



**How to capture package on keyboard by serial cable**

**HIKVISION TECHNICAL SUPPORT TEAM**

## How to capture package on keyboard by serial cable

### Note:

Upgrade of panel version should be done under professional guidance from technical engineer

### Tools needed:

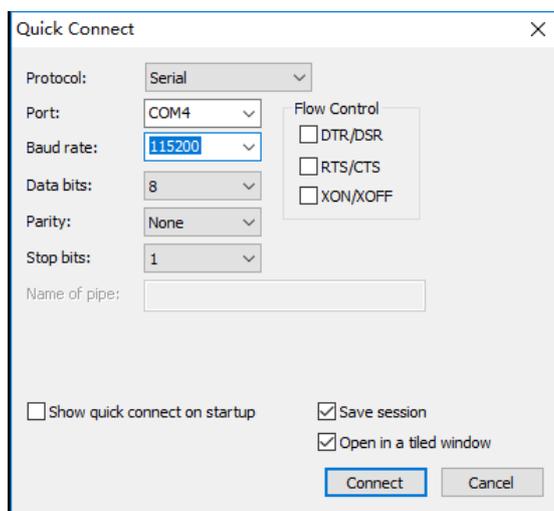
SecureCRT

1. Connect serial cable to keyboard with your computer.
2. Check serial COM number.



3. Open SecureCRT

- 1) Open SecureCRT, click **quick connect**, Select **serial**, input **COM number** of keyboard



- 2) Input **debug**, then it will appear a string, copy the string to OA search for the password.



Note: when you input password, CRT tool doesn't display any "\*", it will still display blank.

### Device Password Resetting

**Custom Message \***

**Device Key**

**Security Code**

```
3PQn47YJbY/ZfZD1W/1KHp5XFT7/OVsODpfzUdsKwh7xkK3b9juBLmwm
eIiXciiWwIyXZ06Xj2gZykOSjYTagFnUFXxzeh3JyDnHUALqIiqJW3On
IN4FwDZ/q6MZMye8w34bGvFf9FMk201mKTOYA5jGDJMmFvV0+PKtsEjo
GMw=
```

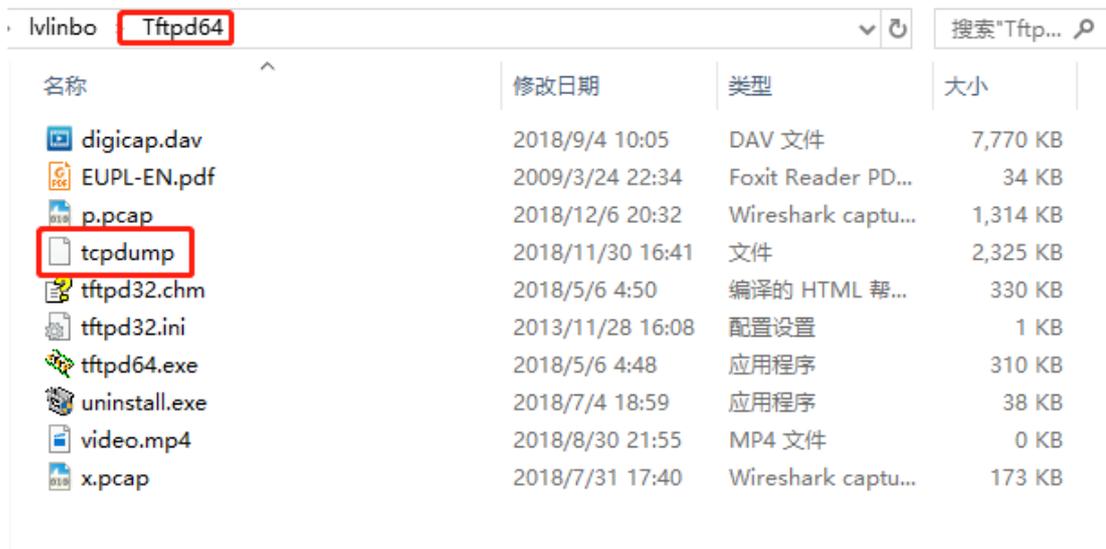
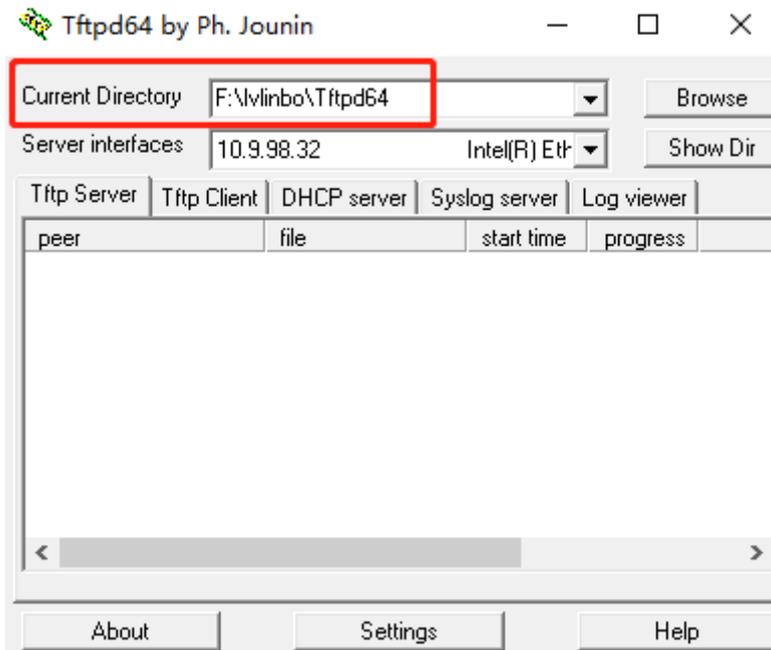
```
#
#
# debug
AwAAALYxmiRNp/bKjRc= → copy it to OA
Password:
Enter Debug Mode.
psh
[1]+ Done /home/start.sh
~ #
~ #
~ #
~ #
~ #
~ #
```

