

## Analysis of data fields in the S7comm protocol

Experimental environment: Siemens S7-300, CUP 315-2DP, step7 5.6, wireshark

Purpose: Restore the PLC code with the captured data packet

Use wireshark to capture data transmitted by PC and PLC, including the data package with PLC code function[Download block], as shown in Figure 1.

45...	6062.89...	192.168.0.13	192.168.0.242	S7CO...	...	ROSCTR:[Job	]	Function:[Request download]	-> Block:[OB 1]
45...	6062.91...	192.168.0.242	192.168.0.13	S7CO...	...	ROSCTR:[Ack_Data]		Function:[Request download]	
45...	6062.93...	192.168.0.242	192.168.0.13	S7CO...	...	ROSCTR:[Job	]	Function:[Download block]	-> Block:[OB 1]
45...	6062.93...	192.168.0.13	192.168.0.242	S7CO...	...	ROSCTR:[Ack_Data]		Function:[Download block]	
45...	6062.97...	192.168.0.242	192.168.0.13	S7CO...	...	ROSCTR:[Job	]	Function:[Download ended]	-> Block:[OB 1]
45...	6062.98...	192.168.0.13	192.168.0.242	S7CO...	...	ROSCTR:[Ack_Data]		Function:[Download ended]	

figure 1

Open this package, after many experimental analysis, the format of the data field is roughly: 7070...0000+**xx**+0000 0000+**????** **????**+30e3...1400+**code**+6500...0100+**????**+0000 0000 0000 0000, where xx represents the length of data.

