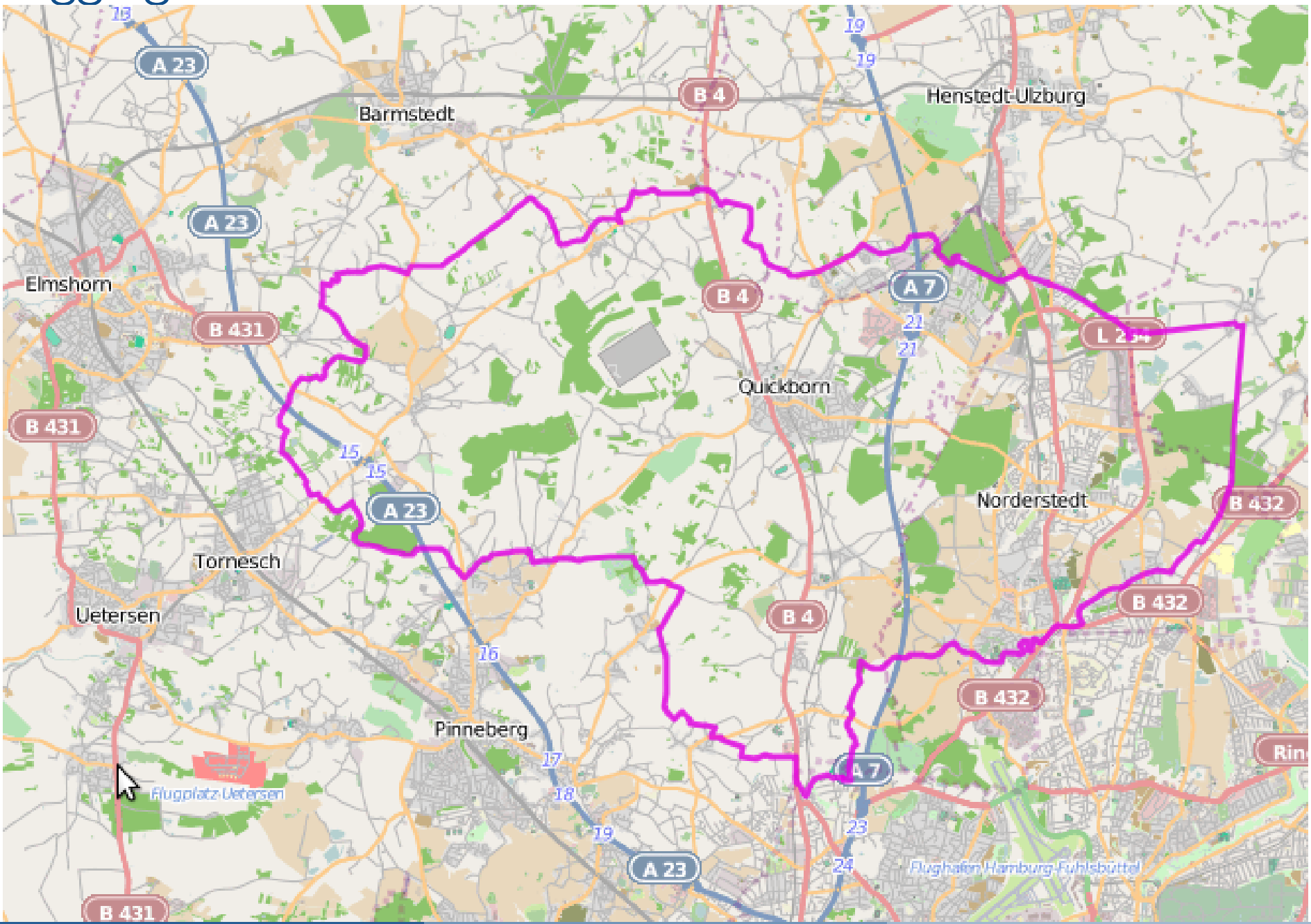
Motivation

- Hardware oft nur unter Windows nutzbar
  - Software nur für Windows verfügbar
  - Keine Quelltexte
  - Keinerlei Spezifikationen
- Software selber schreiben!
- Unbekannte:
  - Kommunikationsprotokoll
  - Datenformat

Gegenstand

- GPS-Mouse/Datalogger: Mainnav MG-950D
- Sirfstar III Chip
- Fahrradtacho
- 2 MB Speicher für ~130'000 Waypoints (Sekundentakt → ~36h)
- Schnittstellen:
  - USB
  - Bluetooth
- Herunterladen der Waypoints mit der Mainnav Software (Windows)
- Aktuelle Positionsdaten auch unter Linux auslesbar (NMEA-Standard)
- Kosten: ~40€ bei eBay

Logging


A 23
B 4
Barmstedt
Henstedt-Ulzburg
A 23
Elmshorn
B 431
B 4
A 7
Quickborn
B 431
A 23
Norderstedt
B 432
Tornesch
Uetersen
B 4
B 432
Pinneberg
B 432
A 7
Flugplatz Uetersen
A 23
Flughafen Hamburg-Fuhlsbüttel
B 431

Voraussetzungen

- Theoretische Grundlagen:
  - Binärcodierungen von Zahlen
  - Endianess
  - ...
- Zeit
- Geduld
- Hohe Frustrationstoleranz
- Gutes Vorstellungvermögen
- Kreativität
- Hex-Editor

Lohnt sich das wirklich?

Theoretische Grundlagen - Binärkodierungen

- Ganzzahlen - Integer:

Dezimalzahl	2-Komplement	1-Komplement	Betrags-Vorzeichen.
17	0 0001 0001	0 0001 0001	0 0001 0001
1	0 0000 0001	0 0000 0001	0 0000 0001
-1	1 1111 1111	1 1111 1110	1 0000 0001
-2	1 1111 1110	1 1111 1101	1 0000 0010

- Brüche → Gleitkomma - Float / Double:
  - IEEE 754 Standard

Theoretische Grundlagen - Byte-Reihenfolge (Endianess)

- Kleinste adressierbare Einheit: 1 Byte
- Reihenfolge bei mehr als einem Byte?

Die Ganzzahl 439.041.101 als 32-bit Integer binär:
00011010 00101011 00111100 01001101

	Big Endian			**Little Endian**		
Adresse	Hex	Dez	Binär	Hex	Dez	Binär
10000	1A	26	00011010	4D	77	01001101
10001	2B	43	00101011	3C	60	00111100
10002	3C	60	00111100	2B	43	00101011
10003	4D	77	01001101	1A	26	00011010

Theoretische Grundlagen - GPS-spezifische Daten

- Längen- und Breitengrade: Float
- Höhe: Int
- Geschwindigkeit: Int
- Zeit: ?

Prinzipielles Vorgehen

Finden von:

- Strukturen
- Ähnlichkeiten
- Unterschiede bei geringen Änderungen der Daten
- Erwarteten Werte

Beispiel am lebendem Objekt

1. Kommunikationsprotokoll herausfinden
2. Heruntergeladene Daten interpretieren

Danke für die Aufmerksamkeit

Quellen

http://de.wikipedia.org/wiki/Integer_(Datentyp)
http://de.wikipedia.org/wiki/Byte-Reihenfolge
http://www.iwriteiam.nl/Ha_HTCABFF.html
http://code.google.com/p/mainnav-reader