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.

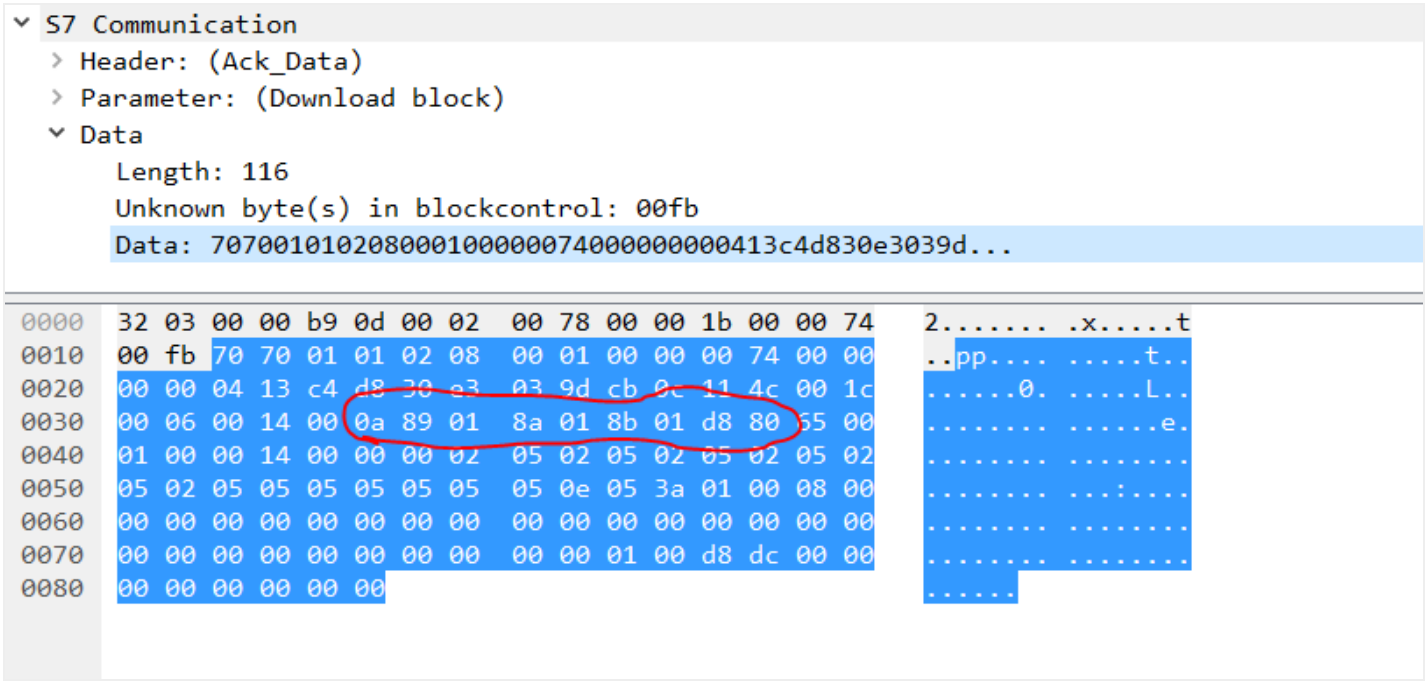


figure 2

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.

