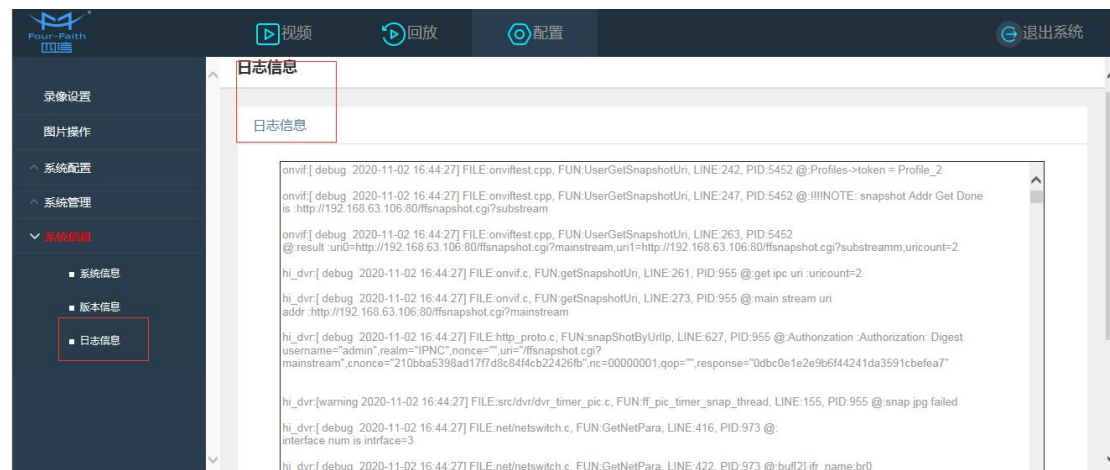
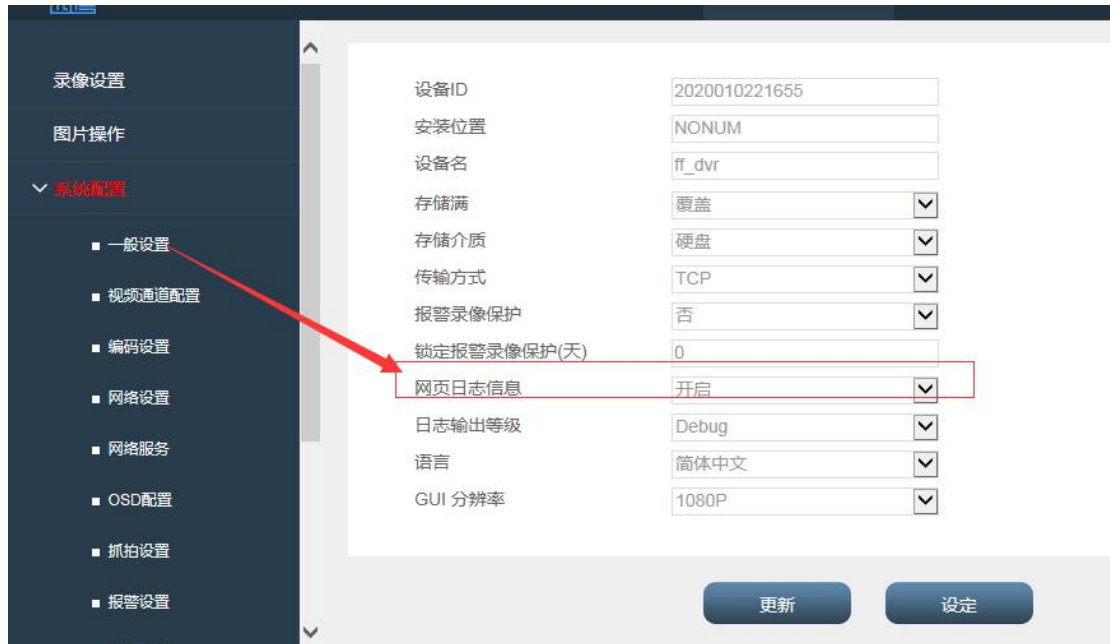


