j0199727

Version:   
Autor:   
Datum:

# Vorbereitung

## Wireshark

Der Wireshark ist ein Programm welches das Netzwerk aushorchen kann, diese Programme nennt man auch sniffer, der wireshart kann mit Hilfe von Plug-Ins verschiedene Protokolle auseinander nehmen und sozusagen in Klartext umwandeln,

wen man dies gemacht hat kann man das auseinandergenommene Protokoll als Text ausdrucken und dies dann mithilfe des Atom Viewer

## Atom Viewer

Um die beigelegten Daten zu betrachten zu können benötigen sie den Atom Viewer [(Installation File (v1.7.1))](file:///E:\S7-comm\AtomSetup(v1.7.1).exe) oder online aktuellste Version vom [Atom](https://atom.io/download/windows) Viewer, zusätzlich wird das von mir erstellte [S7-comm packet](https://github.com/FaMosIndustries/s7-commplus.git) benötigt welches sie über den Link downloaden können, laden sie hierzu am besten das komplette Master Paket herunter und folgt den Anweisungen im readme

Wenn in dem Ordner in dem sich dieses Dokument befand weine s7c Dateien befinden können sie diese [[hier]](https://github.com/FaMosIndustries/s7-commplus.git) herunterladen (derselbe Ort wie das S7-comm packet)

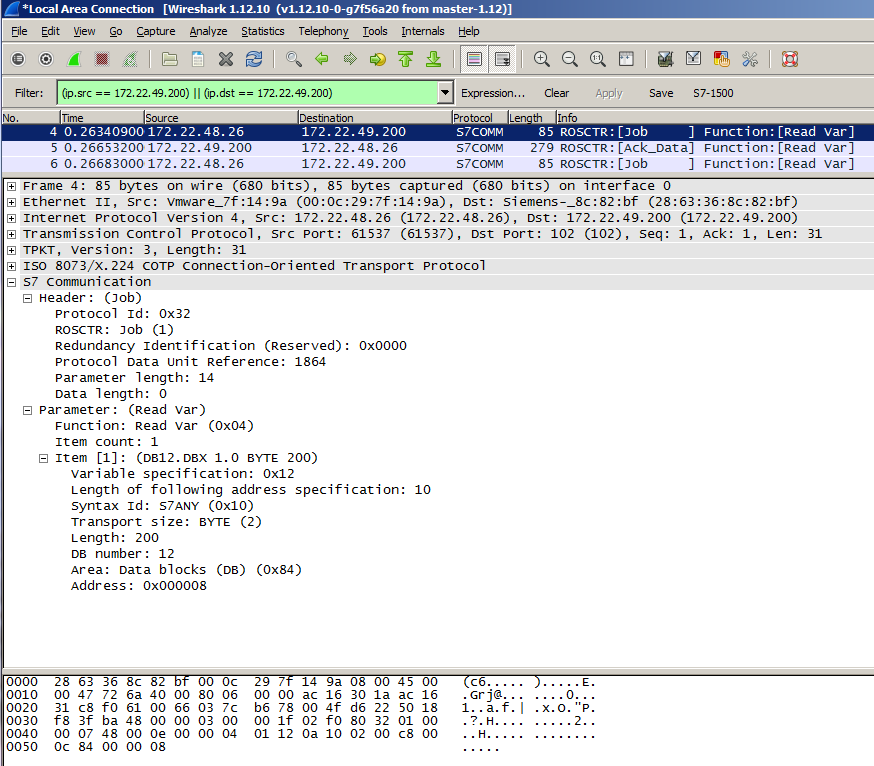
Um die Datei zu öffnen gehen sie wie folgt vor

