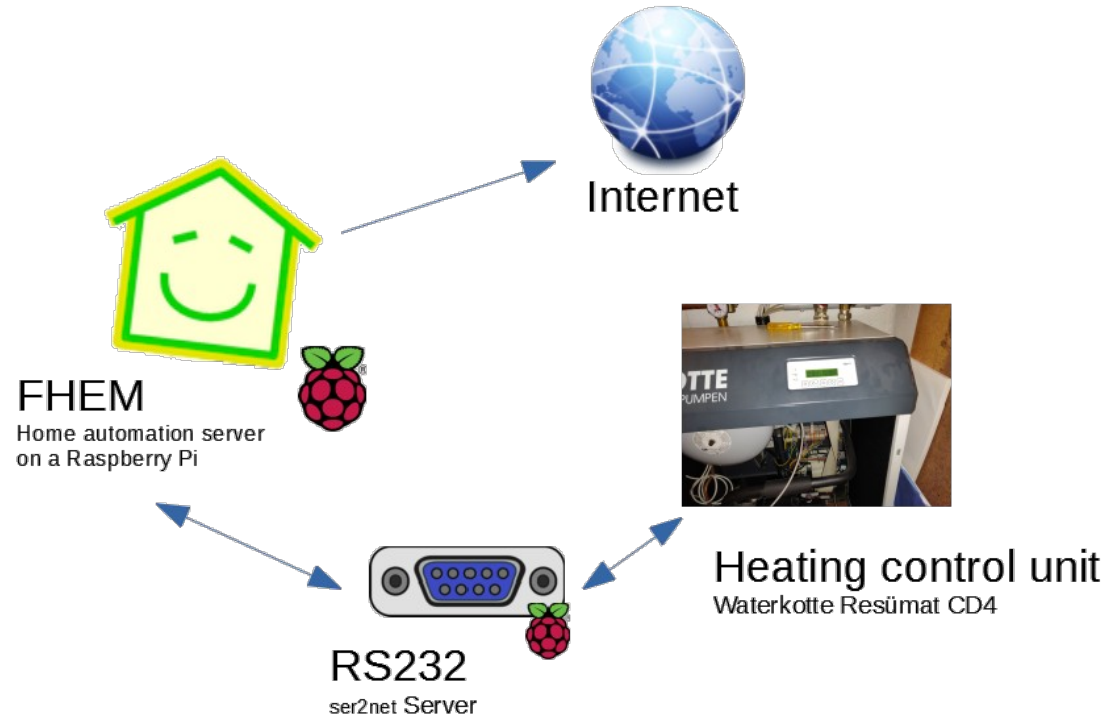


- Waterkotte „Resümat CD4“ (2002) as control unit
- RS232 serial port available
- Serial protocol uses hexadecimal data
- Already reverse engineered by people in online forums
- Protocol has read and write options
- Protocol uses a CRC-16 (checksum) with special parameters



10 02 01 15 0000 00FF 10 03 7C1A
START MODE OFFSET BYTES END CRC

Read 255 bytes starting from 0x00

Available modes:

- 01 15 Read
- 01 14 Set clock (time + date)
- 01 13 Write

CRC-16 (Hex)
CRC-16/BUYPASS

Poly: 0x8005
Init: 0x0000
LSB: 0x0000
Inp. rev: no
Res. rev: no
<https://crccalc.com>

Internet of Things

Manual analysis

Cmd: Read mem
STX: 10 02
Read address: 01 15
Stop address after start: 00 FF
CRC 16, PAY 8005: 10 03
MIT O: 7C 1A
USB D: 7C 1A

