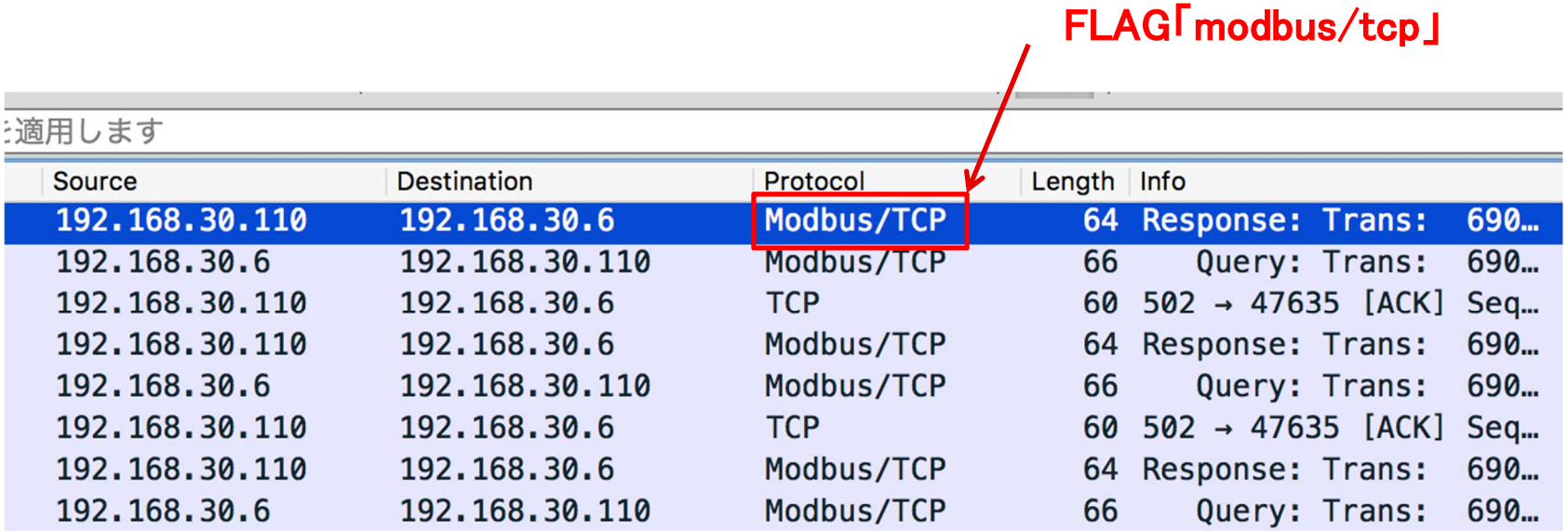
問題解説 OT/IoT

平成30年11月10日

仙台CTF推進プロジェクト
目黒　有輝
戸羽　秀人

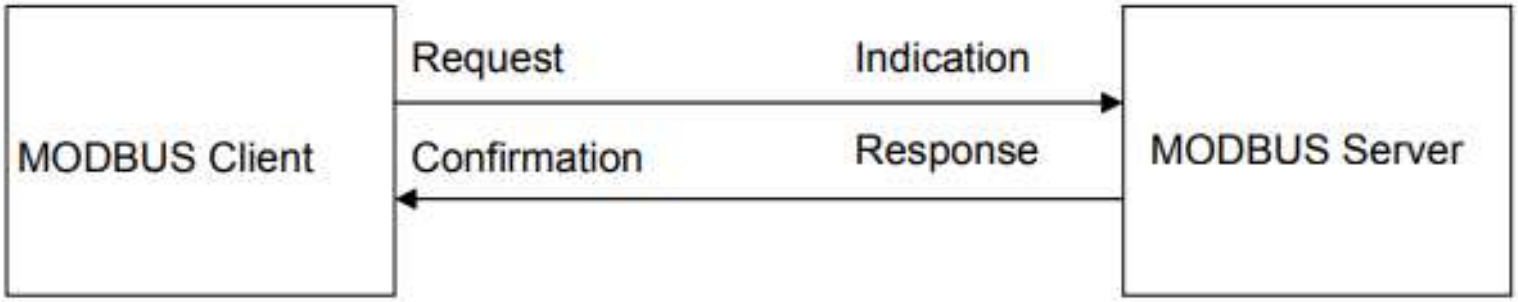
Q1. HMIとPLC間の制御プロトコルを特定して下さい

- sshでEWSにログインし、tcpdumpでパケットをスニフ。pcap形式で保存。
- pcapファイルをscp等でコピーした後、Wiresharkで開いてプロトコルを確認。