1. Wenn sie den Atom Viewer noch nicht installiert haben, installieren sie diesen bitte zuerst bevor sie fortfahren
2. Wenn sie das S7 comm packet bereits in den Ordner packages hinzugefügt haben überspringen sie punkt 3 ansonsten müssen sie schritt 3 Durchführen
3. Öffnen sie das Verzeichnis indem sie Atom installiert haben, meist C:\Users\<USERNAME>\.atom nun benötigen sie das S7 comm packet das sie heruntergeladen haben und entpacken sie dies (wenn noch nicht heruntergeladen [[hier]](https://github.com/FaMosIndustries/s7-commplus.git)) und kopieren sie den Ordner [PRE-RELEAS-S7\_comm-plus] in den Ordner [packages]
4. Nun haben sie die Erweiterung hinzugefügt und sie können den Atom starten
5. Wenn sie den Viewer gestartet haben können sie die Dateien ansehen in dem sie sie entweder per drag and drop in den Viewer ziehen ober in dem sie im Menu "File" auf "Open Files"(Ctrl+O)oder "Open Folder"(Ctrl+Shift+O) gehen und dann die entsprechend Datei oder den entsprechenden Ordner auswählen.

# Vorgehen zur Analyse der Datentelegramme

## Aufzeichnen der Telegramme mit WireShark

Um eine Aufzeichnung zu starten muss die netzwerkkarte ausgewählt werden mit der die Protokolle aufgezeichnet werden können, dann braucht man nur noch den sniffer zu starten und dann kann das entsprechende Daten Paket eingesehen werden, dies ist jedoch nicht sehr komfortabel,

hier ein Ausschnitt vom wiershark eines alten Kommunikation Protokoll, 

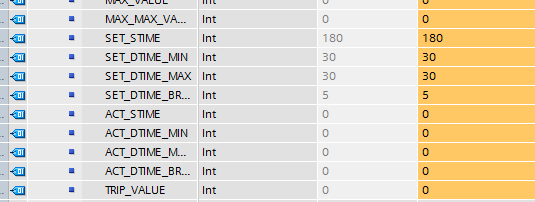
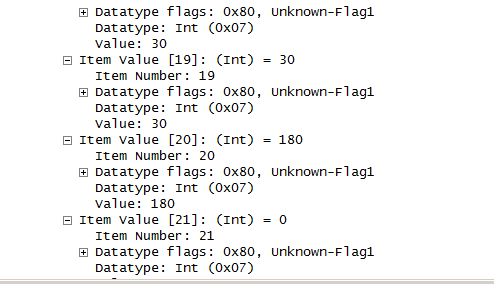
das Telegramm besteht hier aus nur einem wert.

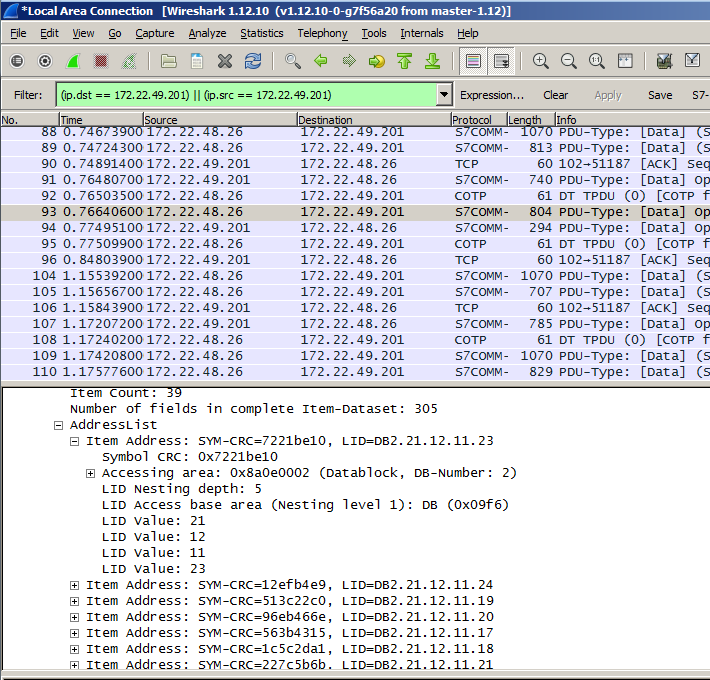
## Export als Text

Via rechtsklick kann man dann auf print gehen und es dann als Datei ausdrucken wodurch man eine Text Datei erhält

