


# 工控CTF之协议分析4——MQTT

原创Shadow、S于 2022-12-20 21:14:49 发布679收藏 2

分类专栏:CTF刷题工控文章标签:安全网络协议

版权

CTF刷题同时被 2 个专栏收录

8 订阅27 篇文章

订阅专栏

## 协议分析

### 流量分析

主要以工控流量和恶意流量为主，难度较低的题目主要考察Wireshark使用和找规律，难度较高的题目主要考察协议定义和特征

简单只能简单得千篇一律，难可以难得五花八门

常见的工控协议有：Modbus、MMS、IEC60870、MQTT、CoAP、COTP、IEC104、IEC61850、S7comm、OMRON等

由于工控技术起步较早但是统一的协议规范制定较晚，所以许多工业设备都有自己的协议，网上资料数量视其设备普及程度而定，还有部分协议为国家制定，但仅在自己国内使用，网上资料数量视其影响力而定

## CTF之协议分析文章合集

- 工控CTF之协议分析1——Modbus
- 工控CTF之协议分析2——MMS
- 工控CTF之协议分析3——IEC60870
- 工控CTF之协议分析4——MQTT
- 工控CTF之协议分析5——COTP
- 工控CTF之协议分析6——s7comm
- 工控CTF之协议分析7——OMRON
- 工控CTF之协议分析8——特殊隧道
- 工控CTF之协议分析9——其他协议