四、日志获取

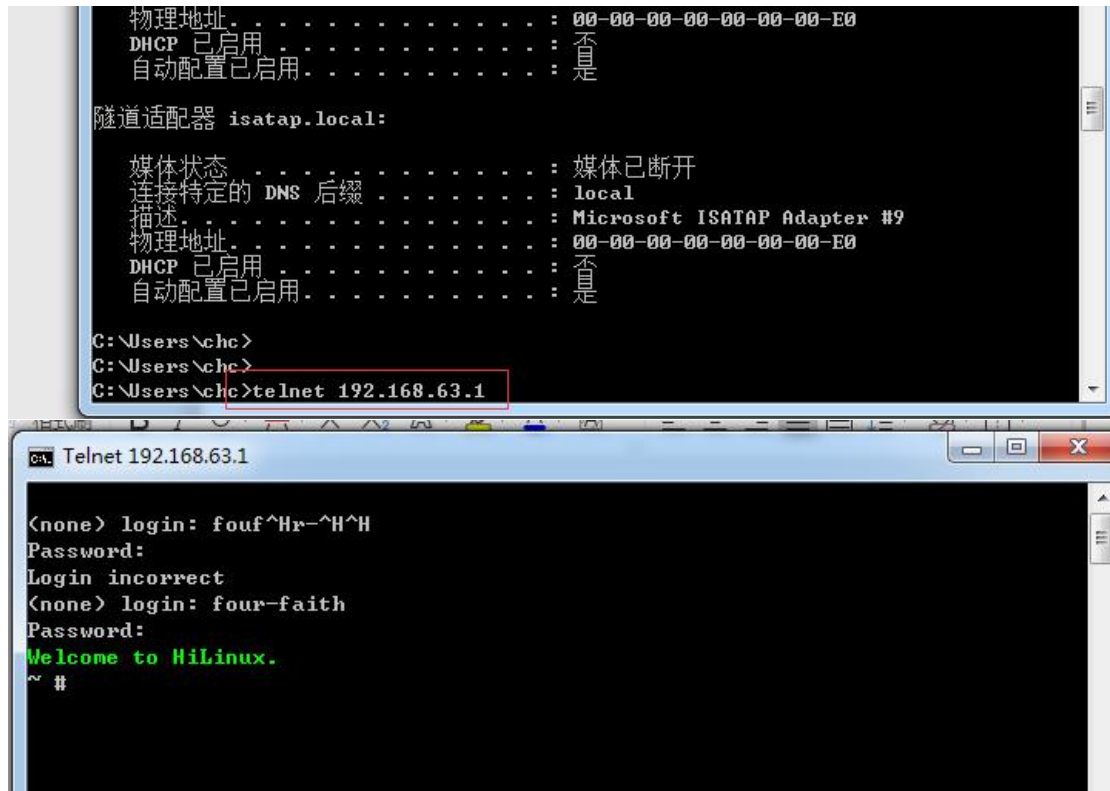
1、NVR 网页日志



1、NVR 工具抓包

(1) telnet 登录 NVR 设备

用户 four-faith 密码 four-faith-dvr



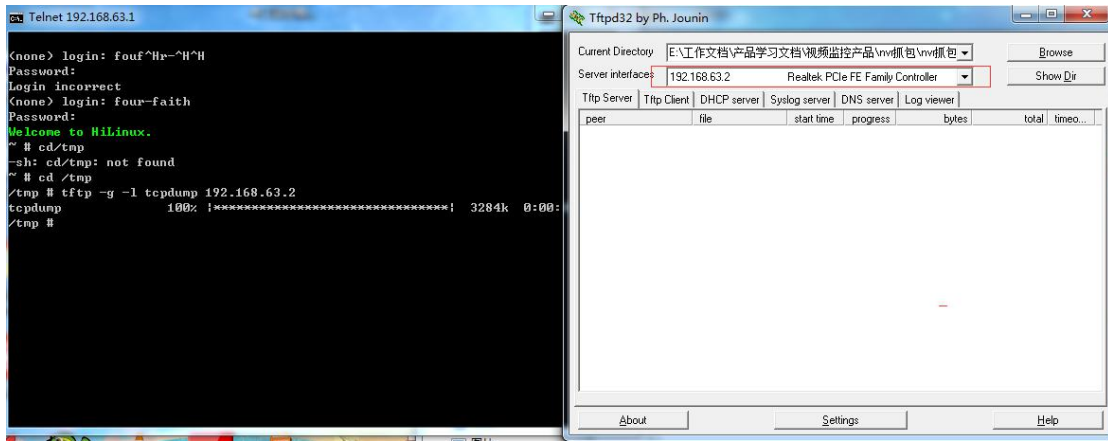
(2) 抓包步骤

- (1) cd /tmp
- (2) 开启 pc 的 tftpd32.exe
- (3) tftp -g -l tcpdump 电脑 ip
- (4) chmod 777 tcpdump
- (5) 抓包命令

