

# Reverse Engineering

## Sniffen

Wie man EMS Telegramme identifiziert und z.B. in den „collectord“ einbaut, hat Michael Moosbauer (moosy) detailliert [im Thread](#) beschrieben. In der Zwischenzeit (Mitte April 2014) sind einige Änderungen eingetreten, so dass moosys aktualisierter Text, auch der einfacheren Auffindbarkeit halber, hier noch einmal wiedergegeben wird.

## HowTo

Der Einbau eines neuen Features ist eigentlich immer gleich:

- Identifizierung der Parameter/Werte, die man ändern/einstellen kann.
- Herausfinden, in welchen Telegrammen sie stecken. Das geht mit dem collectord recht leicht, allerdings muss hierzu der ems-collector mit Raw-Kommando-Support gebaut werden (Zeile 3 des Makefiles auskommentieren, d.h. Raute entfernen). Dann im collectord:

```
a) 'raw read <device> <type> <offset> <len>' also:  
   raw read DE TY 0 25 , wobei DE das DEVICE is (also 0x10=RC35, 0x08=UBA),  
   und TY der Telegrammtyp, den man im Verdacht hat, dass er zuständig ist.  
   Ausgabe merken.  
b) Wert am RCxx[x] verstellen  
c) a) wiederholen. Wenn sich was geändert hat, ist es ein heißer Kandidat.  
d) a) - c) wiederholen um sicherzugehen  
e) raw read DE TY OFF 1 , wobei OFF der ausgezählte Offset ist,  
   so lange probieren, bis genau dieser eine Wert da steht  
f) 'raw write <device> <type> <offset> <data0> ... <dataX>', also:  
   raw write DE TY OFF <andererWert> und gucken, ob sich der Wert am  
   RCxx[x] geändert hat.  
   WENN NICHT: mit raw write DE TY OFF <Wert aus e)> alten Wert  
   wiederherstellen.  
g) Für die Messwerte parallel die Werte am RCxx[x] ablesen und per raw read  
   gucken,  
   ob man sie irgendwo findet (dabei beachten: raw read liefert hex,  
   Temperaturen sind  
   oft verdoppelt  $30^{\circ}=60$  oder verzehnfacht  $30^{\circ}=300$ ).
```

- Ins EMS-Wiki eintragen (lassen)
- In den ems-collector einbauen (lassen)
- Ins Webinterface einbauen (lassen)

From:

<https://emswiki.thefischer.net/> -

Permanent link:

<https://emswiki.thefischer.net/doku.php?id=wiki:ems:re>

Last update: **2015/12/30 21:00**

