

Garmin GCD Firmware Update

File Format

Herbert Oppmann

herby@memotech.franken.de

<http://www.memotech.franken.de/FileFormats/>

2022-05-01

Content

Garmin GCD Firmware Update File Format	3
Basic data types	3
General file structure	3
Header	3
General record structure	4
Sequence of records	5
CheckPoint Record (ID=0x0001)	6
Filler Record (ID=0x0002)	6
Part Number Record (ID=0x0003)	6
Copyright Record (ID=0x0005)	6
Firmware Descriptor Type Record (ID=0x0006)	6
Firmware Descriptor Record (ID=0x0007)	8
Firmware Data Record (ID varies)	9
End Record (ID=0xFFFF)	10
Firmware	10
References	11
Used sources of information	11
Standards and specifications	11
Sources of sample files	11

Garmin GCD Firmware Update File Format

Filename extension *.gcd

This documentation is based on own research and the sources listed in the references section.

Basic data types

All values are serialized in little-endian byte order (least significant byte first).

Type	Length	Description
char	1	ASCII character (see [6])
byte	1	8 bit unsigned integer (range 0 .. 255)
ushort	2	16 bit unsigned integer (range 0 .. 65535)
uint	4	32 bit unsigned integer (range 0 .. 4294967295)

Version:

An ushort where the value is calculated as major version x 100 + minor Version.

E.g. 0x0064 = 100 = V1.0

Compressed part number (see [1]):

The 9x8 bits have to be interpreted as 12 character codes with 6 bits each.

Example: 10 D4 40 56 14 91 0D 14 41

Reverse bytes (shown in binary format with most significant bit (bit 7) first):

0100 0001 0001 0100 0000 1101 ...

Create groups of six bits each:

010000 010001 010000 001101 ...

Add 0x20 = 0010 0000, this may overflow into the 7th bit:

00110000 00110001 00110000 00101101 ...

Interpret bytes as ASCII code:

'0' '1' '0' '-' ...

General file structure

Header
List of Records (without holes)

Header

Type	Content
char[6]	Signature = "GARMIN"
ushort	Format version Seen value: V1.0

General record structure

Type	Content
ushort	Record ID Identifies the record content. See table below.
ushort	Record Length
byte[Record Length]	Record Content

Record ID values for infrastructure records:

Value	Content
0x0001	CheckPoint
0x0002	Filler
0x0003	Part number
0x0005	Copyright message
0x0006	Firmware descriptor type
0x0007	Firmware descriptor
<other>	Firmware data (see table below)
0xFFFF	End

Record ID values for firmware data records:

Value	Content
0x0008	boot.bin
0x02BD	fw_all.bin *.BIN
0x0321	jepp_data – not seen yet
0x0381	bmap_data – not seen yet
0x03C1	bb_data – not seen yet
0x03D5	audio_data – not seen yet
0x03D6	audio_data2 – not seen yet
0x0401	external_data.bin
0x0505	firmware file *.BIN
0x0510	logo (Garmin Bitmap)
0x0511	?
0x051B	?
0x052B	?
0x0533	dskimg_0533.img (in IMG file format containing *.S16 or *.SNR files)
0x0534	?
0x0535	?
0x0536	?
0x0537	?
0x0538	?
0x053A	?
0x0549	?
0x0550	?
0x0555	fw_0555.bin
0x0556	?

Value	Content
0x0557	?
0x055A	?
0x0566	files.bin
0x057F	resources_057F.bin
0x0588	? an ASCII text file
0x0590	?
0x0595	?
0x0599	?
0x059E	resources_059E.bin
0x05A2	? Boot image FAT32 / ZIP file containing *.JPG and *.XML files for Demo
0x05A4	?
0x05A5	TrueType font file, XORed with 0x76 The XOR 0x76 has to be done in addition to (after) the XOR operation indicated in the Firmware Decryptor!
0x05AB	?
0x05B4	?
0x05F5	?
0x05F9	embedded *.GCD file
0x05FA	embedded *.GCD file
0x05FB	embedded *.GCD file
0x05FC	?
0x05FD	embedded *.GCD file
0x05FE	embedded *.GCD file
0x07D0	Just the Firmware Record; no stream (length=0) Combines streams with Record ID values 0x07D1-0x07D3, sometimes only 0x07D3 is present.
0x07D1	?
0x07D2	?
0x07D3	?