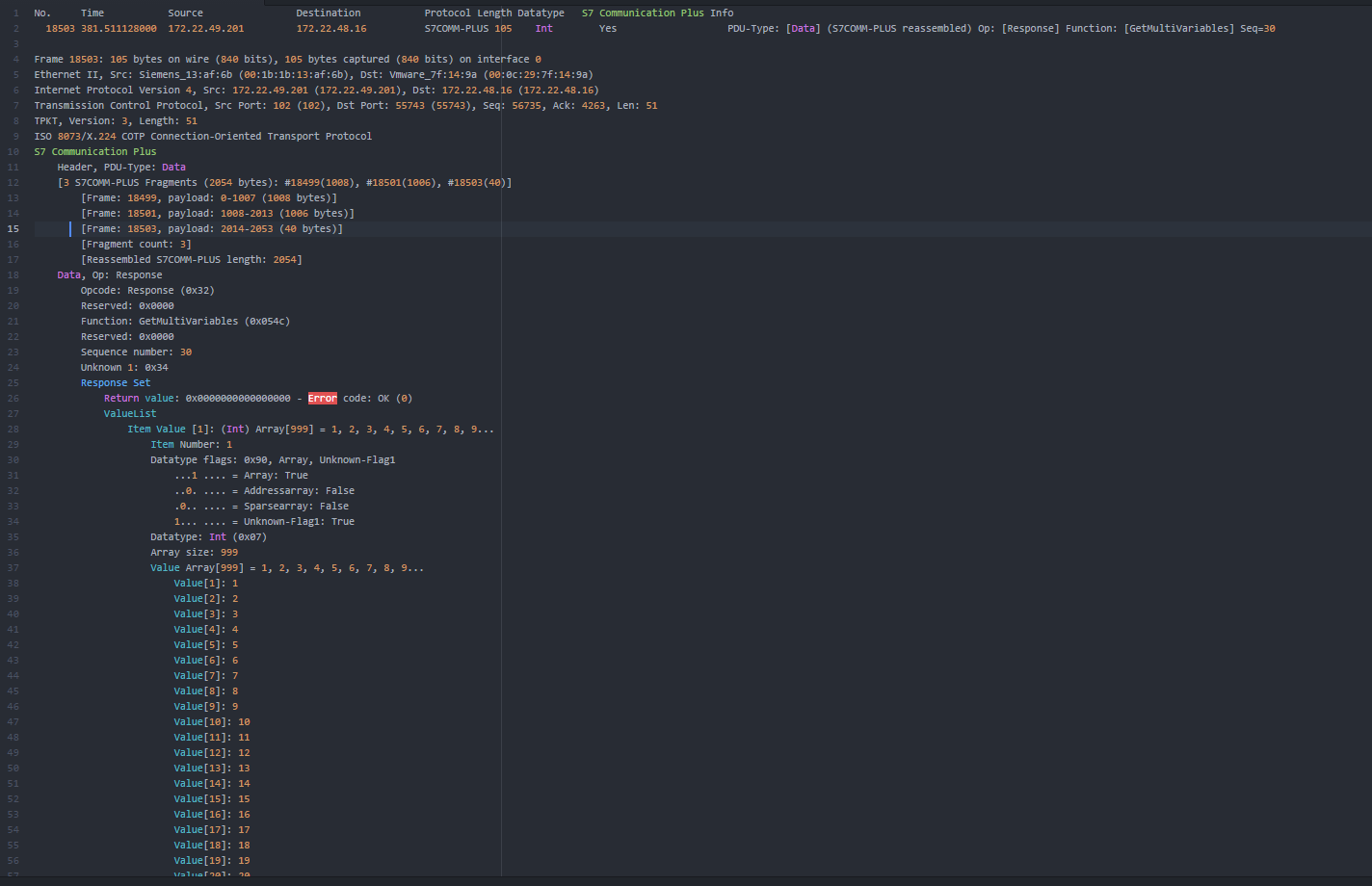
## Analyse mit dem Atom Viewer

Hier noch einen aus schnitt mit dem neuen Protokoll





Zur besseren Übersicht habe ich ein packet für den Atom Viewer erstellt mit dem Stichworte hervorgehoben werden somit kann das die Struktur besser eingesehen werden, dies sieht in etwa wie folgt aus (es ist nicht dasselbe Protokoll)



# Analyse: Array mit 999 Integer-Werten

Um ein Array mit 999 integer (int) zu übertragen wird