

# [工控CTF]2021工业信息安全技能大赛（江西站）-WP

原创

3tefanie、zhou 于 2021-09-30 14:43:14 发布 1711 收藏 5

文章标签：[网络安全](#)

版权声明：本文为博主原创文章，遵循[CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：<https://blog.csdn.net/luochen2436/article/details/120561075>

版权

## 文章目录

[西门子S7协议](#)

[文件分析](#)

[异常流量分析](#)

[应急恢复](#)

[恶意app分析](#)

[工控流量分析](#)

[丢失的密码](#)

[工业固件分析](#)

[opc流量分析](#)

## 西门子S7协议

0300002402f080320100000003000e00050501120a10020001000083000000004000801。请解读以上协议内容，并准确的拿到此报文返回值，flag即为返回值。提交格式：flag{xxx}。

查找西门子S7协议资料，发现是一个写操作，根据其报文格式，获拼接出回复报文

写demo3:

1200 写入: output0=4

PC发出报文分析:

(A[3]~A[4]=0x0024=36=读取报文总长度, A[12]A[13]=0x0008=序列号, A[16]A[17]=0x05=写入byte个数(1)+4, A[23]=0x02=写入方式为byte, A[24]~A[25]=0x0001=1=写入个数count; A[26]A[27]=0x0001=DB1(因为是output,所以DB块编号无所谓), A[28]=0x82=写入的数据类型为output, A[29]A[31]=0x000000=读取偏移量offset( bit为单位)A[32]~A[33]=0x0004=写入方式为byte, A[34]~A[35]=0x0008=1\*8=写入byte的个数, A[36]= 写入数据)

03 00 00 24 02 F0 80 32 01 00 00 00 08 00 0E 00 05 05 01 12 0A 10 02 00 01 00 01 82 00 00 00 04 00 08 04

PLC回复报文分析:

( B[12]~B[13]=0x0565=序列号, 最后一个B[14]=0xFF表示写入)

03 00 00 16 02 F0 80 32 03 00 00 00 08 00 02 00 01 00 00 05 01 FF

写报文:

```
03 00 00 24 02 F0 80 32 01 00 00 00 03 00 0e 00 05 05 01 12 0a 10 02 00 01 00 00 83 00 00 00 00 04 00 08 01
```

回复报文:

```
03 00 00 16 02 F0 80 32 03 00 00 00 03 00 02 00 01 00 00 05 01 FF
```

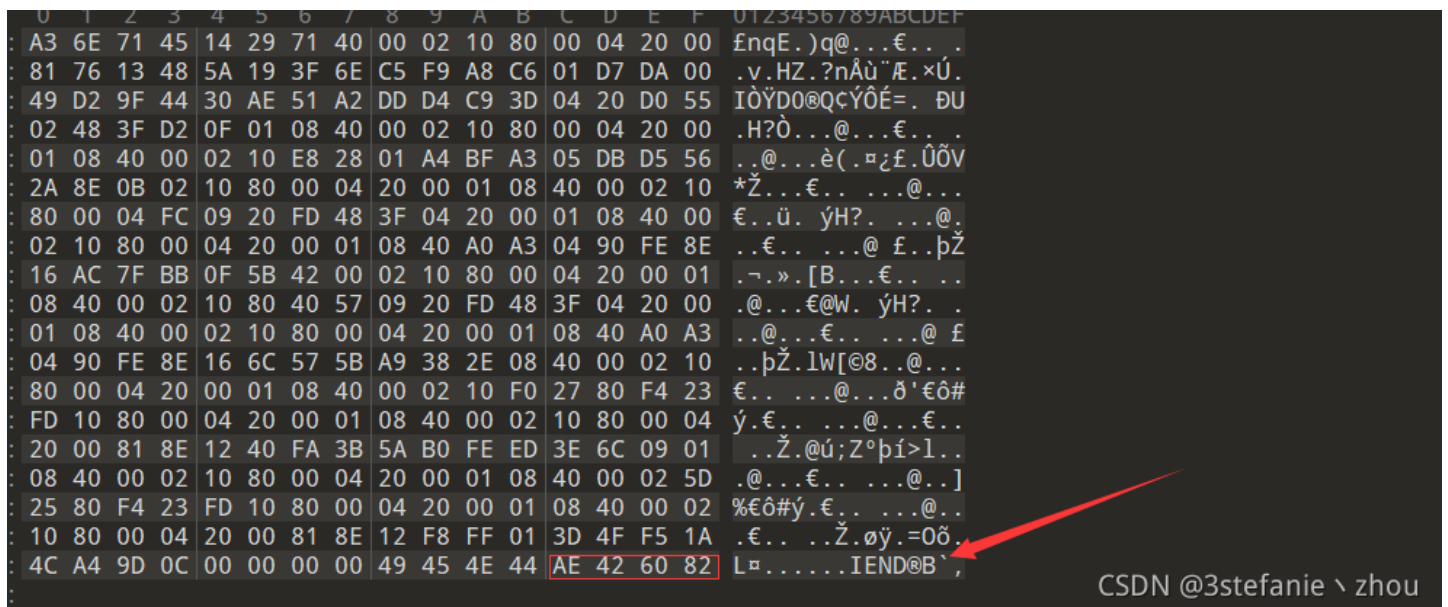
根据题目要求, 回复报文作为flag

```
flag{0300001602f0803203000000030002000100000501ff}
```