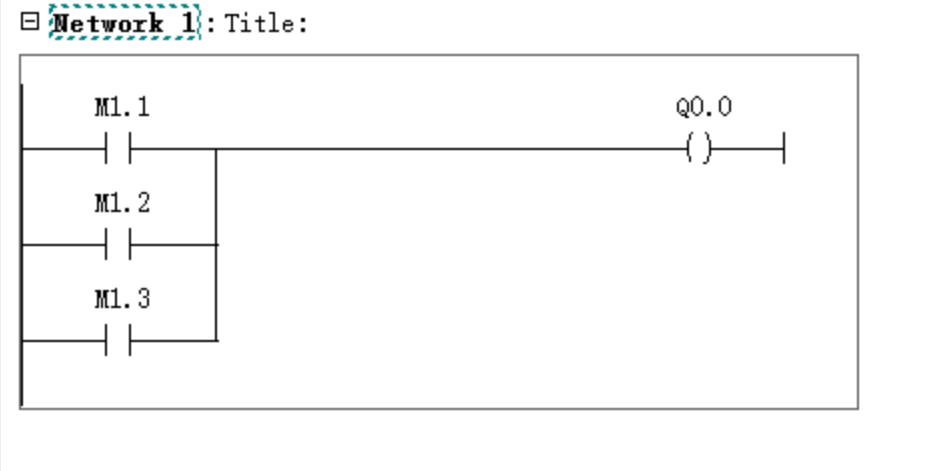


image 3

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

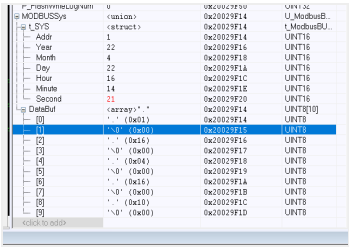
81 01 a2 01 : M1.1 && ^M1.2

89 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



Modbus protocol data analysis

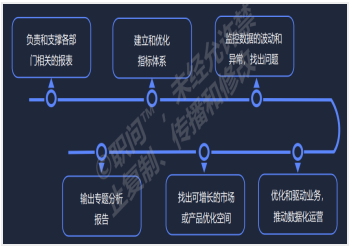
Modbus communication protocol Modbus is a serial communication protocol, which is published by Modicon (now Schneider Electric) to communicate with programmable logic controller (PLC) in 1979. MODBUS ...

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...

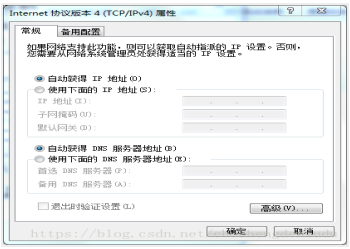
21-Data Analysis Python - pandas - add fields

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



Module 1 Introduction to data analysis application fields

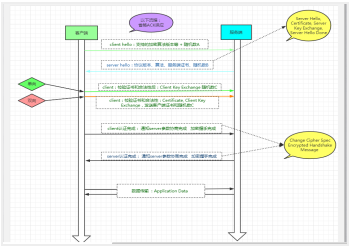
Article Directory Module 1 Introduction to data analysis application field 1. Internet 1.1 Daily work of data analysts in the Internet field 1.2 Tools for data analysts in the Internet field 1.3 Chara...



Protocol network data capture analysis

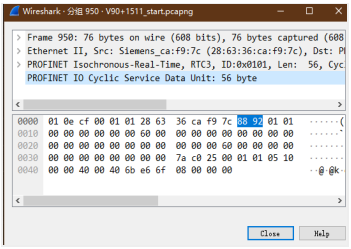
1, first set the IP address and DNS address of the computer are set to automatically obtain status. 2, open Wireshark capture tool, double-click to open the Wi-Fi. (I use the phone hotspot) 3, the fil...

More Recommendation



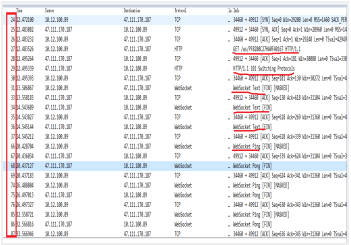
Data and security ③Https protocol analysis

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...

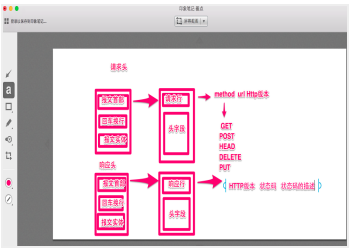


WebSocket protocol data format analysis

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 ...

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

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
- RISCV's cache

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

Related Tags

Siemens PLC Code decompile s7comm

Industrial control

Industrial Control Protocol Series

Safety

plc

S7

socket

java

Internet of Things

The internet