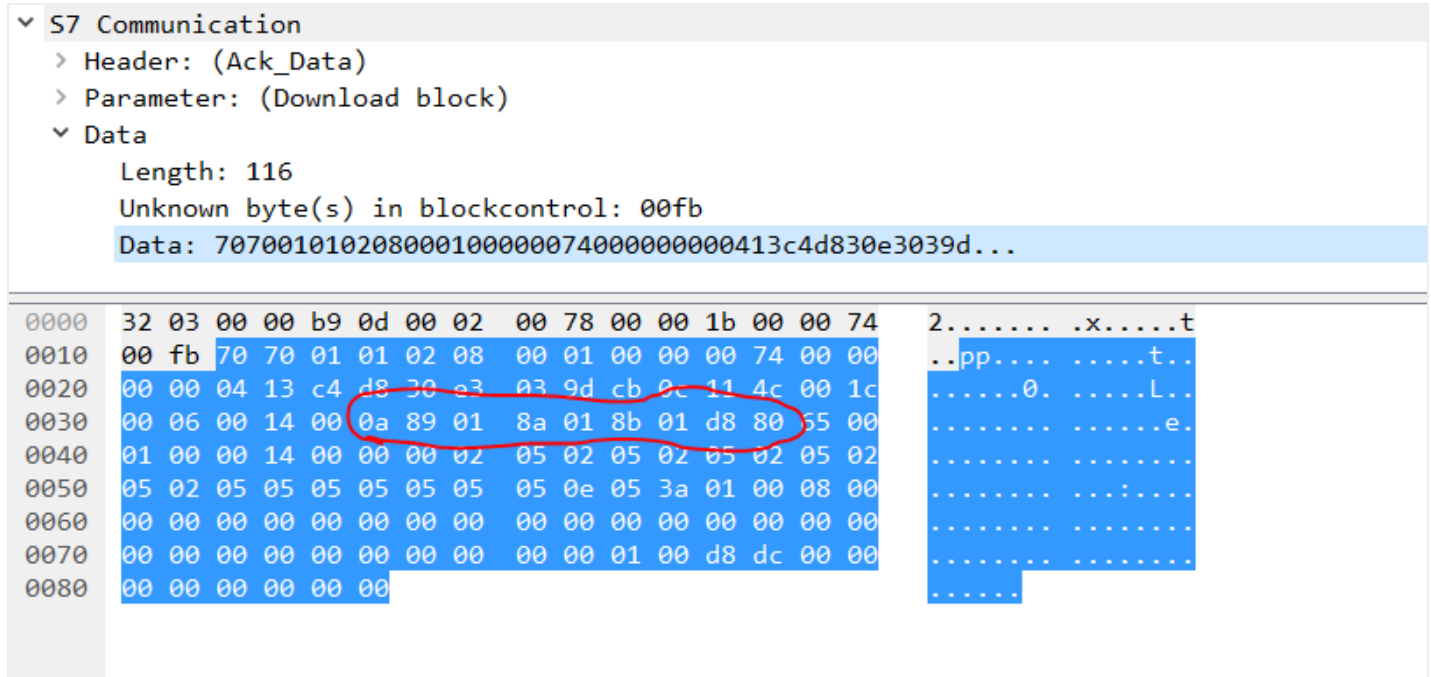


figure 2

The contents of the PLC code shown in Figure 3 in the data packet are the red part of Figure 2: 0a 89 01 8a 01 8b 01 d8 80. Many experiments have found that 0a is converted to decimal as 10, and divided by 2 and subtracted by 1 to get the instruction number 4. The latter part is two bytes for one instruction. The format is: \_ \_ \_ \_, where the last three bits represent the storage address and the first bit represents the type of operation. The size of the second digit also represents series or parallel. The current experiment shows that when the first digit is 8, the second digit is 0-7 (representative **In series with the next instruction**), the second digit is 8-F (representative **Parallel with the previous command**). Here, the series and parallel connection should also be related to the first position (operation type). At present, I have only done a simple experiment, but the principle may be like this.

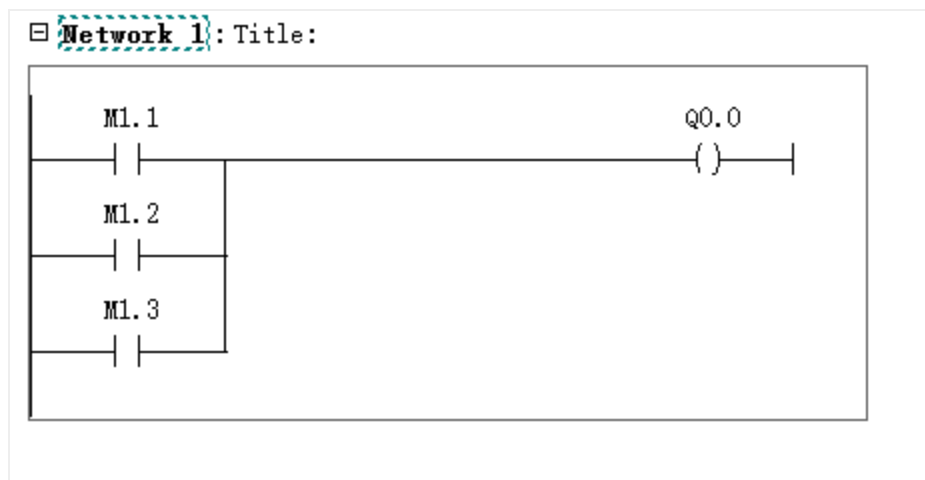


image 3

example:

data : addr opt

81 01 : M1.1 and

82 01 : M1.2 and

A1 01 : M1.1 inversion

data : opt

81 01 82 01 : M1.1 && M1.2

81 01 a2 01 : M1.1 && ^M1.2

8g 01 8a 01 : M1.1 || M1.2

The analysis method was roughly found today, and the results of the subsequent experiments will be updated one after another.