## 文件分析

hint:这是工艺监控流程文件被人破坏, 写入了某些特别的内容, 请根据文件, 找出其中的flag。提交格式: flag{xxx}。

解压文件, 得到一个没有后缀名的文件, 丢进 010 editor中查看



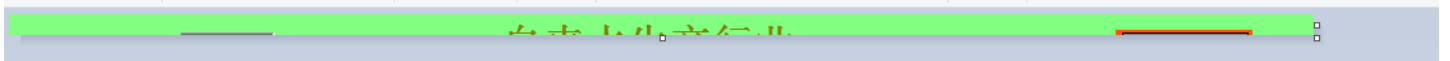
在文件尾出发现 AE 42 60 82,得知是一张图片, 这是png的文件尾格式  
但是缺失文件头, 补上

```

89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
00 00 03 FD 00 00 04 AB 08 06 00 00 00 17 96 D7 ...ý...-x
41 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 A....sRGB.@Î.é..
00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA..±..üa...
00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7 ..pHYs...Û...Û.Ç
6F A8 64 00 00 DC A5 49 44 41 54 78 5E ED BD 0D o`d..Û¥IDATx^í½.
F0 55 D5 7D A8 CD 6D 7A D3 A4 93 1B FB F1 D6 DB ðUÜ}”ÍmzÓ”“úňŎŮ
B4 62 FB 8E 4D 9A 26 D1 E9 5B 92 B9 5E 6F CC FB ‘bûZMš&Né[’^oÏû
4E 6B 2D 6F 12 A7 49 AF F7 B6 4D E8 9D 0C F5 05 Nk-o.šI÷¶Mè..ö.
41 44 09 05 09 12 45 87 82 14 B9 22 21 20 84 10 AD....E‡,..!"...
94 52 11 4D 50 4B 09 91 52 F1 AB 51 8B C4 94 72 "R.MPK.'Rň«Q«Ä”r
FD 20 69 A4 64 12 6F 6D 32 69 66 D2 4E 6F EF CC ý i=d.om2ifŎNoiÏ
EF 3D BF 7D CE 3A 67 9D 7D F6 DE 6B ED EF 8F F3 ĩ=z}Î:g.}öPkiĭ.ó
A0 6B FE FF FF 39 7B AF B5 F6 B3 D6 FE 78 D6 D7 kpyÿ9{µö³ŎpxŎx
9E B1 5A F8 0F 02 10 80 00 04 20 00 01 08 40 00 ž±Zø...€...@.
02 10 80 00 04 20 00 81 2E 12 98 D1 C5 83 E2 98 ..€...~ŇÄfâ~
20 00 01 08 40 00 02 10 80 00 04 20 00 01 08 40 ...@...€...@
00 02 10 58 2D 48 3F 23 1D 20 00 01 08 40 00 02 ...X-H?#. ...@..
10 80 00 04 20 00 01 08 40 00 02 1D 25 80 F4 77 .€...@...%€ôw
B4 60 69 D1 82 00 04 20 00 01 08 40 00 02 10 80 ‘iŇ,.. ...@...€
00 04 20 00 01 08 20 FD 48 3F 04 20 00 01 08 40 ... ýH?...@
00 02 10 80 00 04 20 00 01 08 40 A0 A3 04 90 FE ...€...@ £..p
8E 16 2C ED 59 10 80 00 04 20 00 01 08 40 00 02 Ž.,iY.€...@..
10 80 00 04 20 00 01 A4 1F E9 87 00 04 20 00 01 .€...µ.é‡...
08 40 00 02 10 80 00 04 20 00 01 08 74 94 00 D2 .@...€...t”Ŏ
DF D1 82 A5 3D 0B 02 10 80 00 04 20 00 01 08 40 RŇ ¥= €
CSDN @3stefanie \ zhou