3) Then input `cd ..` to the upper folder list. And afterwards input `ls` check whether you have been there.

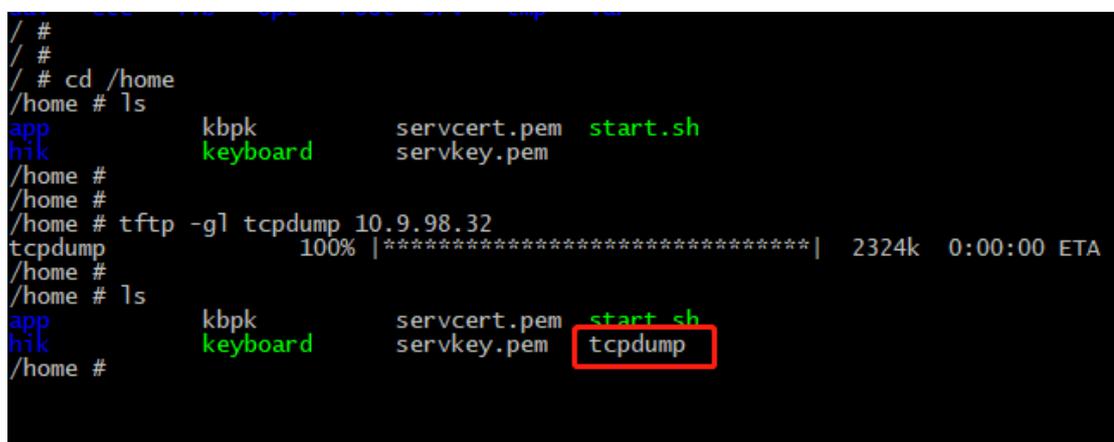
```
~ #
~ #
~ #
~ # cd ..
/ # ls
bin dev home mnt proc sbin sys usr
dav etc lib opt root srv tmp var
/ #
```



4) Put tcpdump tool to the current directory of tftp tool.



5) Input `cd /home`, then input `tftp -gl tcpdump tftp server IP`



- 6) Input `chmod a+x tcpdump`.

```
/home #  
/home #  
/home # chmod a+x tcpdump  
/home #
```

- 7) Input `./tcpdump host IP -w /home/file name` to capture package. File name always name as `xxx.pcap`. Host IP is equal to the IP you want to know the camera or NVR whose interaction between keyboard and them.

```
/home # ./tcpdump host 10.9.98.32 -w /home/p.pcap  
device eth0 entered promiscuous mode  
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes  
00 packets captured  
1 packet received by filter  
0 pdevice eth0 left promiscuous mode  
ackets dropped by kernel  
/home #
```

- 8) Then input `tftp -pl file name tftp server IP` to export file. Send it to HQ to analyze.

```
/home #  
/home #  
/home # tftp -pl p.pcap 10.9.98.32  
p.pcap 100% |*****| 24 0:00:00 ETA  
/home #
```



First Choice for Security Professionals  
Hikvision Technical Support