### 文中题目链接如下

站内下载

网盘下载：<https://pan.baidu.com/s/1vWowLRkd0ldvL8GoMxG-tA?pwd=jkkq>

提取码：jkkq

## MQTT

主要数据交互的消息类型为PUBLISH

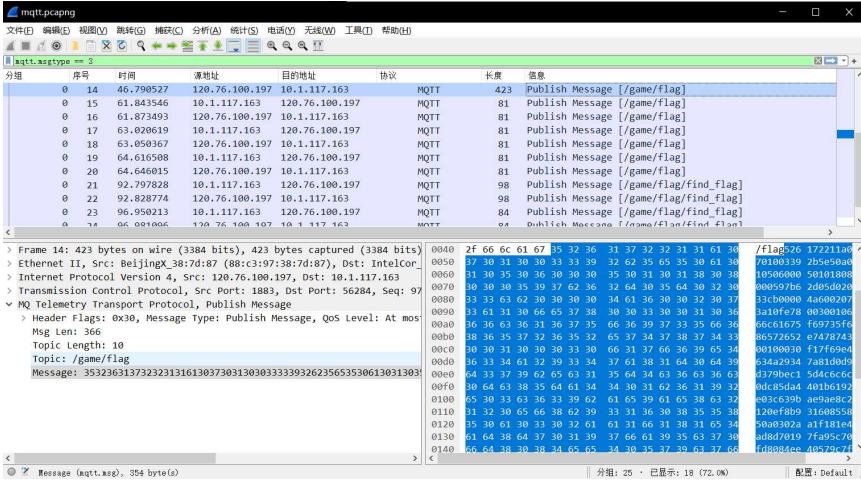
筛选mqtt.msgtype == 3

服务端有若干个主题（topic）可供客户端订阅，客户端订阅后可以收到来自服务端关于这个主题的消息（message），一个主题可以持续产生消息

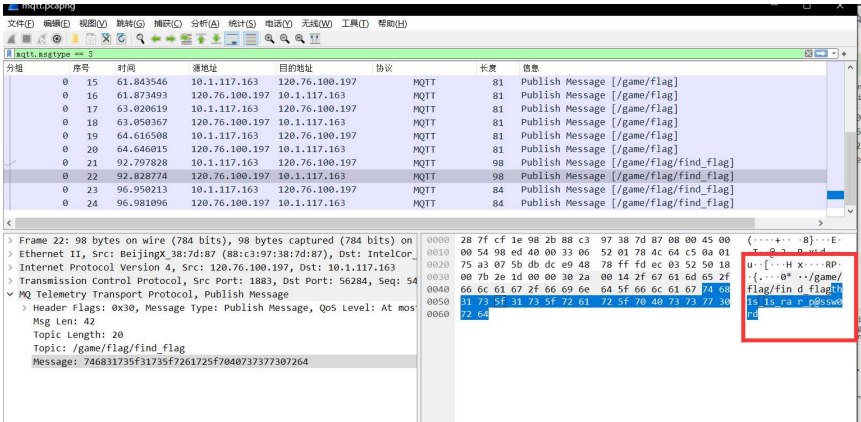
### 例题1 Simple MQTT

打开题目 发现基本都是mqtt协议，直接筛选mqtt.msgtype == 3

在一堆where is flag后发现一大串16进制，解得一个rar压缩包，密码同样在后面找到，解压得到flag



压缩包密码

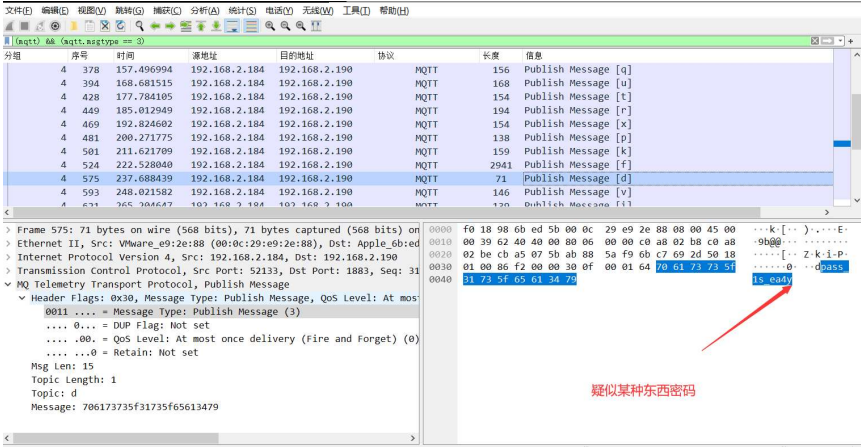


例题2 2020ICSC济南站—工业物联网智能网关数据分析

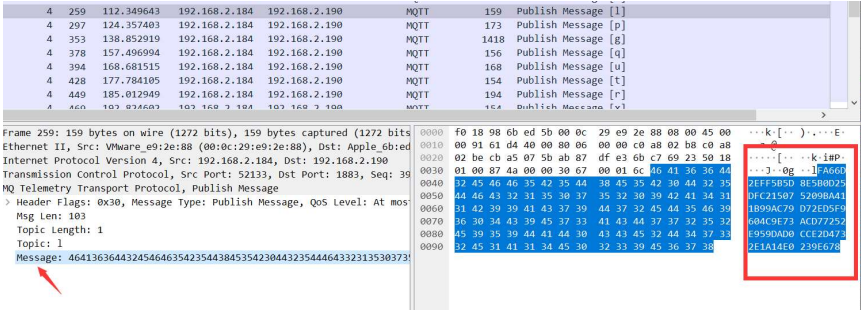
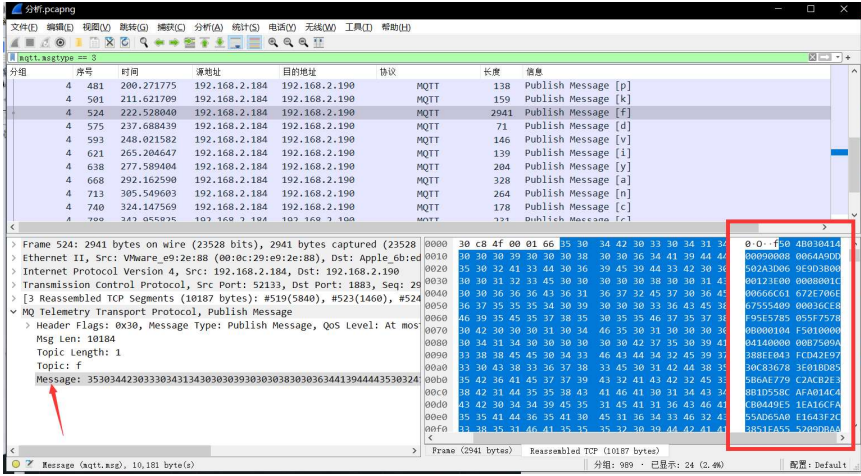
先看协议分级，发现大多与工控没有关系，mqtt占比一般，但是数据量大