```

打开图片



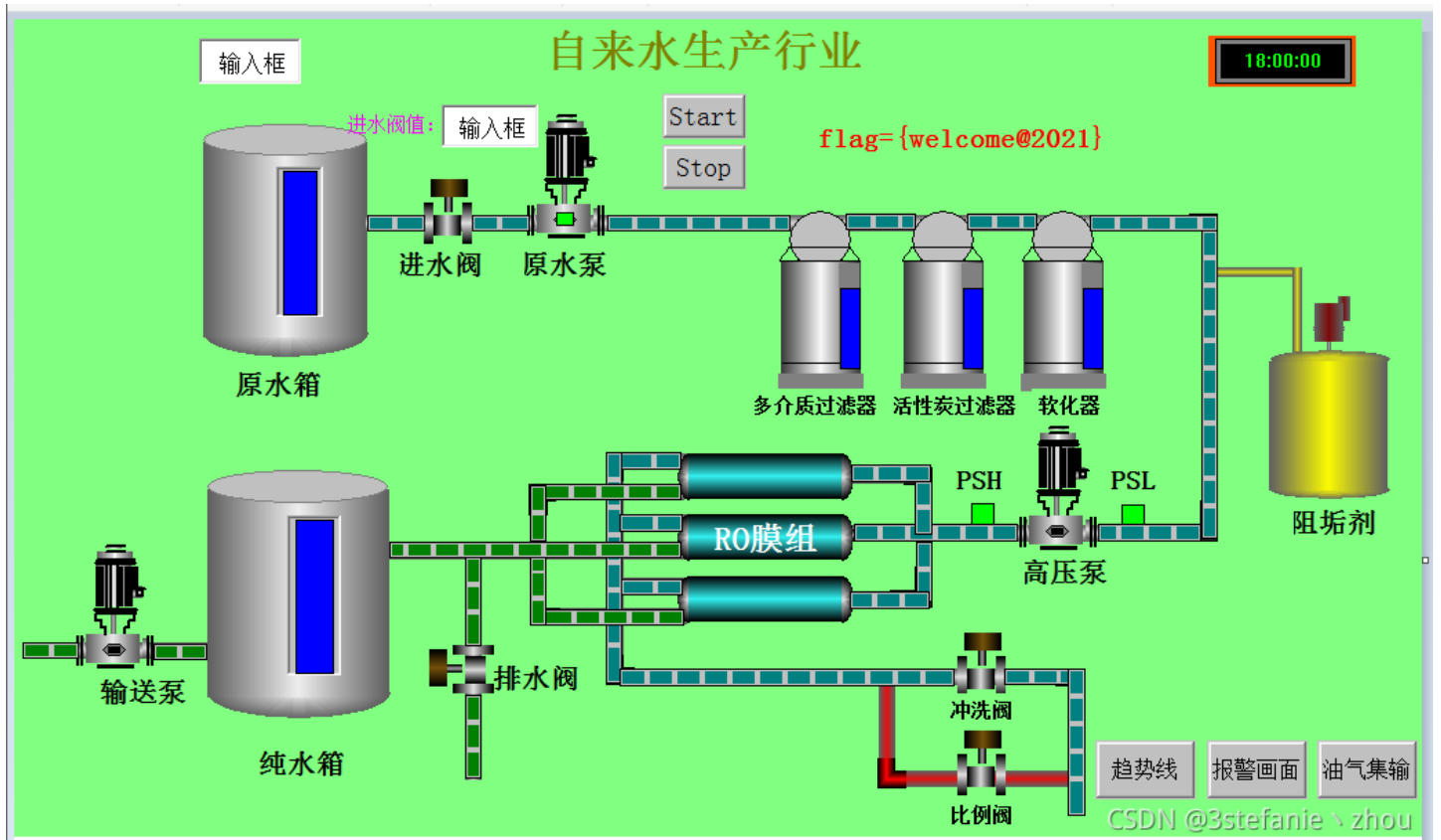
高度很小，修改高度为03 10

```

89 50 4E 47 0D 0A 1A 0A 00 00 00 0D 49 48 44 52 %PNG.....IHDR
00 00 03 FD 00 00 03 10 08 06 00 00 00 17 96 D7 ...ý...-x
41 00 00 00 01 73 52 47 42 00 AE CE 1C E9 00 00 A....sRGB.@Î.é..
00 04 67 41 4D 41 00 00 B1 8F 0B FC 61 05 00 00 ..gAMA..±..üa...
00 09 70 48 59 73 00 00 0E C3 00 00 0E C3 01 C7 ..pHYs...Û...Û.Ç
6F A8 64 00 00 DC A5 49 44 41 54 78 5E ED BD 0D o`d..Û¥IDATx^í½.
F0 55 D5 7D A8 CD 6D 7A D3 A4 93 1B FB F1 D6 DB ðUÜ}”ÍmzÓ”“úňŎŮ
B4 62 FB 8E 4D 9A 26 D1 E9 5B 92 B9 5E 6F CC FB ‘bûZMš&Né[’^oÏû
4E 6B 2D 6F 12 A7 49 AF F7 B6 4D E8 9D 0C F5 05 Nk-o.šI÷¶Mè..ö.
41 44 09 05 09 12 45 87 82 14 B9 22 21 20 84 10 AD....E‡,..!"...
94 52 11 4D 50 4B 09 91 52 F1 AB 51 8B C4 94 72 "R.MPK.'Rň«Q«Ä”r
FD 20 69 A4 64 12 6F 6D 32 69 66 D2 4E 6F EF CC ý i=d.om2ifŎNoiÏ
EF 3D BF 7D CE 3A 67 9D 7D F6 DE 6B ED EF 8F F3 ĩ=z}Î:g.}öPkiĭ.ó
A0 6B FE FF FF 39 7B AF B5 F6 B3 D6 FE 78 D6 D7 kpyÿ9{µö³ŎpxŎx
9E B1 5A F8 0F 02 10 80 00 04 20 00 01 08 40 00 ž±Zø...€...@.
02 10 80 00 04 20 00 81 2E 12 98 D1 C5 83 E2 98 ..€...~ŇÄfâ~
20 00 01 08 40 00 02 10 80 00 04 20 00 01 08 40 ...@...€...@
00 02 10 58 2D 48 3F 23 1D 20 00 01 08 40 00 02 ...X-H?#. ...@..
10 80 00 04 20 00 01 08 40 00 02 1D 25 80 F4 77 .€...@...%€ôw
B4 60 69 D1 82 00 04 20 00 01 08 40 00 02 10 80 ‘iŇ,.. ...@...€
00 04 20 00 01 08 20 FD 48 3F 04 20 00 01 08 40 ... ýH?...@
00 02 10 80 00 04 20 00 01 08 40 A0 A3 04 90 FE ...€...@ £..p
8E 16 2C ED 59 10 80 00 04 20 00 01 08 40 00 02 Ž.,iY.€...@..
10 80 00 04 20 00 01 A4 1F E9 87 00 04 20 00 01 .€...µ.é‡...
08 40 00 02 10 80 00 04 20 00 01 08 74 94 00 D2 .@...€...t”Ŏ
DF D1 82 A5 3D 0B 02 10 80 00 04 20 00 01 08 40 RŇ ¥= €
CSDN @3stefanie \ zhou