（参考）Modbut/TCPとは

- Modbusとは米Modicon社により開発された、PLC用のネットワークプロトコル。
- 仕様は公開されており、制御システムで汎用的に採用されている。

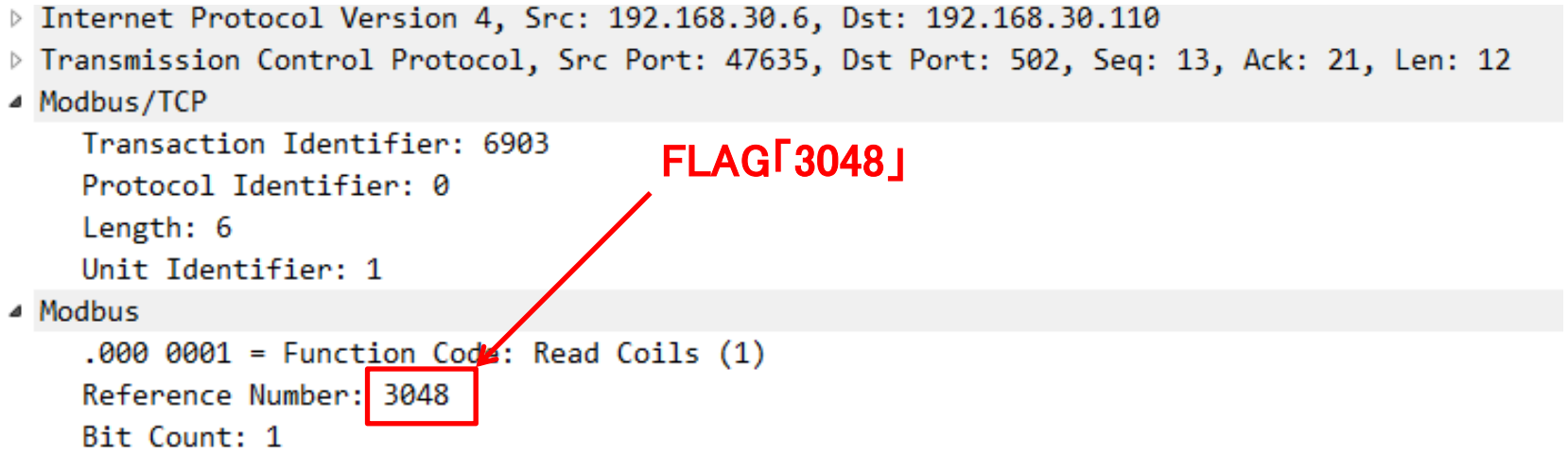


http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

Q2. 照明機能を制御するためのPLCレジスタを特定して下さい

- Modbus/TCPプロトコルのパケットを観察すると、1種類のレジスタに対して連続的にRead命令が行われていることが分かる。

- QueryのReference Numberを確認する。



Q3. 照明機能を復旧させ、復旧させた様子を監視カメラで確認して下さい

- ヒントファイルを参考に、Pythonで簡易Modbusクライアントを作成。
- 宛先IPアドレスはPLC、宛先ポート番号は502番、ペイロード部分には、Write Single Coilのパケット（Q2のヒントファイルに記載されていたペイロード）を転記。
- 作成したPythonプログラムを実行させると照明が3秒間点灯し、明るくなったことで監視カメラ越しに見えたQRコードを読み込むとフラグが確認できる。

```
import socket

client = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
client.connect(("192.168.30.110", 502))
client.send(b"\x00\x03\x00\x00\x00\x06\x01\x05\x0b\xe8\xff\x00")
modbus_client.py (END)
```

FLAG「OK_GOOGLE_DENKI_WO_TSUKETE」