Golang tcp forwarding remoteAddr error

Intelligent Recommendation

U_ModbusSys	0	0x00000000	UINT32
U_ModbusSys	1	0x00000000	UINT32
U_ModbusSys	2	0x00000000	UINT32
U_ModbusSys	3	0x00000000	UINT32
U_ModbusSys	4	0x00000000	UINT32
U_ModbusSys	5	0x00000000	UINT32
U_ModbusSys	6	0x00000000	UINT32
U_ModbusSys	7	0x00000000	UINT32
U_ModbusSys	8	0x00000000	UINT32
U_ModbusSys	9	0x00000000	UINT32
U_ModbusSys	10	0x00000000	UINT32
U_ModbusSys	11	0x00000000	UINT32
U_ModbusSys	12	0x00000000	UINT32
U_ModbusSys	13	0x00000000	UINT32
U_ModbusSys	14	0x00000000	UINT32
U_ModbusSys	15	0x00000000	UINT32
U_ModbusSys	16	0x00000000	UINT32
U_ModbusSys	17	0x00000000	UINT32
U_ModbusSys	18	0x00000000	UINT32
U_ModbusSys	19	0x00000000	UINT32
U_ModbusSys	20	0x00000000	UINT32
U_ModbusSys	21	0x00000000	UINT32
U_ModbusSys	22	0x00000000	UINT32
U_ModbusSys	23	0x00000000	UINT32
U_ModbusSys	24	0x00000000	UINT32
U_ModbusSys	25	0x00000000	UINT32
U_ModbusSys	26	0x00000000	UINT32
U_ModbusSys	27	0x00000000	UINT32
U_ModbusSys	28	0x00000000	UINT32
U_ModbusSys	29	0x00000000	UINT32
U_ModbusSys	30	0x00000000	UINT32
U_ModbusSys	31	0x00000000	UINT32
U_ModbusSys	32	0x00000000	UINT32
U_ModbusSys	33	0x00000000	UINT32
U_ModbusSys	34	0x00000000	UINT32
U_ModbusSys	35	0x00000000	UINT32
U_ModbusSys	36	0x00000000	UINT32
U_ModbusSys	37	0x00000000	UINT32
U_ModbusSys	38	0x00000000	UINT32
U_ModbusSys	39	0x00000000	UINT32
U_ModbusSys	40	0x00000000	UINT32
U_ModbusSys	41	0x00000000	UINT32
U_ModbusSys	42	0x00000000	UINT32
U_ModbusSys	43	0x00000000	UINT32
U_ModbusSys	44	0x00000000	UINT32
U_ModbusSys	45	0x00000000	UINT32
U_ModbusSys	46	0x00000000	UINT32
U_ModbusSys	47	0x00000000	UINT32
U_ModbusSys	48	0x00000000	UINT32
U_ModbusSys	49	0x00000000	UINT32
U_ModbusSys	50	0x00000000	UINT32
U_ModbusSys	51	0x00000000	UINT32
U_ModbusSys	52	0x00000000	UINT32
U_ModbusSys	53	0x00000000	UINT32
U_ModbusSys	54	0x00000000	UINT32
U_ModbusSys	55	0x00000000	UINT32
U_ModbusSys	56	0x00000000	UINT32
U_ModbusSys	57	0x00000000	UINT32
U_ModbusSys	58	0x00000000	UINT32
U_ModbusSys	59	0x00000000	UINT32
U_ModbusSys	60	0x00000000	UINT32
U_ModbusSys	61	0x00000000	UINT32
U_ModbusSys	62	0x00000000	UINT32
U_ModbusSys	63	0x00000000	UINT32
U_ModbusSys	64	0x00000000	UINT32
U_ModbusSys	65	0x00000000	UINT32
U_ModbusSys	66	0x00000000	UINT32
U_ModbusSys	67	0x00000000	UINT32
U_ModbusSys	68	0x00000000	UINT32
U_ModbusSys	69	0x00000000	UINT32
U_ModbusSys	70	0x00000000	UINT32
U_ModbusSys	71	0x00000000	UINT32
U_ModbusSys	72	0x00000000	UINT32
U_ModbusSys	73	0x00000000	UINT32
U_ModbusSys	74	0x00000000	UINT32
U_ModbusSys	75	0x00000000	UINT32
U_ModbusSys	76	0x00000000	UINT32
U_ModbusSys	77	0x00000000	UINT32
U_ModbusSys	78	0x00000000	UINT32
U_ModbusSys	79	0x00000000	UINT32
U_ModbusSys	80	0x00000000	UINT32
U_ModbusSys	81	0x00000000	UINT32
U_ModbusSys	82	0x00000000	UINT32
U_ModbusSys	83	0x00000000	UINT32
U_ModbusSys	84	0x00000000	UINT32
U_ModbusSys	85	0x00000000	UINT32
U_ModbusSys	86	0x00000000	UINT32
U_ModbusSys	87	0x00000000	UINT32
U_ModbusSys	88	0x00000000	UINT32
U_ModbusSys	89	0x00000000	UINT32
U_ModbusSys	90	0x00000000	UINT32
U_ModbusSys	91	0x00000000	UINT32
U_ModbusSys	92	0x00000000	UINT32
U_ModbusSys	93	0x00000000	UINT32
U_ModbusSys	94	0x00000000	UINT32
U_ModbusSys	95	0x00000000	UINT32
U_ModbusSys	96	0x00000000	UINT32
U_ModbusSys	97	0x00000000	UINT32
U_ModbusSys	98	0x00000000	UINT32
U_ModbusSys	99	0x00000000	UINT32
U_ModbusSys	100	0x00000000	UINT32

