

# 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, hier noch einmal wieder gegeben wird.

## HowTo

Der Einbau eines neuen Features ist eigentlich immer gleich:

1. Identifizierung der Parameter/Werte, die man ändern/einstellen kann. 2. 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 10=RC35, 08=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) emsqry DE TY OFF 1 , wobei OFF der ausgeählte Offset ist,  
so lange probieren, bis genau dieser eine Wert da steht
- f) emscmd DE TY OFF <andererWert> und gucken, ob sich der Wert am  
RC35 geändert hat.  
WENN NICHT: mit emscmd DE TY OFF <Wert aus e)> alten Wert  
wiederherstellen.

3. Für die Messwerte parallel die Werte am RC35 ablesen und per emsqry

gucken, ob man sie irgendwo findet (dabei beachten: emsqry liefert

hex,

Temperaturen sind oft verdoppelt  $30^\circ = 60$  oder verzehnfacht  $30^\circ =$

300).

4. Ins EMS-Wiki eintragen (lassen) 5. In den ems-collector einbauen (lassen) 6. Ins Webinterface einbauen (lassen)

From:

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

Permanent link:

<https://emswiki.thefischer.net/dokuwiki/doku.php?id=wiki:ems:re&rev=1397835637>



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