Kennwort 99 → Mehr Infos

WATERKOTTE RESUMAT CD4

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|--|--|
| 00000000 | 16 | 18 | 02 | 00 | 17 | 52 | 6C | 83 | 3F | 20 | 5C | 3E | 3F | F7 | 3C | 84 | 3F | 5F | EF | D5 | 41 | E8 | 21 | E4 | 41 | 71 | 2E | 09 | 42 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | E0 | B8 | D4 | | |
| 00000028 | 3E | 16 | 55 | 22 | C0 | 85 | 08 | 39 | C0 | 21 | 9E | F4 | 41 | 72 | 72 | 42 | 42 | 22 | 26 | 0F | 1E | 0C | 12 | 1C | 1E | 08 | 07 | 09 | 01 | 2B | A1 | EE | 46 | 93 | 1F | C0 | 45 | 00 | 01 | 01 | | | | | |
| 00000050 | 01 | 01 | 01 | 01 | 5F | 97 | 0F | 47 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 26 | D5 | 00 | 00 | 00 | 00 | 35 | 38 | 12 | 1C | 02 | 10 | 10 | 40 | 2C | 24 | 00 | 00 | E1 | C5 | 2E | 41 | 70 | B4 | | | | | |
| 00000078 | 12 | 3F | FE | 67 | C6 | BF | 57 | C4 | 2B | 40 | EC | 85 | AD | 41 | 2A | 92 | 65 | 42 | 0D | CF | 3F | 42 | 30 | BC | D7 | 41 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 00 | 01 | 00 | 00 | 02 | A3 | 20 | 00 | | | | |
| 000000a0 | 20 | 00 | 00 | 00 | 02 | 00 | 00 | 00 | 00 | 00 | 03 | 01 | 04 | 1C | 04 | 00 | 0C | 0A | 0E | 1E | 0C | 12 | A6 | 23 | 00 | 00 | D4 | FF | 7F | 41 | 5A | 00 | B8 | 41 | F2 | FF | C7 | 41 | 00 | 00 | | | | | |
| 000000c8 | 00 | 00 | 00 | 00 | 18 | 00 | 00 | 15 | 00 | 00 | 05 | 5A | 00 | 00 | 00 | 00 | 00 | 00 | 00 | C0 | 00 | 00 | 20 | 42 | 00 | 00 | 20 | 42 | 00 | 00 | 00 | 40 | 02 | 00 | 00 | 00 | 05 | 00 | 00 | 17 | | | | | |
| 000000f0 | 18 | 00 | 44 | 42 | 00 | 00 | 00 | 41 | F5 | FF | BF | 40 | 00 | 00 | 00 | 3F | 1F | 3F | 00 | 02 | 04 | 10 | 03 | 86 | C6 | 16 | 1 | | | | | | | | | | | | | | | | | | |