The region byte in an RGN file (see my other document [Garmin_RGN_Format](#)) corresponds to the least significant byte of the Record ID in the range 0x0500 to 0x05FF. Additionally, Record ID 0x0008 corresponds with region 0x0C, and Record ID 0x02BD corresponds with region 0x0E.

Sequence of records

Copyright*, Part Number, Copyright*, (Firmware Descriptor Type, Firmware Descriptor, Firmware Data*, Copyright*)+, End

* = zero or more occurrences, + = at least one occurrence

CheckPoint Records and Filler Records may be inserted anywhere in this sequence.

Firmware Data records must cover the complete Length as indicated in the Firmware Descriptor (and may be missing altogether when Length=0).

CheckPoint Record (ID=0x0001)

Length = 1, content is checksum byte.

Can appear anywhere. The content byte is chosen so that the sum over all bytes from the start of the file up to and including the CheckPoint Record is 0x00. It's a way to verify file integrity up to this point.

Filler Record (ID=0x0002)

Length varies, content is always empty (0x00).

Can appear anywhere.

Part Number Record (ID=0x0003)

If Length= 2, the value is 2 bytes HWID

If Length= 9, the value is 9 byte compressed part number

Is always = 0x10, 0xD4, 0x5C, 0x13, 0x04, 0x45, 0x0D, 0x14, 0x41 = "010-10037-00"

Copyright Record (ID=0x0005)

ASCII string, not 0-terminated.

Firmware Descriptor Type Record (ID=0x0006)

Length is multiple of 2.

This is a sequence of field descriptions, each being 2 byte long.

The following Firmware Descriptor Record then contains a sequence of field values, that exactly follows this regarding type and meaning.

Type	Content
byte	Field ID
byte	Field type

Note: For the same Field ID, the meaning is sometimes different depending on the Field type!

Field type values:

Value	Meaning
0x00	byte
0x10	ushort
0x20	uint
0x40	31-byte
0x50	end-of-list

Field ID / Field type combinations:

Field ID	Field type	Meaning
3	end-of-list	End of the list
7	31-byte	
8	ushort	Length of firmware in byte – not seen yet
9	ushort	HWID (hardware identification)
10	byte	XOR used for obfuscating the firmware stream
10	ushort	Record ID used by the following Firmware Data Records for this firmware stream. See table above.
11	byte	Erase flag
12	byte	?
12	ushort	Minimum version
13	ushort	SW (software) version
14	ushort	?
15	ushort	?
16	ushort	?
17	ushort	?
18	ushort	?
19	ushort	?
20	ushort	Some version
21	ushort	Remote software version
21	uint	Length of firmware in byte
22	ushort	?
23	uint	Length of firmware part 1 in byte Only used in Record ID 0x07D0. Part 1 is in Record ID 0x07D1.
24	uint	Length of firmware part 2 in byte Only used in Record ID 0x07D0. Part 2 is in Record ID 0x07D2.
25	uint	Length of firmware part 3 in byte Only used in Record ID 0x07D0. Part 3 is in Record ID 0x07D3.
26	uint	Destination address
32	byte	?

As the length of the firmware descriptor type record is known, there is no real need for the end-of-list field, and actually it is sometimes missing.

Seen sequences of fields:

- Erase flag (byte), XOR (byte), Record ID (ushort), Length (uint), End
- Erase flag (byte), XOR (byte), Record ID (ushort), Length (uint), Version21 (ushort), End
- Erase flag (byte), XOR (byte), Record ID (ushort), Length (uint), Value22 (ushort), End
- Erase flag (byte), XOR (byte), Record ID (ushort), Length (uint), Version21 (ushort), Value22 (ushort), End
- Erase flag (byte), XOR (byte), Record ID (ushort), Length (uint), HWID (ushort), End
- Erase flag (byte), XOR (byte), Record ID (ushort), Length (uint), HWID (ushort), SW Version (ushort), End
- Erase flag (byte), XOR (byte), Record ID (ushort), Length (uint), HWID (ushort), Version12 (ushort), SW Version (ushort), End
- Erase flag (byte), XOR (byte), Record ID (ushort), Length (uint), HWID (ushort), Version20 (ushort), SW Version (ushort), End