Modbus protocol data analysis

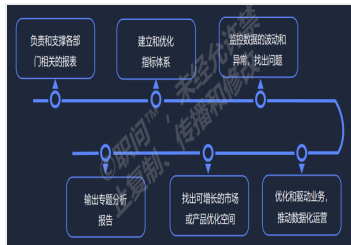
Modbus communication protocol Modbus is a serial communication protocol, which is published by Modicon (now Schneider Electric) to communicate with programmable logic controller (PLC) in 1979. MODBUS ...

Sending and analysis of protocol data

Sending and analysis of protocol data For languages such as C, C ++, we often have a variety of basic data types, such as Char, int, Float, Double, and so on. In order to review the specific data ty...

21-Data Analysis Python - pandas - add fields

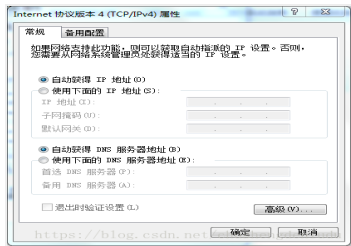
This chapter includes: Changing the time field Reprinted at:  
<https://www.jianshu.com/p/4dc6fc3a5390...>



## Module 1 Introduction to data analysis application fields

Article Directory Module 1 Introduction to data analysis application field 1. Internet 1.1 Daily work of data analysts in the Internet field 1.2 Tools for data analysts in the Internet field 1.3

Chara...

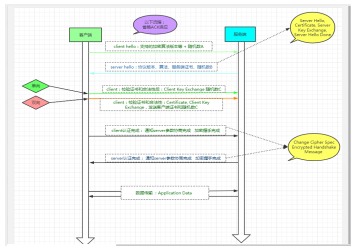


## Protocol network data capture analysis

1, first set the IP address and DNS address of the computer are set to automatically obtain status. 2, open Wireshark capture tool, double-click to open the Wi-Fi. (I use the phone hotspot) 3, the fil...