in diesem Fall (das Array wird Komplet übertragen es beginnt mit dem Wert 1 und endet mit dem Wert 999) nur ein Telegramm Benötigt welcher aus 3 Frames besteht, die einzelnen Frames (in unserem Beispiel

[3 S7COMM-PLUS Fragments (2054 bytes): #18499(1008), #18501(1006), #18503(40)]

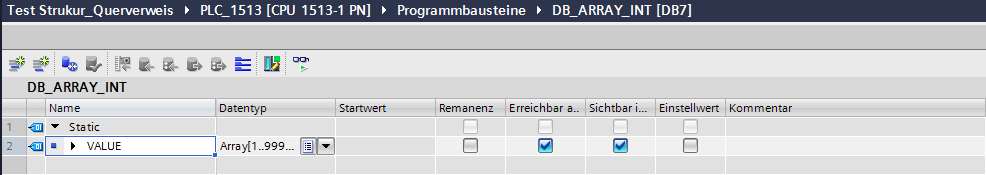
[Frame: 18499, payload: 0-1007 (1008 bytes)]

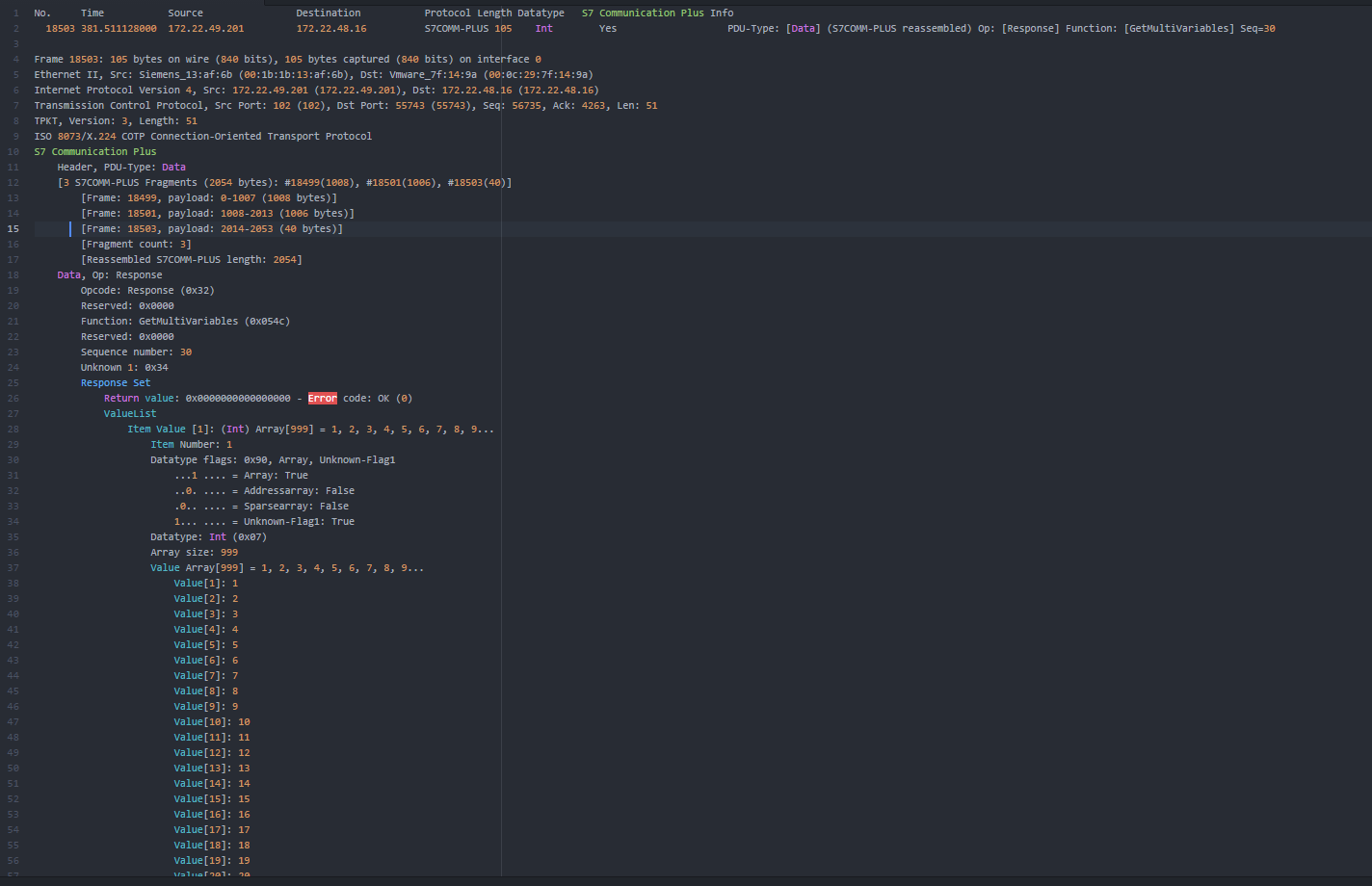
[Frame: 18501, payload: 1008-2013 (1006 bytes)]