- Erase flag (byte), XOR (byte), Record ID (ushort), Length (uint), HWID (ushort), Version20 (ushort), Version21 (ushort), SW Version (ushort), End
- Record ID (ushort), Length (uint), End
- Record ID (ushort), SW Version (ushort), Length (uint), End
- Record ID (ushort), Length (uint), HWID (ushort), End
- Record ID (ushort), Length (uint), HWID (ushort), SW Version (ushort), End
- Record ID (ushort), Length (uint), HWID (ushort), Version12 (ushort), SW Version (ushort), End
- Record ID (ushort), Length (uint), HWID (ushort), SW Version (ushort), Value22 (ushort), End
- Record ID (ushort), Length (uint), HWID (ushort), Version20 (ushort), Version21 (ushort), SW Version (ushort), End
- Record ID (ushort), Length (uint), HWID (ushort), Version20 (ushort), Version21 (ushort), SW Version (ushort), Value22 (ushort)
- Record ID (ushort), Length (uint), HWID (ushort), Version20 (ushort), Version21 (ushort), SW Version (ushort), Value22 (ushort), End
- 7 (31 byte), Value32 (byte), Record ID (ushort), Value12 (byte), SW Version (ushort), Value14 (ushort), Value15 (ushort), Value16 (ushort), Value17 (ushort), Value18 (ushort), Value19 (ushort), Length (uint), Destination address (uint), End
- HWID (ushort), Record ID (ushort), Length (uint), Length part 3 (uint), End
- HWID (ushort), Record ID (ushort), Length (uint), Length part 1 (uint), Length part 2 (uint), Length part 3 (uint), End
- Length part 2 (uint), HWID (ushort), Record ID (ushort), Length (uint), Length part 3 (uint), End

Observations:

- Field Value22, if present, is always at the end
- The fields Erase flag (byte) and XOR (byte) form a set; they are present all or none
- The fields Value7, Value32, Value12, Value14-19 and Destination address form a set; they are present all or none

Firmware Descriptor Record (ID=0x0007)

This record has a variable length. It contains the sequence of fields as described in the Firmware Descriptor Type Record.

Seen values:

Field ID	Field type	Meaning
3	end-of-list	- none -
7	31-byte	2f 29 fe 3f ba af ee f7 16 6d 4f 37 31 a3 1f 4d 40 5a 1e 18 3a 90 ea 53 8f 02 5e e8 db a7 39 e8 50 11 47 b9 62 1a e8 65 e7 c6 9c 5a 1a 78 b4 97 e6 d8 b8 cf 2d 84 63 71 4f 5c b4 42 05 5e 62 ae 87 e0 82 9b 2a 29 77 b9 d2 59 a5 ba 5b 49 ea da fa 8e cb bb b6 85 13 5e 1f 8b 28 9a 7b ...
9	ushort	HWID (hardware identification) For a list of known values see my other document Garmin_BIN_Format
10	byte	XOR used for obfuscating the firmware stream 0x00, 0x01, 0x13, 0x1B, 0x43, 0x45, 0x49, 0x52 The XOR value is usually the same for all firmware streams within one GCD file.