./tcpdump -i any -f "port 5060" -s 0 -v -w ./sip.pcap (日志名)
(5060 根据实际端口填入)

./tcpdump -i any -f "ip host 192.168.63.2 and port 80" -s 0 -v -w ./onvif916.pcap
(针对某个 ip, onvif916.pcap 为保存的日志名称)

- (6) ctrl+c 关闭刚才的命令
- (7) tftp -p -l onvif916.pcap 192.168.63.2
tftp -p -l sip.pcap 192.168.63.2
- (8) 在抓包目录中找到 onvif916.pcap



```

/tmp # tftp -g -l tcpdump 192.168.63.2
tcpdump 100% !*****! 3284k 0:00:00 ETA
/tmp # chmod 777 tcpdump

```

```

/tmp # ./tcpdump -i any -f "ip host 192.168.63.2 and port 80" -s 0 -v -w ./onvif916.pcap
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size 262144 bytes
^C112 packets captured
116 packets received by filter
0 packets dropped by kernel
/tmp # tftp -p -l onvif916.pcap 192.168.63.2
onvif916.pcap 100% !*****! 13326 0:00:00 ETA
/tmp #

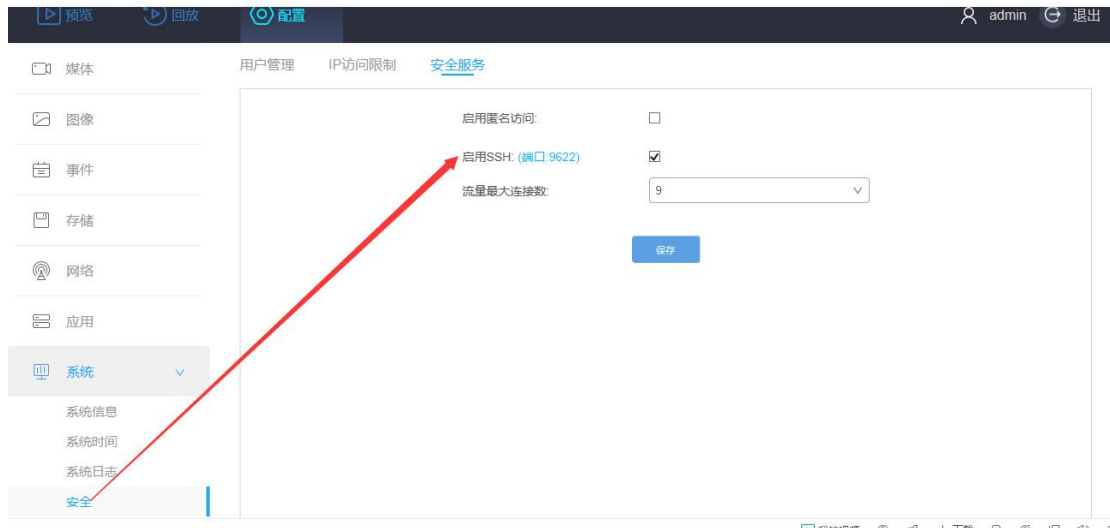
```