```

打开图片，发现flag



flag{welcome@2021}

## 异常流量分析

hint:某企业的运维工程师发现网络中出现流量异常，于是从场内一交换机抓取了数据包，请协助找出流量中针对正常的业务的异常数据内容，flag提交形式为flag{xxxx}。

使用wireshark打开流量包，追踪tcp流

在流41发现一串字符串，syntvfguvfZbqohffffff

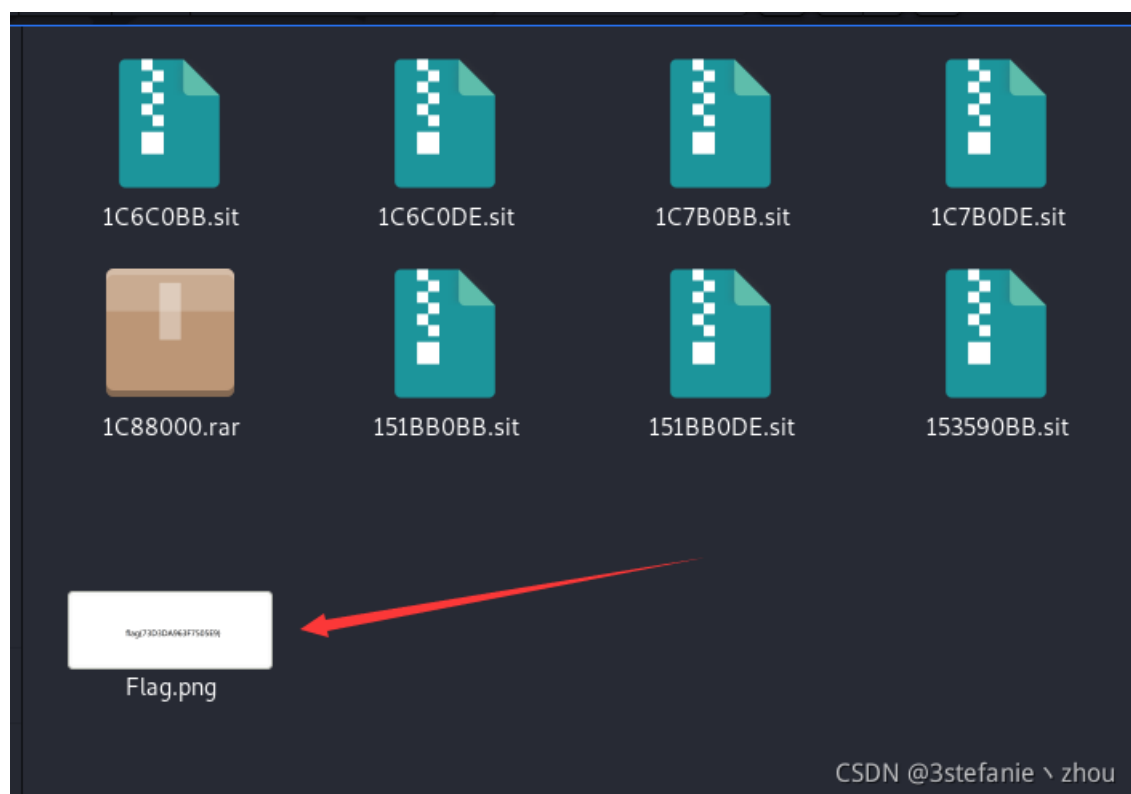


synt开头，显然这是flag经过rot13编码，直接解码,得到flag



## 应急恢复

得到一个data.img的光盘映像文件  
丢进kali，binwalk分析一下  
发现压缩包文件，文件分离一下  
发现flag.png



flag{73D3DA963F7505E9}

CSDN @3stefanie \ zhou

flag{73D3DA963F750E9}

## 恶意app分析

hint:在某工控人员手机中发现一个疑似远控木马样本，请分析该样本，请找到回传数据的目标邮箱地址，为后续的攻击溯源提供帮助，flag提交格式为：flag{邮箱地址}。

解压文件，得到一个apk文件

直接丢进jadx反编译，全局搜索email

```
email
在以下位置搜索：
 类名  方法名  变量名  代码
搜索选项：
 忽略大小写

代码
void
    throw new MessagingException("can't determine local email address");
    public class EmailSender {
    trin... public void sendEmail(String str, String str2, String str3) throws MessagingException {
    ) vo... EmailSender emailSender = new EmailSender();
    ) vo... emailSender.setProperties("smtp.163.com", "25");
    ) vo... emailSender.setMessage("testmail0917@163.com", "test", string);
    ) vo... emailSender.setReceiver(new String[]{"hahaha_wtf@163.com"});
    ) vo... emailSender.sendEmail("smtp.163.com", "testmail0917@163.com", "KCNTEKSKGMGCTGEV");
    }
}
CSDN @3stefanie \ zhou
```

```
flag{hahaha_wtf@163.com}
```

## 工控流量分析

hint:某企业车间PLC运行异常，造成生产线无法正常运行。请您帮助改企业车间分析出PLC遭到异常的原因。flag格式为:flag{}

PLC运行异常，将数据包丢进科来分析数据包

发现3397，3398，7287，7509这四个数据包TCP数据包错误

故障	传输层	错误的TCP数据包校验和(请看数据包: 3397)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
故障	传输层	错误的TCP数据包校验和(请看数据包: 3398)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 3580)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 3680)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
故障	传输层	企图重复建立TCP连接(请看数据包: 4142)	192.168.99.199	Cloud Network Technology (S...	switch.pcfg.cache.wpscdn.cn
性能	传输层	TCP重复的确认(请看数据包: 4146)	192.168.99.199	Cloud Network Technology (S...	switch.pcfg.cache.wpscdn.cn
性能	传输层	TCP重复的确认(请看数据包: 4154)	192.168.99.199	Cloud Network Technology (S...	switch.pcfg.cache.wpscdn.cn
故障	传输层	企图重复建立TCP连接(请看数据包: 4673)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 4676)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 4699)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 4785)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 4845)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 4871)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 4893)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 4974)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
故障	传输层	错误的TCP数据包校验和(请看数据包: 5476)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34