[Frame: 18503, payload: 2014-2053 (40 bytes)]

Zur besseren Ansicht empfehle ich es das man das Ganze im Editor (Atom) anschaut es ist übersichtlicher)

Die Datei hier zu [aray(999).s7c]





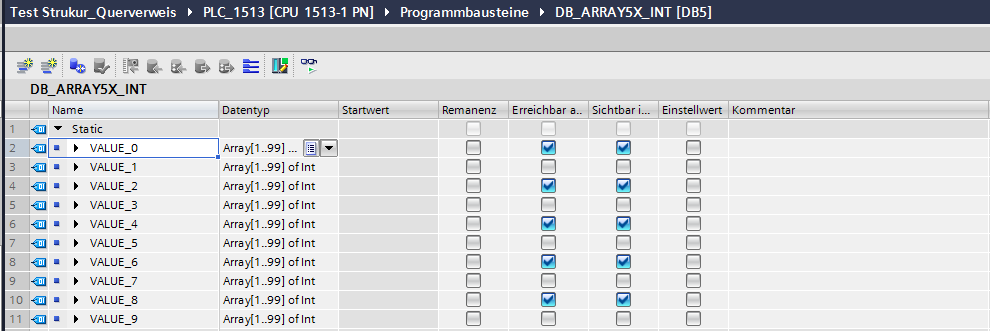
# Analyse: 10 Arrays mit je 199 Integer-Werten