Field ID	Field type	Meaning
10	ushort	Record ID used by the following Firmware Data Records for this firmware stream. See table above.
11	byte	Erase flag seen: 0 and 1
12	byte	1
12	ushort	Minimum version seen: 0.50, 1.2, 1.6, 3.20
13	ushort	SW version
14	ushort	seen: 0xFE39, 0x3DA3, 0x1634, 0x823F, 0xBD51, 0xF19F
15	ushort	seen: 16..32
16	ushort	seen: 0xAAC2, 0xB587, 0x4989, 0x5867, 0x5128, 0xA722
17	ushort	seen: 0x84F9, 0xB353, 0x85F6, 0xCC0E, 0xD6FA, 0x2611
18	ushort	seen: 0xAF2F, 0xE55F, 0x593D, 0xBF7B, 0x372D, 0x90B6
19	ushort	seen: 0x1A98, 0x751A, 0xDF34, 0x904F, 0x8932, 0xA92D
20	ushort	Some version 0.1, 0.23, 0.24, 0.28, 0.30, 0.34, 0.43, 0.50, 0.53, 0.54, 0.70, 0.74, 0.89, 1.2, 1.3, 1.4, 1.19, 1.80, 2.0, 2.2, 2.3, 2.10, 2.20, 2.30, 2.40, 2.50, 3.00, 3.14, 3.42, 4.87
21	ushort	Remote software version 0.1, 0.10, 0.11, 0.20, 0.21, 0.25, 0.50, 0.59, 0.78, 0.90, 1.0, 1.1, 1.4, 1.31, 1.42, 1.7, 2.0, 2.3, 2.10, 2.20, 2.30, 2.31, 2.60, 2.82, 3.8, 3.10, 3.20, 3.41, 3.90, 4.2, 4.40, 4.62, 4.80, 5.3, 5.17, 7.32, 8.0
21	uint	Length of firmware in byte
22	ushort	0x0000, 0x0400, 0x0800, 0x0C00, 0x1000, 0x1400, 0x1800, 0x1C00, 0x2000, 0x2400, 0x2800, 0x2C00, 0x3340, 0x3800, 0x3801, 0x3C00, 0x4400, 0x4800, 0x4B01, 0x5000, 0x5400, 0x5800, 0x6400, 0x6800, 0x6C00, 0x7000, 0x7400, 0x7800, 0x8000, 0x8400, 0x8800, 0x8C00, 0x9000, 0x91B4, 0x9400, 0x9401, 0x957E, 0x9800, 0x9C00, 0xA000, 0xA400, 0xA800, 0xAC00, 0xB000, 0xB400, 0xB800, 0xBC00, 0xC000, 0xC400, 0xC800, 0xCC00, 0xD000, 0xD400, 0xDC00, 0xE000, 0xE400, 0xE800, 0xEC00, 0xFC00, 0xFC01
23	uint	Length of firmware part 1 in byte Only used in Record ID 0x07D0. Part 1 is in Record ID 0x07D1.
24	uint	Length of firmware part 2 in byte Only used in Record ID 0x07D0. Part 2 is in Record ID 0x07D2.
25	uint	Length of firmware part 3 in byte Only used in Record ID 0x07D0. Part 3 is in Record ID 0x07D3.
26	uint	Destination address
32	byte	seen: practically all byte values

Firmware Data Record (ID varies)

The Firmware Descriptor Record contains the length of the firmware stream. This length can be much more than what a single Firmware Data Record may hold, so there are as many Firmware Data Records following until the complete firmware stream is done. The total length of a firmware stream is sometimes four more than the size indicated in the Firmware Descriptor Record.

Each Firmware Data Record can hold up to 0xFFFF byte, but the usual length, except for the last record of course, is 0xFF00. But other lengths have also been seen on the first record:

0xFF08, 0xFF40

The Record ID varies (see Record ID table above), but it is the same across all Firmware Data Records belonging to one firmware stream. The same Record ID can appear multiple times in a GCD file, so it is more a firmware stream type than a unique identification.

End Record (ID=0xFFFF)

Length is 0.

Firmware

See my other document [Garmin_BIN_Format](#).

References

Used sources of information

- [1] <https://www.gpspower.net/garmin-maps/266563-garmin-transalpin-2012-pro-10.html>
- [2] <https://reverseengineering.stackexchange.com/questions/6867/trying-to-reverse-gps-watch-firmware-image-with-binwalk>
- [3] http://www.gpspassion.com/forumsen/topic.asp?TOPIC_ID=115804
- [4] http://www.gpspassion.com/forumsen/topic.asp?TOPIC_ID=117239
- [5] RGN_Tool http://www.gpspassion.com/forumsen/topic.asp?TOPIC_ID=137838,
https://web.archive.org/web/20170718095456/http://turboccc.wikispaces.com:80/RGN_Tool

Standards and specifications

- [6] ISO/IEC 646:1991, Information technology – ISO 7-bit coded character set for information interchange

Sources of sample files

- [7] Garmin Marine Device Software Updates <http://www8.garmin.com/support/software/marine.html>
- [8] Russification of Garmin GPS devices <https://sourceforge.net/projects/flawia/?source=navbar>
- [9] <http://www.gmaptool.eu/pl/content/trail>
- [10] <http://gpsrchive.com/>
- [11] <https://www.dropbox.com/sh/60fl2temsbf29j/AAAAX1-vz-M-LWhnGs5aAsvCa?dl=0>
- [12] <https://wiki.ubuntuusers.de/Garmin/Firmware/>
- [13] <http://www.tramsoft.ch/DOWNLOADS/GARMIN/>