性能	传输层	TCP重复的确认(请看数据包: 6162)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 6236)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
故障	传输层	错误的TCP数据包校验和(请看数据包: 7287)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
故障	传输层	错误的TCP数据包校验和(请看数据包: 7509)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 7581)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 7755)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 9052)	192.168.99.199	Cloud Network Technology (S...	switch.pcfg.cache.wp
故障	传输层	企图重复建立TCP连接(请看数据包: 9378)	192.168.99.199	Cloud Network Technology (S...	120.52.183.165
性能	传输层	TCP重复的确认(请看数据包: 9382)	192.168.99.199	Cloud Network Technology (S...	120.52.183.165
性能	传输层	TCP重复的确认(请看数据包: 9399)	192.168.99.199	Cloud Network Technology (S...	120.52.183.165
故障	传输层	企图重复建立TCP连接(请看数据包: 9718)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 9722)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 9783)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 9825)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34
性能	传输层	TCP重复的确认(请看数据包: 9884)	192.168.99.199	Cloud Network Technology (S...	192.168.99.34

使用wireshark来继续分析



对3397, 3398, 7287, 7509周围几个数据包分析  
在3399发现一个可疑信息, dHEyeXNkczY2  
对其进行解码尝试, 发现base64解码得到内容比较可靠

```
tq2ysds66
```

```
dHEyeXNkczY2
```

CSDN @3stefanie \ zhou

```
flag{tq2ysds66}
```

## 丢失的密码

**hint:**小明作为工厂运维人员, 对路由器固件进行升级操作。升级后尝试使用默认帐户信息以admin / admin身份登录以设置路由器, 但无法连接。分析原因并获取帐户信息。密码即为flag。

使用binwalk - e , 分离文件, 根据提示, 密码为flag

在分离的目录下, 全局搜索password

得到如下密码



```
root@localhost:~/test/10/_takeme.bin.extracted# grep -r 'password' ./squashfs-root/
./squashfs-root/url.html: <input name="passwd" sid="C_URL_PASSWD" type="password" maxlength="32" style="ime-mode:disabled"></div>
./squashfs-root/sysconf_login.js: if(F.password_view && F.password_view.checked == true )
./squashfs-root/sysconf_login.js: if(F.password_view && F.password_view.checked == true )
./squashfs-root/sw:wl_helper.password=12098309ausoifua0sidfAisur091Q84uoqif
匹配到二进制文件 ./squashfs-root/libcgl.so
匹配到二进制文件 ./squashfs-root/m.cgi
./squashfs-root/expertconf_pptvpn.js: var passobj = F.password;
./squashfs-root/expertconf_pptvpn.js: var txtobj = F.password_text;
./squashfs-root/expertconf_pptvpn.js: F.password.value = '';
./squashfs-root/expertconf_pptvpn.js: F.password_text.value = '';
./squashfs-root/expertconf_pptvpn.js: if(F.password_text.value == '')
./squashfs-root/expertconf_pptvpn.js: F.password_text.focus();
./squashfs-root/expertconf_pptvpn.js: if(F.password.value == '')
./squashfs-root/expertconf_pptvpn.js: F.password.focus();
./squashfs-root/expertconf_pptvpn.js: F.password.value = F.password_text.value;
./squashfs-root/expertconf_pptvpn.js: add_hiddeninput(iform, F.password);
./squashfs-root/placeholders.js: 'password',
./squashfs-root/placeholders.js: ( elem.type == 'password' && !elem.getAttribute(ATTR_INPUT_TYPE) )
./squashfs-root/placeholders.js: // Attempt to change the type of password inputs (fails in IE < 9).
./squashfs-root/placeholders.js: elem.type == 'password' &&
./squashfs-root/placeholders.js: elem.setAttribute(ATTR_INPUT_TYPE, 'password');
./squashfs-root/placeholders.js: // If the type of element needs to change, change it (e.g. password
./squashfs-root/placeholders.js: } else if ( elem.type == 'password' && changeType(elem, 'text') ) {
./squashfs-root/placeholders.js: elem.setAttribute(ATTR_INPUT_TYPE, 'password');
```