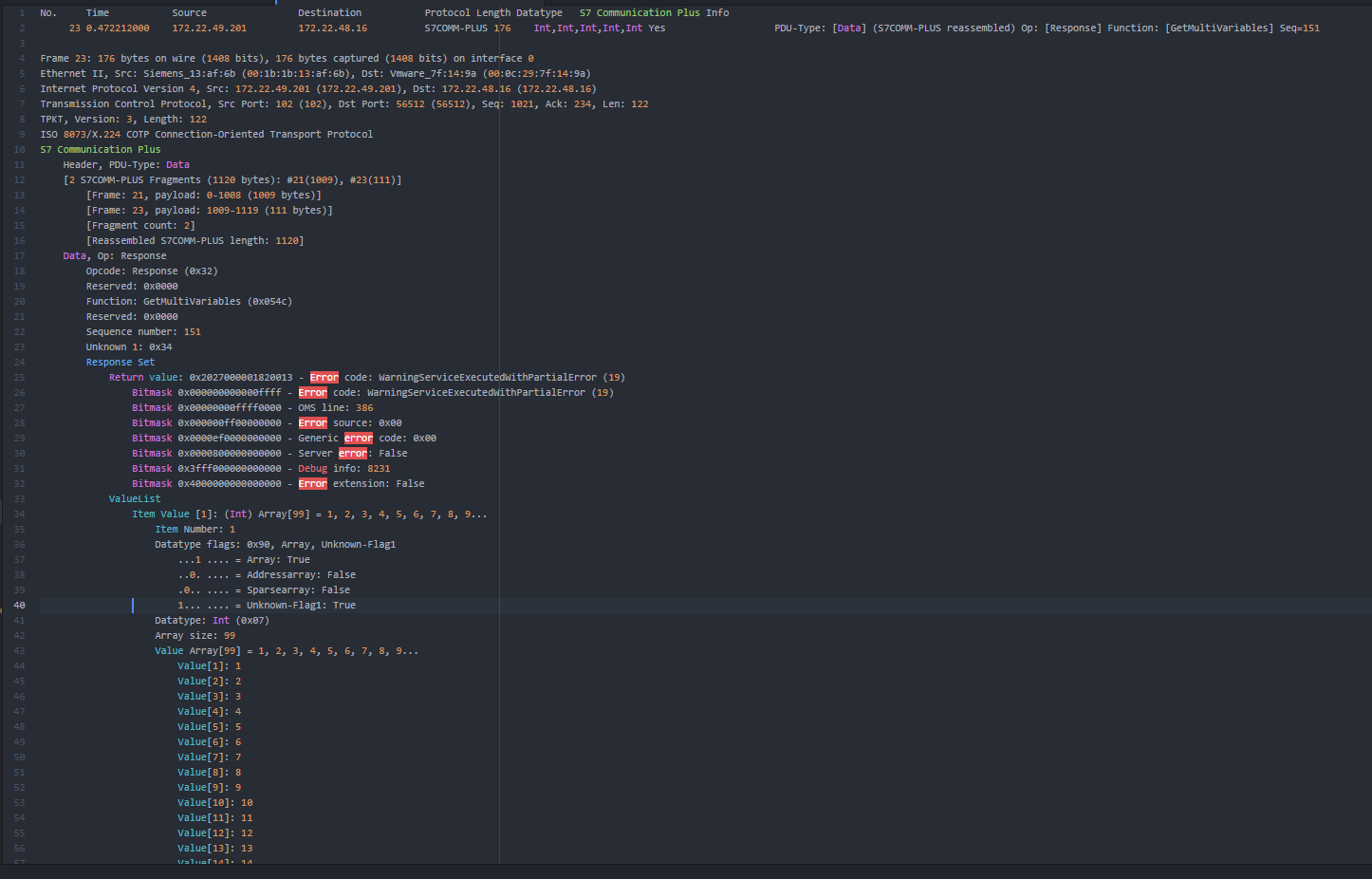
Um ein Array zu übertragen in welchem nicht alle Einträge übertragen werden sollen (in diesem Beispiel erneut ein Array mit 999 Einträgen, jedoch sollen nur die folgende Einträge übertragen werden: 1-99, 201-299, 401-499, 601-699, 801-899)

Hierfür wird erneut ein Telegramm verwendet dies ist jedoch anders strukturiert und besteht aus 2 Frames. (auch hier bitte im Editor anschauen)

Die Datei zu diesem Beispiel [array(999#0.5).s7c]

Dieser DB enthält 10 Arrays, aber nur jedes 2te Array ist als sichtbar/erreichbar markiert. Somit entstehen im DB Lücken, die nicht kommuniziert werden müssen.