Länge
0x109

Uhrzeit: 23:02:56

a3b a3a a39

wof d45 a26 d38

a17

a3c a3d a3e

1e 0c a17

d30 d42 d48

Datum: 31.12.18

d34

a41 a40 a3F

08 1e d30 1c d28

Versions-Datum

aad. 0xae. 0xaf

y28.04.2000

04C 04 00

2.07 Ww Zeit Ein

05 00 00

0xec 0xeb 0xee

2.02 Ww Zeit Aus

0xef 0xee 0xed

0x17 00 00

y22

Messbeginn-Zeit

HH:MM:SS

a41 a40 a3F

08 1e d30 1c d28

CPU-Boot-Zeit

0xb2 0xb1 0xb0

0xb2 0xb1 0xb0

CPU-Boot-Datum

0xb3 0xb4 0xb5

1e 0c 12

d30 d42 d48

3.07 Kompr Beginn-Zeit

0x50 0x4F 0x4E

01 01 01

3.08 Kompr Beginn Datum

DD.MM.YY

0x51 0x52 0x53

Messbeginn-Datum

DD.MM.YY

a42 a43 a44

07 09 01

1.08 Anhebung Aus

HH:MM:SS

aed2 aed1 aed0

05 00 00

1.07 Anhebung Ein

HH:MM:SS

aecf aeae aecd

0x15 00 00

d21

Ausfall-Zeit

0xb8 0xb7 0xb6

0x12 0x38 0x35

d48 d56 d53

Hz

1.06 Zeit Aus

HH:MM:SS

acec acdb accd

0x10 0x00 00

1.07 Zeit Ein

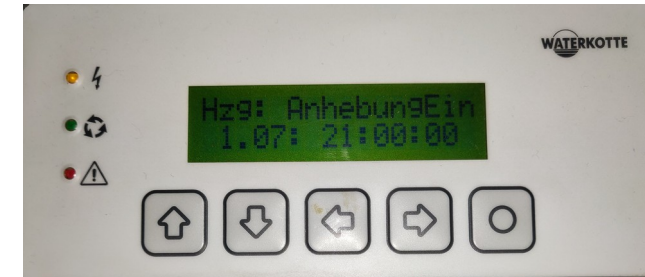
HH:MM:SS

acd9 acd8 acd7

00 00 00

6.00 Kennwort

0x99 01



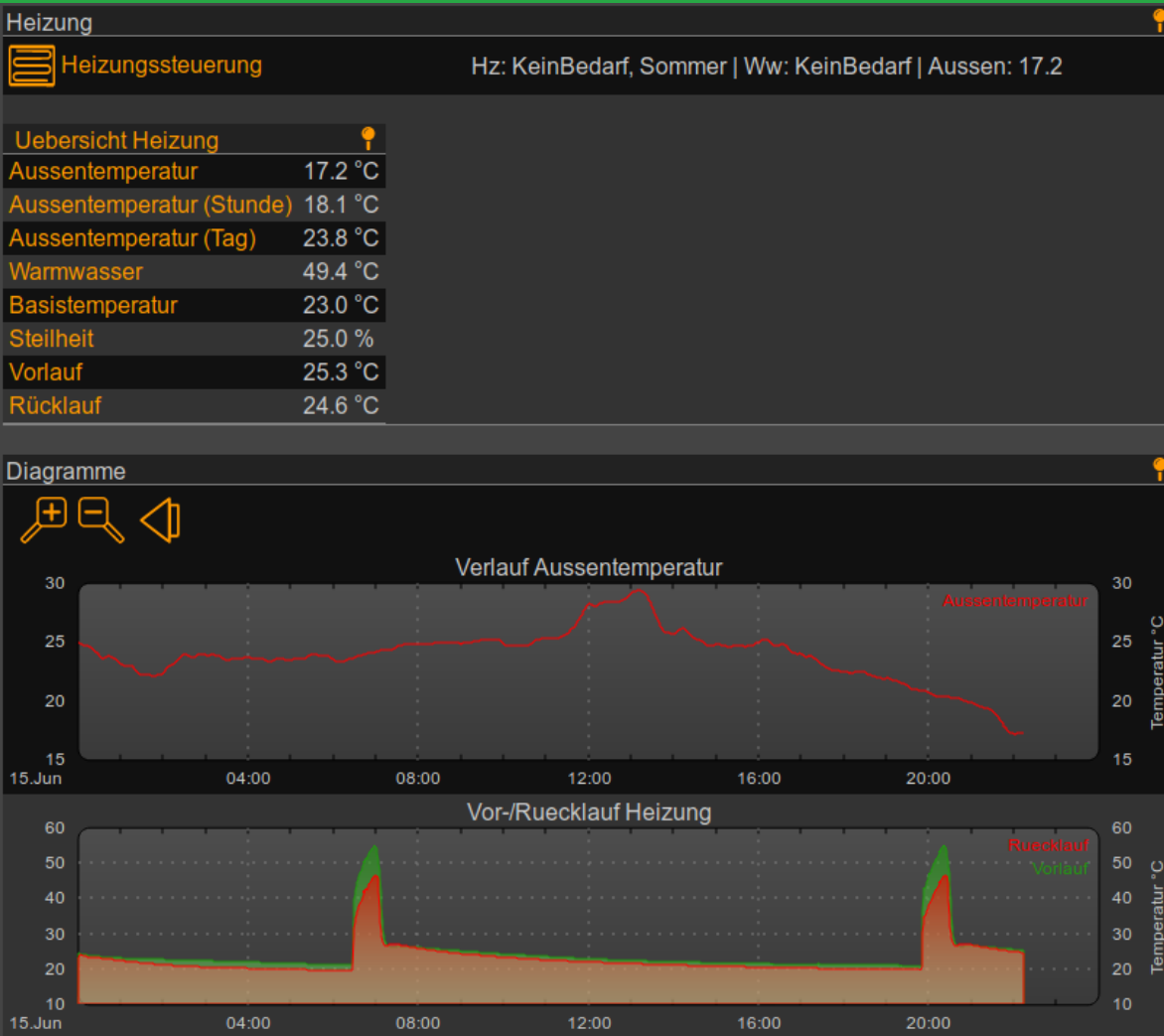
- Finding out offsets/addresses by comparing hex data with values on the display
- Floats: IEEE 754 (little endian)
- Used hex editor: Bless