CSDN @3stefanie \ zhou

```
./squashfs-root/squashfs-root/home/httpd/sysconf/info/js/mobile.js: $password.closest(".row_div").show();
./squashfs-root/squashfs-root/home/httpd/sysconf/info/js/mobile.js: $password.text( _getPASSWORD( data ) );
./squashfs-root/squashfs-root/home/httpd/sysconf/info/js/mobile.js: if($password.text().length > 0)
./squashfs-root/squashfs-root/home/httpd/sysconf/info/js/mobile.js: var $menu, $ssid, $mode, $password, $pwLine, $checkboxbox;
./squashfs-root/squashfs-root/home/httpd/sysconf/info/js/mobile.js: $password = $menu.find("#vghz_password");
./squashfs-root/squashfs-root/home/httpd/sysconf/info/js/mobile.js: $pwLine = $password.closest(".row_div");
./squashfs-root/squashfs-root/home/httpd/sysconf/info/js/mobile.js: $password.closest(".row_div").hide();
./squashfs-root/squashfs-root/home/httpd/sysconf/info/js/mobile.js: $password.closest(".row_div").show();
./squashfs-root/squashfs-root/home/httpd/sysconf/info/js/mobile.js: $password.text( _getPASSWORD( data ) );
./squashfs-root/squashfs-root/home/httpd/sysconf/info/js/mobile.js: if($password.text().length > 0)
./squashfs-root/squashfs-root/home/httpd/sysconf/info/html/main.html: <p class = "lc_grayfont_text" id = "iighz_password"></p>
./squashfs-root/squashfs-root/home/httpd/sysconf/info/html/main.html: <p class = "lc_grayfont_text" id = "vghz_password"></p>
./squashfs-root/squashfs-root/home/httpd/expertconf/pptvpn/js/mobile.js: $('[#id="ADD_PASSWORD"]').attr("type", "password");
./squashfs-root/squashfs-root/home/httpd/expertconf/pptvpn/html/add.html: <input name="password" sid="ADD_PASSWORD" type="password" maxlength="32" style="margin-left: 0.5em;">
./squashfs-root/squashfs-root/home/httpd/netinfo/waninfo/js/mobile.js: $('[#id="C_PPPOE_USERPW"]').attr("type", "password");
./squashfs-root/squashfs-root/home/httpd/netinfo/waninfo/html/main.html: <input name="userpw" sid="C_PPPOE_USERPW" type="password" maxlength="32" style="ime-mode:disabled">
./squashfs-root/squashfs-root/default/var/wps/wscd.conf:device_password_id = 0
./squashfs-root/squashfs-root/default/var/run/si/sw:wl_helper.password=12098309ausoifua0sidfAisur091Q84uoqif
./squashfs-root/squashfs-root/default/etc/iconfig.cfg:password=Wld0b2J5NWllV1YwZER4
匹配到二进制文件 ./squashfs-root/ez-ipupdate
./squashfs-root/wirelessconf_basicsetup.js: var passview = doc.getElementsByName('password')[0];
./squashfs-root/wirelessconf_basicsetup.js: var passviewtext = doc.getElementsByName('password_text')[0];
./squashfs-root/wirelessconf_basicsetup.js: var password = doc.getElementsByName('password')[0];
./squashfs-root/wirelessconf_basicsetup.js: var passwordtext = doc.getElementsByName('password_text')[0];
./squashfs-root/wirelessconf_basicsetup.js: if(F2.password.style.display == 'none')
./squashfs-root/wirelessconf_basicsetup.js: val = F2.password_text.value;
./squashfs-root/wirelessconf_basicsetup.js: val = F2.password.value;
./squashfs-root/wirelessconf_basicsetup.js: if(F2.password.style.display == 'none')
./squashfs-root/wirelessconf_basicsetup.js: F1.wpapsk.value = F2.password_text.value;
./squashfs-root/wirelessconf_basicsetup.js: F1.wpapsk.value = F2.password.value;
./squashfs-root/wirelessconf_basicsetup.js: EnableObj_V2(F.password); EnableObj_V2(F.password_text); EnableObj_V2(F.passview);
./squashfs-root/wirelessconf_basicsetup.js: DisableObj_V2(F.password); DisableObj_V2(F.password_text); DisableObj_V2(F.passview);
./squashfs-root/wirelessconf_basicsetup.js: F.password.value = F2.wpapsk.value;
./squashfs-root/wirelessconf_basicsetup.js: F.password_text.value = F2.wpapsk.value;
```

CSDN @3stefanie \ zhou

```
./squashfs-root/common.js: function PasswordView(password, password_text, password_view)
./squashfs-root/common.js: if(password_view.checked == true)
./squashfs-root/common.js: password.style.display = "none";
./squashfs-root/common.js: password_text.style.display = "inline";
./squashfs-root/common.js: password_text.value = password.value;
./squashfs-root/common.js: password_text.style.display = "none";
./squashfs-root/common.js: password.value = password_text.value;
./squashfs-root/common.js: password.style.display = "inline";
./squashfs-root/common.js: if(F.nopassword && F.nopassword.value == '1')
匹配到二进制文件 ./squashfs-root/wscd
./squashfs-root/account.html: <input name="new_passwd" sid="LOGIN_PASSWORD" type="password" maxlength="32">
./squashfs-root/rsync.html: <input name="passwd" sid="C_RSYNC_PASSWD" type="password" maxlength="32" style="ime-mode:disabled"></div>
./squashfs-root/add.html: <input name="password" sid="ADD_PASSWORD" type="password" maxlength="32" style="margin-left: 0.5em;">
./squashfs-root/wscd.conf:device_password_id = 0
./squashfs-root/iconfig.cfg:password=hacked123
./squashfs-root/jquery.js: !function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a){if(!a.docume
```