# Analyse: Gemischter DB mit PLC Variablentypen

Um einen gemischten DB zu übertragen [(Beispiel in Excel Tabelle beiliegend)](file:///E:\S7-comm\DB6.xlsx) wird der DB mit den zu übertragenden werten in mehreren Telegrammen übertragen, anders als bei den obigen Beispielen sind hier mehrere Strukturen die übertragen werden, diese werden nahezu lückenlos übertragen eine Struktur wird übertragen, nach dieser kommt direkt die nächste Struktur, die Strukturen sind ziemlich durcheinander gewürfelt da der DB optimiert ist.

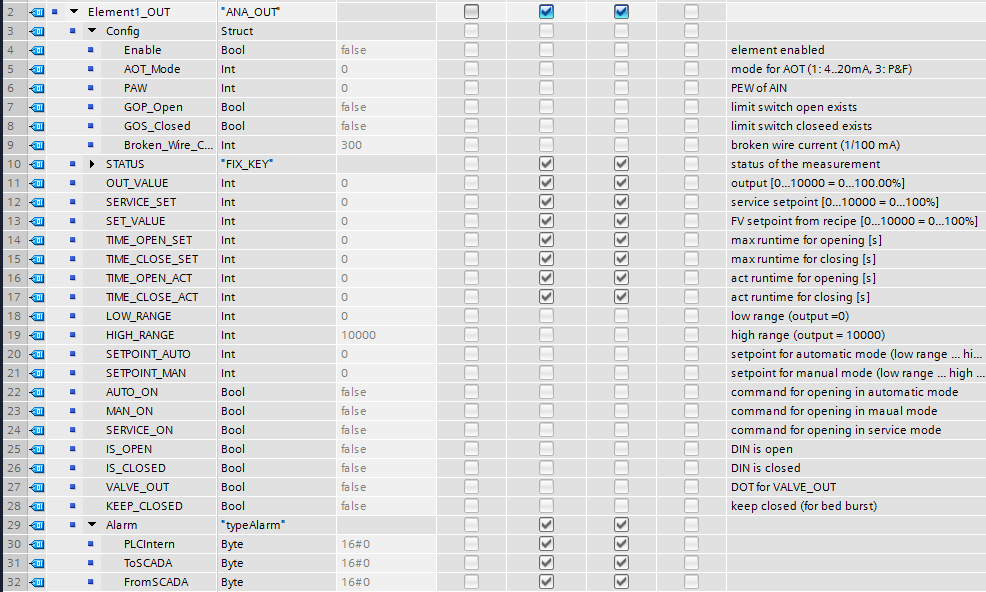
Auch hier die Beispiel Datei im Editor öffnen [DB6.s7c]

Hier eine nochmal (der 2. Durchlauf) [DB6.2.s7c]

Dieser DB enthält 7 Mal je die Struktur ANA\_OUT und ANA\_VALUE:

