How to use tcpdump to capture packet of 6900UDI (serial)

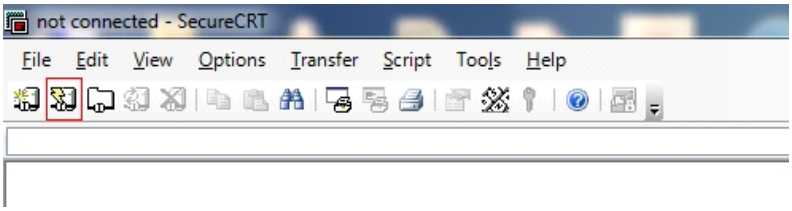
HIKVISION TECHNICAL SUPPORT TEAM

2017-6-10

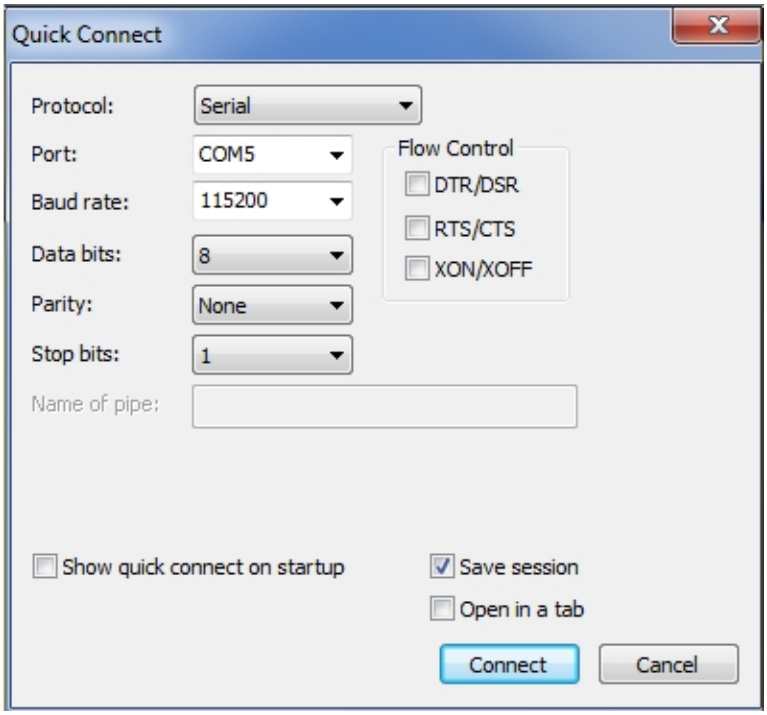
How to use tcpdump to capture packet of 6900UDI (serial)

This document is intended to guide the method of packet capture through serial operations. Sometimes decoder cannot get stream from encoding devices successfully, in this case, we need to use tcpdump to analyze where the problem comes from.