2、摄像头 IPC 网页日志



3、摄像头工具抓包

(1) 打开摄像头网页，开启 SSH 服务，默认端口 9622



SecureCRT(1).rar

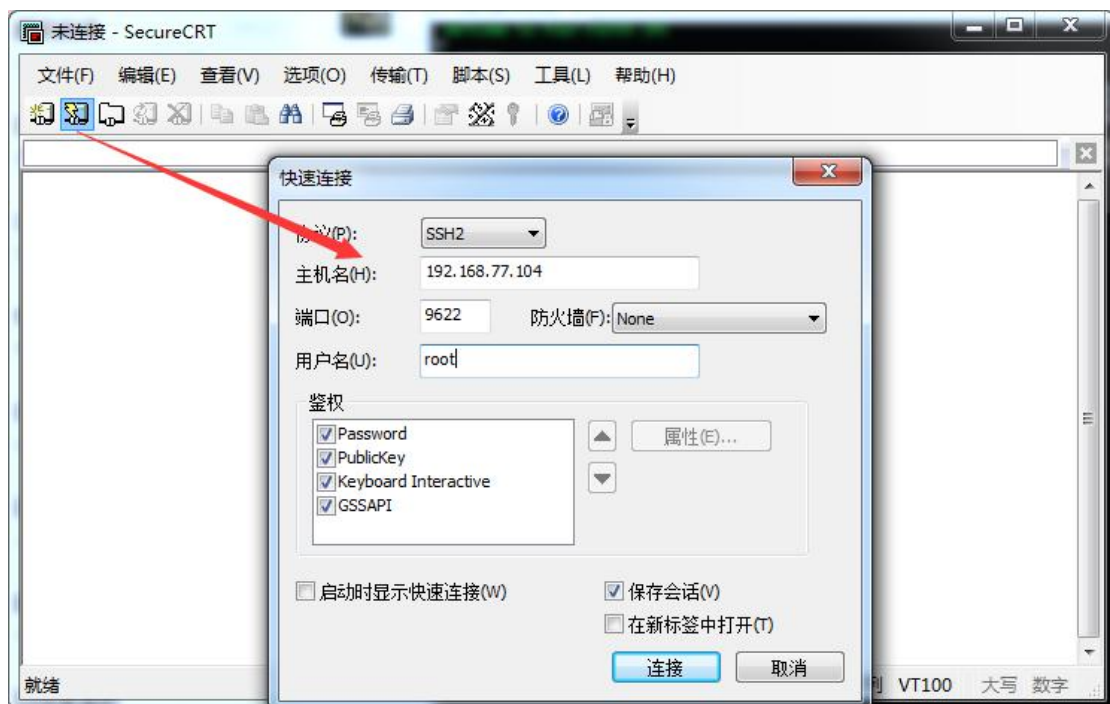
(2) 开启抓包工具 CRT，点击新建连接，设置参数。

协议：SSH2

端口：9622

用户名：root

密码：ff666





(3) 连接成功，输入指令 `touch /tmp/d2p0`

```
#
# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
default 192.168.77.1 0.0.0.0 UG 0 0 0 eth0
127.0.0.0 * 255.0.0.0 U 0 0 0 lo
192.168.77.0 * 255.255.255.0 U 0 0 0 eth0
224.0.0.0 * 224.0.0.0 U 0 0 0 eth0
# touch /tmp/d2p0
# [2020-11-02 10:40:47.716][ffwater KPA(1424)][I][ PRINT][ffwater_monitor.c:133] set gpio AT+GPIO=setdata,2,0,1
[2020-11-02 10:40:48.217][ffwater KPA(1424)][I][ PRINT][ffwater_monitor.c:133] set gpio AT+GPIO=setdata,1,11,1
[CREATE FILE] /dev/usbdev1.9
[2020-11-02 10:40:59.995][ffcore MMC(1388)][I][ STG][ffcore_stg.c:746] the power is need open -1
[2020-11-02 10:40:59.996][ffcore MMC(1388)][I][ STG][ffcore_stg.c:763] cmd : echo -n 1 > /sys/bus/usb/devices/1-1.4/bConfigur
[CREATE FILE] /dev/qcqm10
[CREATE FILE] /dev/ttyUSB0
[CREATE FILE] /dev/ttyUSB1
[CREATE FILE] /dev/ttyUSB2
[CREATE FILE] /dev/ttyUSB3
[2020-11-02 10:41:29.961][ffweb ffweb(1470)][D][ FFweb][ffweb_translate.c:4022] [gbvideidx.] not found
[2020-11-02 10:41:32.712][ffweb ffweb(1470)][D][ FFweb][ffweb_translate.c:4022] [gbvideidx.] not found
[2020-11-02 10:41:36.769][ffcore workq(1283)][D][ IPC][ffss_ipcm.c:569] MSG(3013):MSG_CORE_LOG_SAVE from:Unknow begin
[2020-11-02 10:41:36.769][ffcore workq(1283)][D][ IPC][ffss_ipcm.c:594] MSG(3013):MSG_CORE_LOG_SAVE from:Unknow end
[2020-11-02 10:41:36.858][ffcore log(1387)][N][ Log][ffstg_log.c:353] log write backup to success 264 3
[2020-11-02 10:41:37.290][ffwater KPA(1424)][I][ PRINT][ffwater_monitor.c:133] set gpio AT+GPIO=setdata,2,0,0
[2020-11-02 10:41:37.388][ffwater ffweb(1470)][D][ FFweb][ffweb_translate.c:4022] [gbvideidx.] not found
[DELETE FILE] /dev/qcqm10
[DELETE FILE] /dev/ttyUSB0
[DELETE FILE] /dev/ttyUSB1
[DELETE FILE] /dev/ttyUSB2
[DELETE FILE] /dev/ttyUSB3
```

(4) 保存日志信息

点击文件--记录会话--保存日志路径。