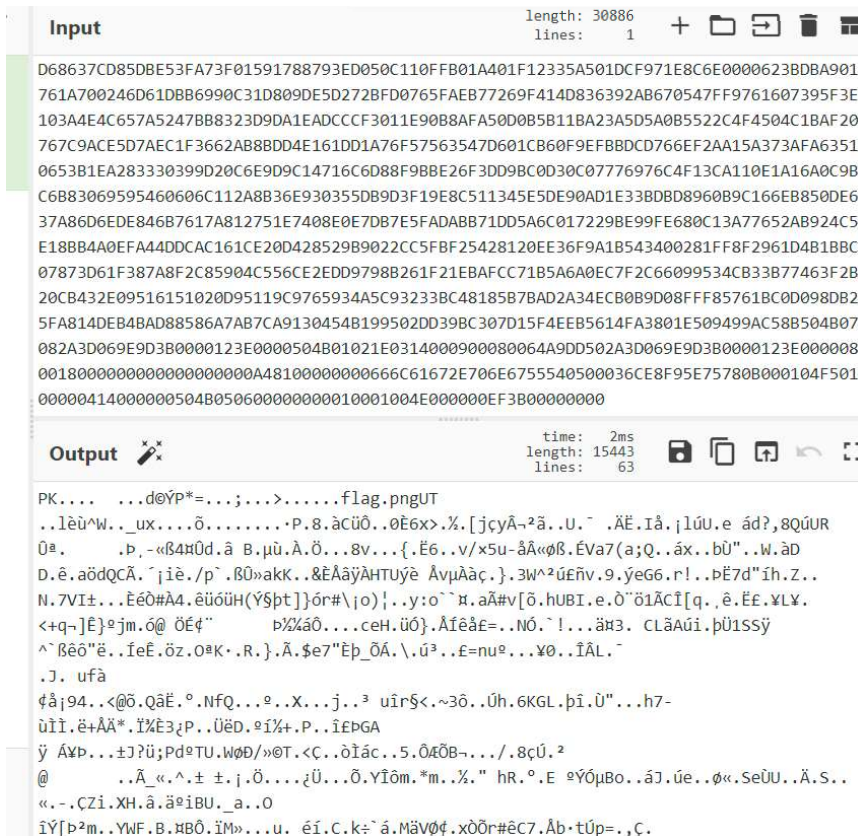
老规矩，直接看mqtt的publish

大致看一遍数据包，发现疑似密码



小技巧 密码一般在加密文件之后出现，从这条数据往上找，发现以f为主题（topic）的数据包是zip压缩包的头部，但是压缩包不完整，又发现只有flag的主题中16进制为大写字母，猜测以分别flag为topic的数据包拼接后得到完整压缩包