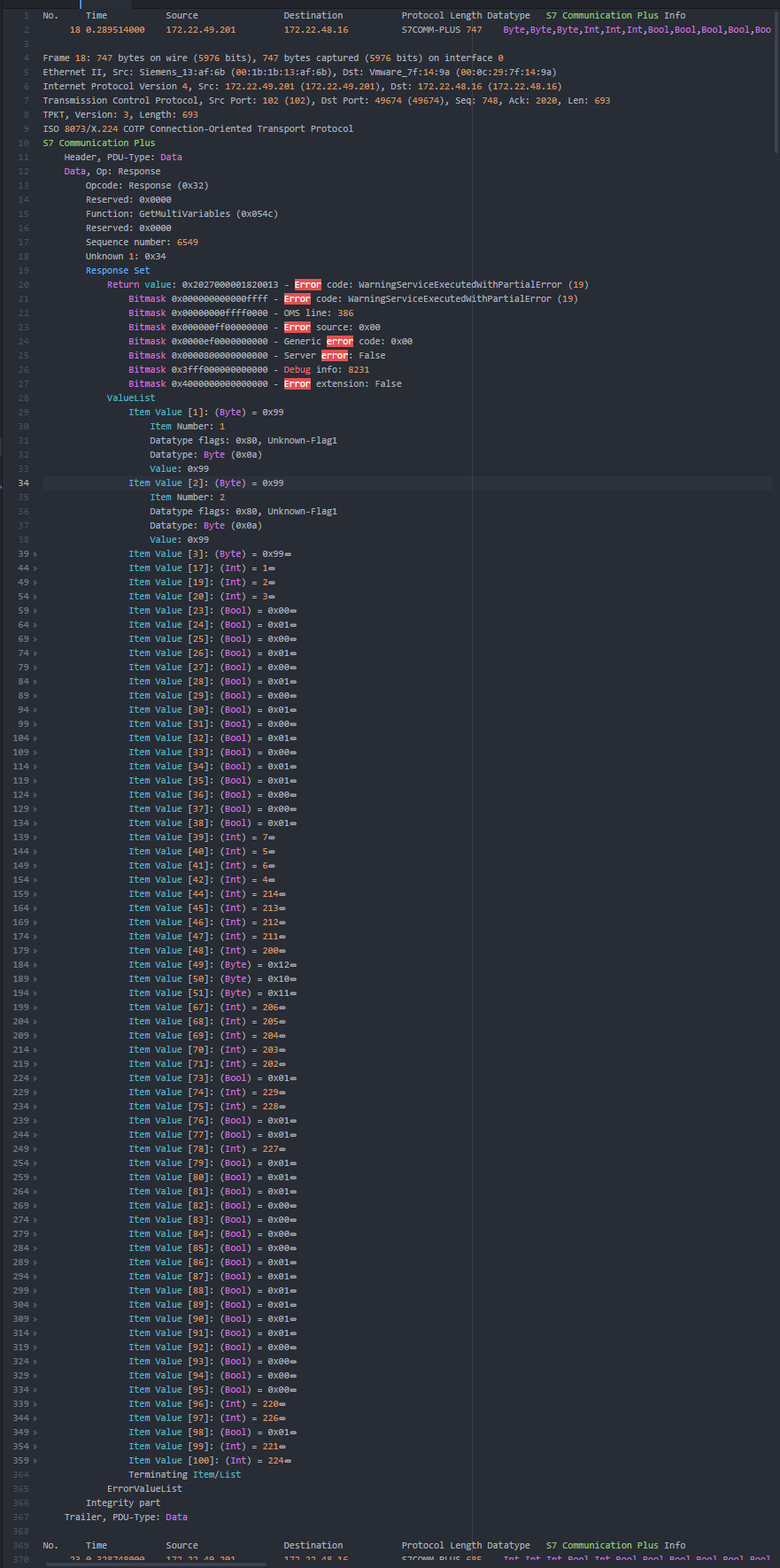


Die Daten in den PLC-Datentypen sind mehr oder weniger wild durcheinander gewürfelt:  
BOOL, INT, Byte, FIX\_KEY. Auch von Sichtbarkeit/Erreichbarkeit sind die Daten unterschiedlich konfiguriert:



Im WireShark sieht man nun, dass im Telegramm wiederum immer nur die sichtbar konfigurierten Daten übertragen werden. Es werden immer bis max. 100 Daten in einem Telegramm zusammengefasst. Die Reihenfolge dabei ist mehr oder weniger wie in der DB-Struktur definiert.

Für die insgesamt 1013 Tags werden 11 Telegramme mit total etwa 7150 byte verwendet.



# Das Endergebnis

Wenn man einen gemischten DB hat werden die zu übertragenden Werte zusammengefasst und in 100er Paketen via Telegramm verschickt so ist das Telegramm mit ca. 100 Einträgen kompakt und lückenlos, dies ist effizienter als mit dem alten Protokoll.