| Feldname | Menünummer | Adresse | Länge | Typ |
|-----------------------|------------|---------|-------|-----|
| Temp-Aussen | 0.00 | 0 | 4 | f |
| Temp-Aussen-24h | 0.01 | 4 | 4 | f |
| Temp-Aussen-1h | 0.02 | 8 | 4 | f |
| Temp-Ruecklauf-Soll | 0.03 | 0C | 4 | f |
| Temp-Ruecklauf | 0.04 | 10 | 4 | f |
| Temp-Vorlauf | 0.05 | 14 | 4 | f |
| Temp-Raum | 0.06 | 18 | 4 | f |
| Temp-Raum-1h | 0.07 | 1C | 4 | f |
| Temp-WQuelle-Ein | 0.08 | 20 | 4 | f |
| Temp-WQuelle-Aus | 0.09 | 24 | 4 | f |
| Temp-Verdampfer | 0.10 | 28 | 4 | f |
| Temp-Kondensator | 0.11 | 2C | 4 | f |
| Ww-Temp | 2.03 | 30 | 4 | f |
| Uhrzeit | 3.00 | 34 | 3 | t |
| Datum | 3.01 | 37 | 3 | d |
| Messbeginn-Zeit | 3.02 | 3A | 3 | t |
| Messbeginn-Datum | 3.03 | 3D | 3 | d |
| Hz-Messergebnis | 3.04 | 41 | 4 | f |
| Ww-Messergebnis | 3.05 | 44 | 4 | f |
| Mess-Reset | 3.06 | 48 | 1 | c |
| KomprBeginn-Zeit | 3.07 | 49 | 3 | t |
| KomprBeginn-Datum | 3.08 | 4C | 3 | d |
| KomprBetrStunden | 3.09 | 4F | 4 | f |
| Kompr-Mess-Reset | 3.10 | 53 | 1 | c |
| Unterbrechungen | 4.00 | 54 | 1 | b |
| Warnung-Eingang | 4.01 | 55 | 1 | b |
| Warnung-Ausgang | 4.02 | 56 | 1 | b |
| Warnung-Sonstige | 4.03 | 57 | 1 | b |
| Ausfaelle | 4.04 | 58 | 1 | b |
| Fuehler-Ausfall | 4.05 | 59 | 1 | b |
| Fuehler-KurzSchl | 4.06 | 5A | 1 | b |
| FuehlerZaehler0 | 4.07 | 5B | 2 | n |
| FuehlRaum-Ausfall | 4.08 | 5D | 1 | b |
| FuehlRaum-KurzSchl | 4.09 | 5E | 1 | b |
| FuehlRaum-Zaehler0 | 4.10 | 5F | 2 | n |
| Ausfall-Zeit | 5.00 | 61 | 3 | t |
| Ausfall-Datum | 5.01 | 64 | 3 | d |
| Ausfall-Betriebszust. | 5.02 | 67 | 1 | b |
| Ausfall-Do-Buffer | 5.03 | 68 | 1 | b |
| Ausfall-Di-Buffer | 5.04 | 69 | 1 | b |
| Ausfall-FuehlAusfall | 5.05 | 6A | 1 | b |

- Inserting the new addresses into the FHEM plugin (Perl)
- Add some own improvements (writing special fields)

```
my %frameReadings = (  
  'Temp-Aussen'          => { addr => 0x000, bytes => 0x004,  
                               menu => '0.00', fmat => '%0.1f', unp => 'f<' },  
  
  'Temp-Ruecklauf-Soll'  => { addr => 0x00C, bytes => 0x004,  
                               menu => '0.03', fmat => '%0.1f', unp => 'f<' },  
  
  'Temp-Ruecklauf'       => { addr => 0x010, bytes => 0x004,  
                               menu => '0.04', fmat => '%0.1f', unp => 'f<' },  
  
  'Temp-Vorlauf'         => { addr => 0x014, bytes => 0x004,  
                               menu => '0.05', fmat => '%0.1f', unp => 'f<' }  
);
```

- FHEM plugin requests and processes heating data every minute



Thanks for your attention!

Further questions?

Sources:

- Private knowledge
- <https://www.iotforall.com>
- <https://www.wired.co.uk>
- <https://www.pocket-lint.com>
- <https://digibusters.com>
- <https://www.sap.com>