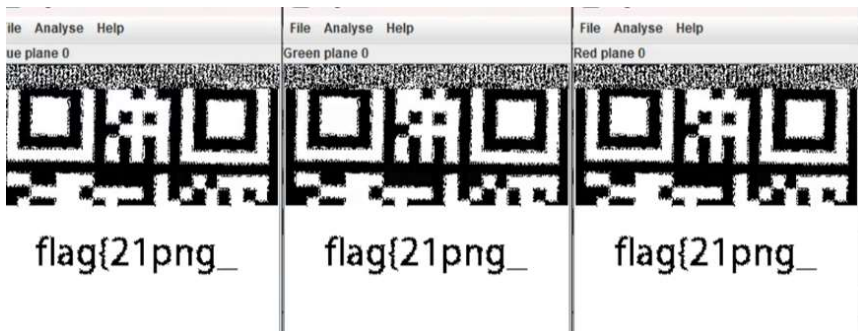


保存为zip后，用之前获取的密码解压得到半张二维码，猜测图片隐写，用010打开，果然报错，高度错误，修改高度后得到半个flag



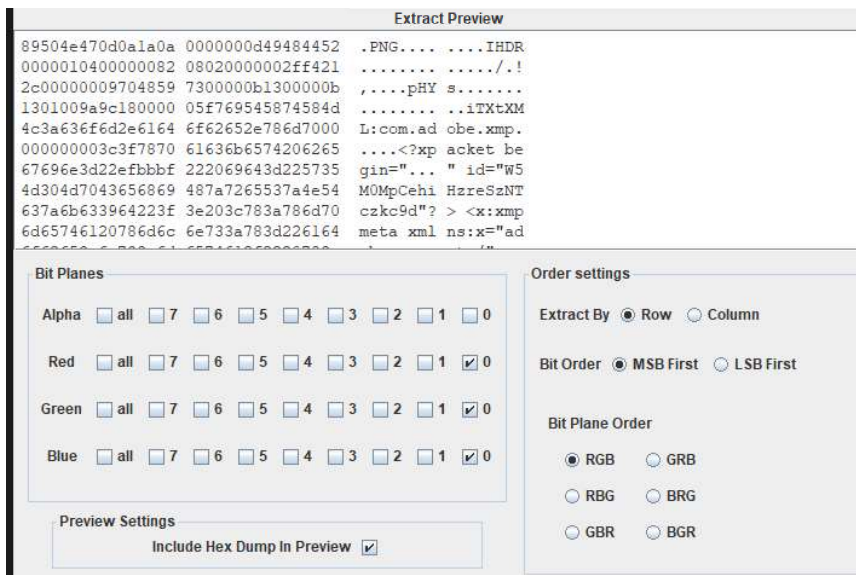
flag{21png\_

用stegsolve打开，发现分别在R0, G0, B0通道图片上半部分有异常，可能存在LSB隐写



根据提示处理通道R0, G0, B0, 得到下半部分二维码





将两部分二维码拼接扫描得到另一半flag



文章知识点与官方知识档案匹配，可进一步学习相关知识

网络技能树 支撑应用程序的协议 应用层的作用 35917 人正在系统学习中

	<a href="#">mqtt通信协议实现代码</a> 使用Python语言实现 <a href="#">mqtt协议</a> ，完成数据的发布于订阅功能	05-31
	<a href="#">MQTT协议应用TLS</a>	qq_41381461的博文 7099
	<p>前言 做了很久的实验，一直没能成功，最后还是down的大佬的源码，侵删。正文 简介 <a href="#">MQTT协议是...</a></p> <p>book_scanner:使用书籍扫描仪的简单程序_图书扫码枪怎样录入图书...</p> <p>ha_nfc_scanner:使用<a href="#">MQTT</a>操作将NFC标签卡扫描到家庭助理 etp.zip_Scanner_java调用扫描仪_扫描...</p>	7-21
	<a href="#">Android 手把手带你玩转自定义相机 - 一口仁馍 - 博客频道 - CSDN...</a>	10-19
	<a href="#">qq_17250009: @q1454739828:自己用MQTT实现推送或者IM比较复杂且难度较大,好处是灵活,可定制...</a>	
	<a href="#">2020工业控制安全大赛试题.zip</a>	09-12
	<a href="#">"中能融合杯"第六届全国工控系统信息安全攻防竞赛于9月12日上午9: 00准时开赛, 工控系统...</a>	
	<a href="#">工控CTF协议分析学习题目合集</a>	12-20
	<a href="#">主页工控CTF学习配套题目, 搭配学习</a>	
	<a href="#">【系列连载2】RT-Thread Smart和树莓派:wget &amp; cURL网络客户端_RT-Thr...</a>	7-14
	<a href="#">本次培训RT-Thread将以ART-Pi为硬件平台+RT-Thread物联网操作系统提供MQTT网关原型,希望帮助...</a>	
	<a href="#">2021CTF工业信息安全大赛第一场题.rar</a>	07-02
	<a href="#">2021CTF工业信息安全大赛第一场题.rar</a>	

## 一道MMS工控协议CTF题的WriteUp



## Shadow、S

关注

0 2

0x01 赛题说明 赛题说明： 只能变电站通过 61850 规约进行监控层到间隔层的数据采集，请分析网络...