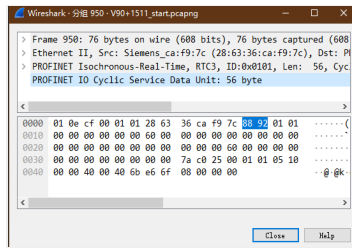
**Khu Pho Luong Binh: Click Here To See The Price Of Solar Panels**  
Solar Panels | Search Ads

## More Recommendation



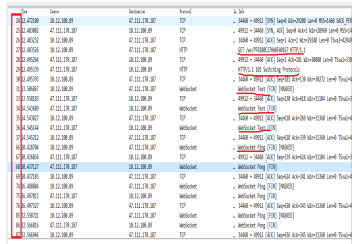
## Data and security ③Https protocol analysis

You can view the previous two articles Data and security ①Summary of encryption and decryption theory , Data and security ②HTTPS one-way and two-way authentication Those interested in ssl can have...



# Profinet protocol analysis-process data

A new article, let's talk about the next point-process data. Process data, as the name suggests, is data that has been cyclically transmitted, and is continuously transmitted throughout t...

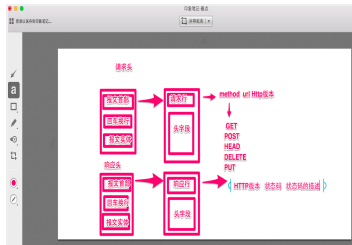


# WebSocket protocol data format analysis

Figure 1 Description: The websocket protocol is an application layer protocol based on TCP. Explain one by one according to the serial numbers expanded by red rectangles on the left of Figure 1.10.12....

# Analysis of a general network protocol data

1. Network data analysis In practical applications, network data analysis is a very common method of data processing. So is there any more common data analysis processing method? The following is a pe...



# HTTP protocol common fields

URI&URL URI: Uniform resource identifier, not only can identify http, ftp and other network resources URL: Uniform Resource Locator Request header GET: Get a resource, and the parameters directly ...

**Breathtaking Places You Should Visit Before You Die**  
BuzznFun.com

## Related Posts

- S7comm protocol analysis of the data fields (1)
- (2) Analysis of S7COMM protocol
- S7Comm Plus protocol research
- Siemens PLC protocol-S7COMM
- Siemens PLC protocol-S7COMM-extended
- S7Comm Plus protocol research dynamic debugging two
- Dynamic debugging of S7Comm Plus protocol research
- Analysis of Siemens S7comm-plus communication process and replay attack
- Robot data protocol analysis
- RTCM protocol data analysis

## Ghế sofa showroom được bán gần như miễn phí (tìm ưu đãi)

Couches & Sofa | Tìm kiếm quảng cáo  
Sponsored Links by Taboola

## Popular Posts

- Keywords: packet
- idea integrates tomcat and solves the console garbled problem
- [SOJ 639] trees
- Xiaobaixue front-end -----CSS basic grammar
- MYSQL date and time type format (detailed introduction)
- Network stream (template transfer)

- Layui jq finds the elements of the first element
- Python Algorithm Learning: Competitive Code Programming-Lanqiao Cup School Trial (Preliminary) Replay
- Freeswitch startup service script
- RISC-V's cache

### Affordable Los Angeles Auto Warranties

Auto Insurance | Search Ads

Search Now

### Xem thử bạn có nhận ra ai trong số những người nổi tiếng không tran...

BestFamilyMag

Sponsored Links by Taboola

## Recommended Posts

- Data Structures and Algorithms basis
- Front End Knowledge Sharing - SHEETJS Usage Experience
- Solve Endnote's reference to the problem without GBT7714 format



- Day04 (array)
- Mac installation git
- Image and large array types
- Convert grayscale image to pseudo-color image-pseudo-color processing
- GHOST blog build
- Android application component - Service
- Krpano tutorial - view tag Chinese description

**Find out: this is how you clean your  
yoga mat!**

Kingdom Of Men

Sponsored Links by Taboola

## Related Tags

Siemens PLC Code decompile s7comm

Industrial control

Industrial Control Protocol Series

Safety

plc

S7

socket

java

Internet of Things

The internet

Copyright **DMCA** 2018-2023 - All Rights Reserved -  
[www.programmersought.com](http://www.programmersought.com) **User Notice**