1. Open SecureCRT software and click Quick Connect



2. Choose Serial protocol, configure the parameters as below, disable flow control, and select the right COM port

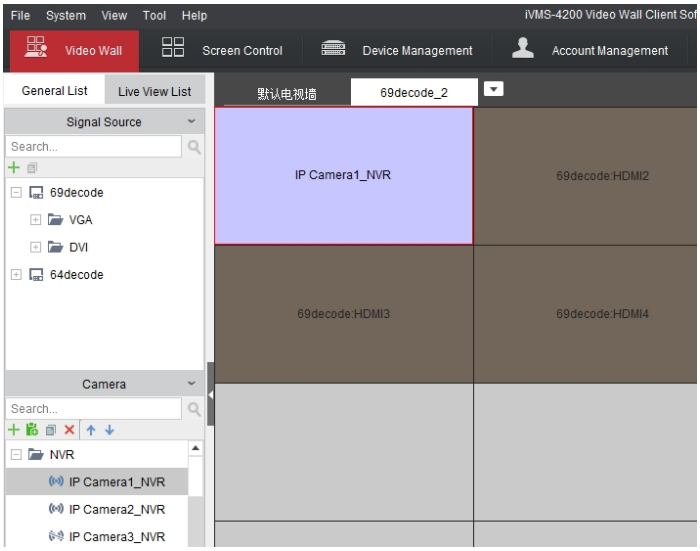


3. Input “zhimakaimen”, fill in the security code exported from OA to enter debug mode


```
# zhimakaimen
AwAAAIznSJVboHUbQ2s=
Password:
Enter Debug Mode.
[1]+  Done                    /dav/initrun.78x60.sh
[root@Hik-DECODER-M ] # Niwd+7iH5HRe275GZU+7Qe/M5tb/M7KZAAOjrsa22LSZ0udjj2gBwrSc
SHcD/ZR82s+10P4FpzmvDBJpomDWEu+0=
-/bin/sh: Niwd+7iH5HRe275GZU+7Qe/M5tb/M7KZAAOjrsa22LSZ0udjj2gBwrScSHcD/ZR82s+10P4
[root@Hik-DECODER-M ] #
```

4. Packet capture

   Drag the channel you wanted to analyze on the video wall client (In order to locate the problem, keep the only camera to decode on the video wall)



   For 6900UDI

① Input cd home/program to enter program file, use ls to check the tcpdump command

```
[root@Hik-DECODER-M ] # cd home/program
[root@Hik-DECODER-M program] # ls
CpuOverLoad.yuv     libnl.so.2          t1
NoResource.yuv      libsqlite3.so.0.8.6 tcpdump
decore              logSearch           vitest
devKfile            netradbg            votest
dspcore             noNetVideo_cn.yuv   wifi.sh
dspdebug            noNetVideo_en.yuv   wifitest
libiconv.so         shellTools          wpa_cli
libnl-genl.so.2     start.sh            wpa_supplicant
```

② Input ./tcpdump –w /home/x.pcap to start packet capturing (For the capturing of encoding device with certain IP, use ./tcpdump –w host *IP address* –w 111.pcap, the IP address is the IP of encoding device)

```
[root@Hik-DECODER-M program] # ./tcpdump -w /home/x.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 b
ytes
^C26935 packets captured
26935 packets received by filter
0 packets dropped by kernel
```

③ After about 1 minute, press CTRL+C to quit packet capture

④ Open cisco tftp, input cd .. (to quit to home file), ls to check if the x.pcap document exported successfully

```
[root@Hik-DECODER-M program] # cd ..
[root@Hik-DECODER-M home] # ls
cmd.socket  opt         shellpid    system      x.pcap
config      program     streamSave  webs
```

⑤ Input tftp –pl x.pcap *IP address* (IP of tftp server) to export the x.pcap to the file of tftp tool

```
[root@Hik-DECODER-M home] # tftp -pl x.pcap 10.5.2.11
x.pcap          0% |                                |  36864   0:10:08 E
x.pcap          1% |                                |    425k  0:01:41 E
x.pcap          3% |*                               |    741k  0:01:25 E
x.pcap          4% |*                               |   1004k  0:01:23 E
x.pcap          5% |*                               |   1238k  0:01:23 E
```

TFTPServer	2004/7/30 12:35	Application	23 KB
tftpsvc.dll	1998/7/8 11:12	Application extens...	19 KB
u-boot	2010/12/6 9:02	VLC media file (.bi...	143 KB
u-boot_8127	2015/10/14 20:11	VLC media file (.bi...	384 KB
uImage_flash	2007/12/4 15:41	File	1,122 KB
x	2017/6/10 19:32	Wireshark capture...	21,941 KB
yuv.yuv	2011/7/27 14:43	YUV File	1,152 KB
yuv2.yuv	2011/7/27 14:46	YUV File	1,152 KB

Note: 1. Use “cd filename” to enter certain file
2. Use “cd ..” to return to previous directory
3. Use “ls” to check the files in the directory

First Choice for Security Professionals
Hikvision Technical Support