Bugku -simple MQTT 【MISC】 soysauce123的博客 363  
看到这里提示可以翻译为 this is rar passwork那么就显而易见我们要找到一个rar或者是rar的十六进制...

MQTT介绍及与其他协议的比较 lomman\_q的博客 3760  
MQTT (Message Queuing Telemetry Transport，消息队列遥测传输) 一种针对移动终端设备的基于...

MQTT采集协议转换器转103 104 cdt 61850动环工业网关可定... YEYUANGEN的专栏 993  
信迈科技工业网关，支持多种协议转换，不同软硬件配置，可支持定制。硬件配置：AM335X/IMX6U...

工控CTF之协议分析2——MMS song123sh的博客 1035  
工控CTF之协议分析2——MMS

CTF之二维码扫描.7z 12-02  
CTF入门之二维码扫描神器，支持二维码修复

app下载H5页面.zip\_APP\_H5 app\_height63k\_triangleloc\_下载APP H5页面 09-20  
app引导页，界面超级好看，以后有好的回来上传

从CTF到工控安全.pdf 02-26  
从CTF到工控安全.pdf

pybas-master.zip 04-04  
天牛须算法的python版本，可以安装使用，里面有两个demo可以运行，类似于贪心算法，具有...

2022工业互联网大赛-杭州-CTF题目 09-14  
第一次参加工控类的CTF，然后正好团队中有一个小伙伴电脑连不上局域网，只能从我电脑中...

一道MMS工控协议CTF题的WriteUp-附件资源 03-02  
一道MMS工控协议CTF题的WriteUp-附件资源

阿里第一代 android dex加固的脱壳方法 coc\_k的博客 8620  
测试程序 链接：http://pan.baidu.com/s/1cMGmF8 密码：8xgn脱壳环境： Android 4.2、dalvik模式、...

ctf中常用的PHP伪协议 最新发布 02-15  
在CTF比赛中，常常会使用PHP伪协议来绕过服务器的安全限制或者执行本不应该执行的操作。PHP...

“相关推荐”对你有帮助么？

非常没帮助 没帮助 一般 有帮助 非常有帮助

关于我们 招贤纳士 商务合作 寻求报道 400-660-0108 kefu@csdn.net 在线客服 工作时间 8:30-22:00

公安备案号11010502030143 京ICP备19004658号 京网文〔2020〕1039-165号 经营性网站备案信息  
北京互联网违法和不良信息举报中心 家长监护 网络110报警服务 中国互联网举报中心 Chrome商店下载 账号管理规范  
版权与免责声明 版权申诉 出版物许可证 营业执照 ©1999-2023北京创新乐知网络技术有限公司

Shadow丶S

码龄4年 高校学生

126

4万+

2万+

25万+

原创

周排名

总排名

访问

等级

1830

202

306

48

1675

积分

粉丝

获赞

评论

收藏

私信

关注

搜博主文章

热门文章

Shadow丶S 关注

0 2

ACL原理及配置 14442

eNSP下载安装超详细，华为模拟器下载安装 11328

域——windows服务器域详解 8888

分类专栏

	CTF刷题	27篇
	工控	9篇
	渗透测试	55篇
	逆向分析	1篇
	网络安全	46篇
	计算机网络	16篇

最新评论

【计算机网络】IP地址详解  
大口喝咖啡: 应该是本地地址吧  
华为模拟器eNSP免费下载  
指尖上的圍春: 链接挂了  
域——windows服务器域详解  
Shadow、S: 什么参数，具体点  
域——windows服务器域详解  
sweet-琉璃: 参数不正确怎么办呢?  
华为模拟器eNSP免费下载  
打码不打你: 文件没了

最新文章

LitCTF2023 WP  
工控CTF之协议分析7——OMRON  
工控CTF之协议分析6——s7comm

2023年 1篇      2022年 91篇  
2021年 34篇

目录

协议分析

- CTF之协议分析文章合集
- MQTT
  - 例题1 Simple MQTT
  - 例题2 2020ICSC济南站—工业物...