CSDN @3stefanie \ zhou

逐一作为flag尝试

正确flag为

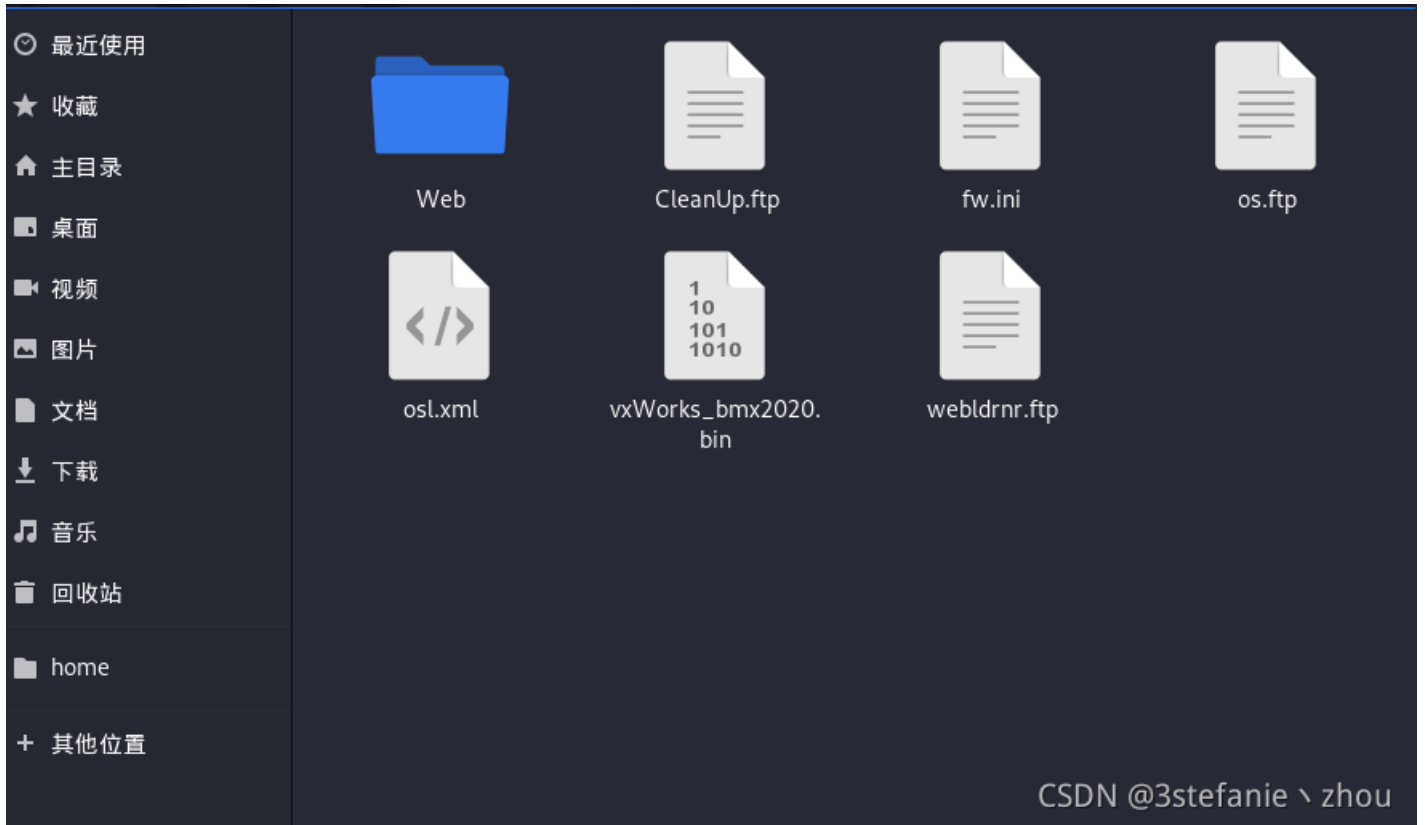
flag{Wld0b2J5NWllV1YwZER4}

## 工业固件分析

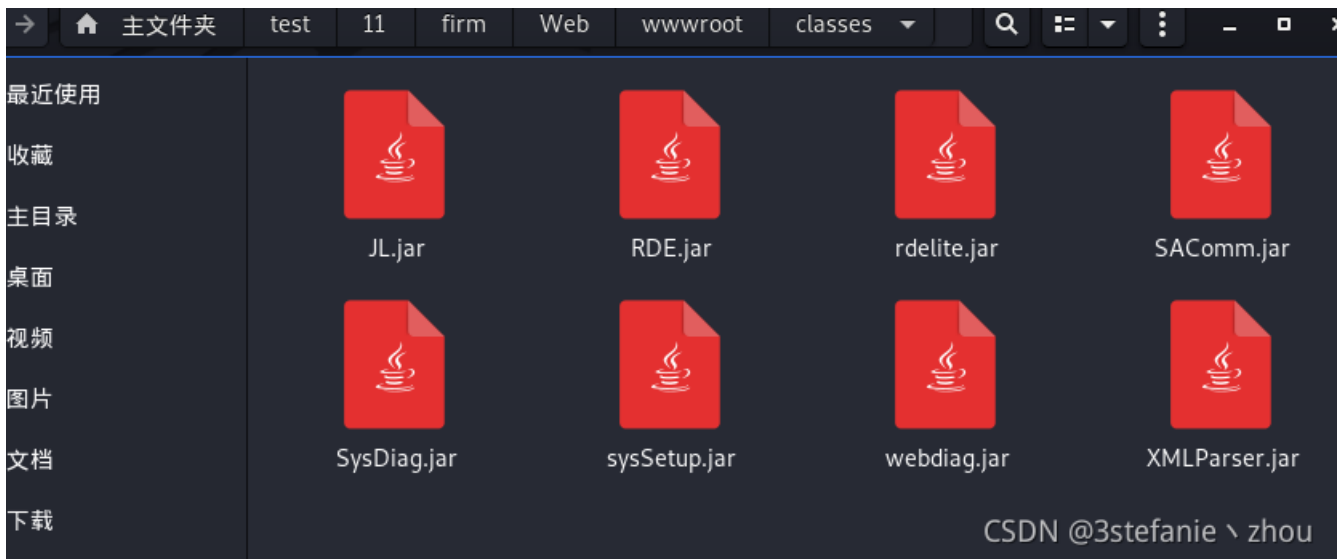
hint:某PLC设备的固件已被攻击者提取并打包，请对固件进行分析，获取固件中被硬编码的ftp账户用户名密码信息。

flag格式为：flag{ftp username+ftp password}，例如，用户名为admin，密码为123，则flag为flag{admin+123}。

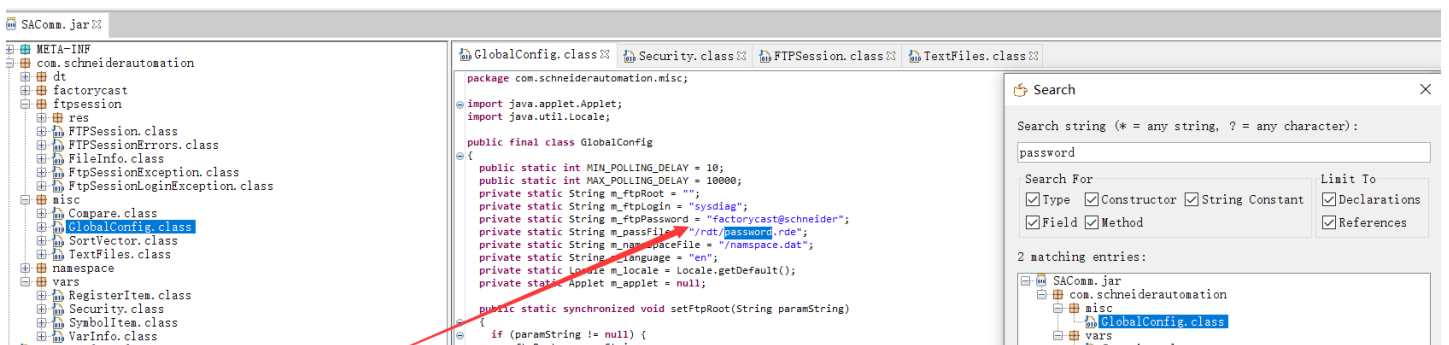
根据提示信息，解压压缩包，得到如下文件



由于ftp账户用户名密码信息被硬编码在代码中，所以找到如下jar包



逐一丢进jd里面反编译，然后全局搜索password  
最终在SACComm.jar这个Jar包中发现ftp的账户密码信息



```
    }  
    }  
    public static synchronized String getFtpRoot()  
    {  
        return _ftpRoot;  
    }  
    public static synchronized void setFtpUser(String paramString)  
    {  
        if (paramString != null) {
```

CSDN @3stefanie \ zhou

```
flag{sysdiag+factorycast@schneider}
```

## opc流量分析

hint:OPC是微软公司的对象连接和嵌入技术在过程控制方面的应用，OPC标准定义了基于PC的客户机之间进行自动化数据实时交换的方法，因此OPC协议在工业控制现场使用非常多。请对提供的OPC通信流量进行分析，尝试找出流量中的flag。



4.b.f.9.3.4.5.9.a.e.7.d.3.e.d.4.9.5.8.f.7.8.6.2.4.5.3.1.7.9.c.8  
5.3.5.5.4.E.5.4.6.1.6.E.6.8.4.1.4.D.6.A.4.1.7.9.4.D.5.1.3.d.3.d  
7.a.5.d.8.a.4.b.4.9.5.8.a.4.b.f.9.3.4.5.9.a.e.7.d.3.e.d.4.9.5.8  
9.a.9.e.4.d.6.f.2.a.4.b.3.c.4.a.4.f.6.e.7.c.8.b.9.d.6.f.4.a.6.f  
8.a.9.b.7.e.1.f.7.8.6.2.4.5.3.1.7.9.c.8.9.a.1.4.5.4.6.9.4.7.1.6  
a.4.b.3.c.4.9.5.8.f.7.8.4.d.6.f.2.a.4.b.3.c.4.9.5.8.f.7.4.5.3.1  
1.7.9.c.8.9.a.1.4.5.4.6.9.4.7.1.6.f.9.3.4.5.9.a.e.7.d.3.e.4.7.9  
去除小数点,得到**16进制数据**

4bf93459ae7d3ed4958f7862453179c8  
53554E54616E68414D6A41794D513d3d  
7a5d8a4b4958a4bf93459ae7d3ed4958  
9a9e4d6f2a4b3c4a4f6e7c8b9d6f4a6f  
8a9b7e1f7862453179c89a1454694716  
a4b3c4958f784d6f2a4b3c4958f74531  
179c89a1454694716f93459ae7d3e479

转成字符串

Kù4Y@}>Ô•xbE1yĚ  
SUNTanhAMjAyMQ==  
z]ŠKIXꞑ¿“EšçÓilX  
šžMoK<JOn|ꞑoJo  
Š}~xbE1yĚšTiG  
ꞑ³Ă•xMoK<IX÷E1  
œ%∞jEF”qo“EšçÓäy

将唯一的正常字符串进行base64解码

```
ICSjx@2021
```

```
SUNTanhAMjAyMQ==
```

多行 [Base64编码](#) [Base64解码](#) [清空结果](#)  
CSDN @3stefanie、zhou

得到flag

```
flag{ICSjx@2021}
```

【吾有所思人，隔在远远乡】