Preparation

1. FreeNFS tool.
2. Specific Tcpdump file.
3. SecureCRT.

How to Capture Packet via Tcpdump

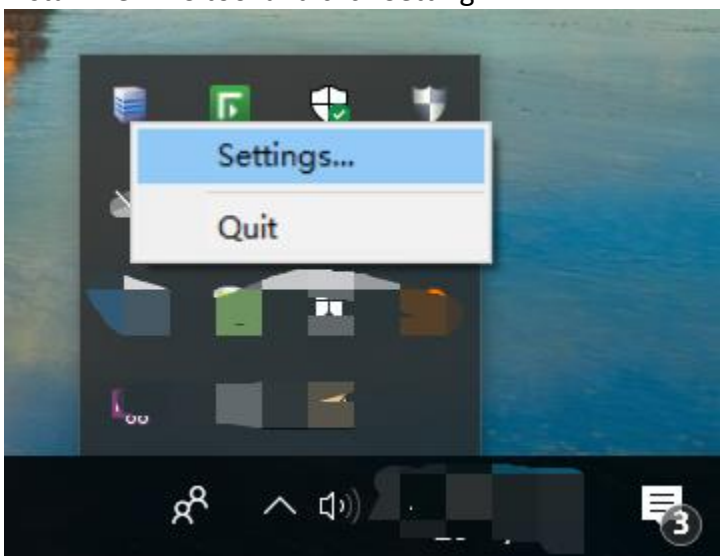
No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China • Tel: +86-571-8807-5998 • Fax: +1 909-595-0788
E-Mail: support@hikvision.com • www.hikvision.com

When we troubleshoot protocol problems in daily work, usually need to capture the packet to obtain the interaction information between the device side and the platform, but under the influence of the site's inherent environment, there may not be conditions that can capture the network information flow on the device side on the switch. Under this condition, we can obtain it through the underlying packet capture method on the device side, that is tcpdump. The following describes the two common capture methods of tcpdump packet.

1. NFS mount capture

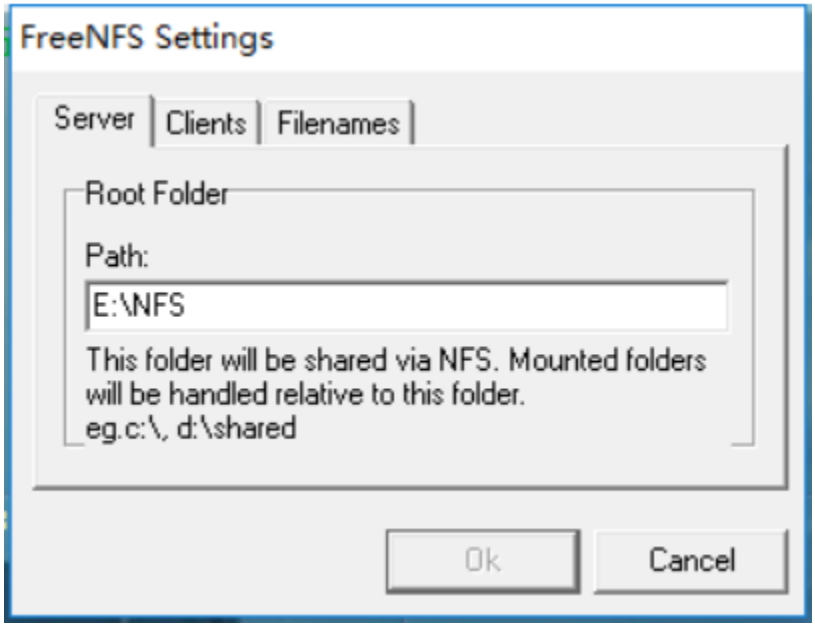
1) Crate a new folder on PC and name NFS, which is mount folder.

2) Install FreeNFS tool and click Setting.



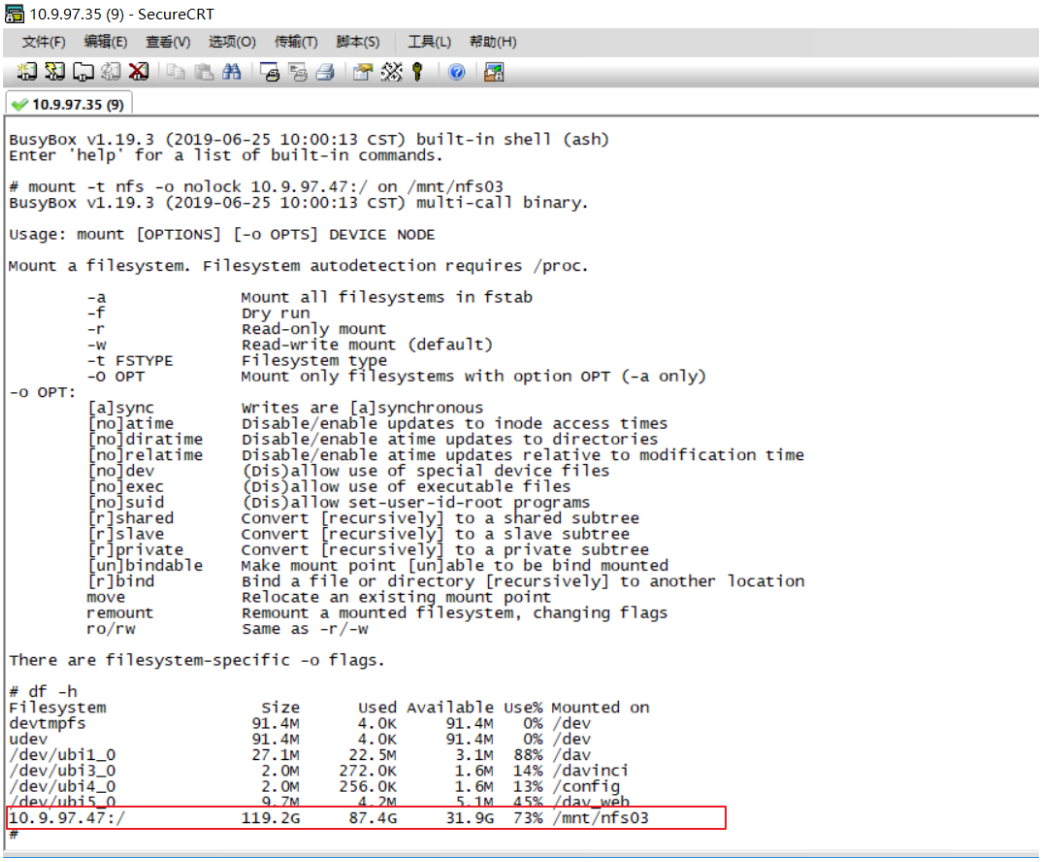
Input folder path created in step 1 (eg: If crated it in Disk E, fill in E:\NFS). And copy Tcpdump file to this folder.

No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China • Tel: +86-571-8807-5998 • Fax: +1 909-595-0788
E-Mail: support@hikvision.com • www.hikvision.com



3) Access CRT via SSH, than input zhimakaimen(debug) to enter debug mode.

4) Input command "**mount -t nfs -o nolock 10.9.97.47:/ /mnt/nfs03**" to mount PC path on camera (10.9.97.47 is PC's IP address), and you can check Filesystem via "**df -h**".



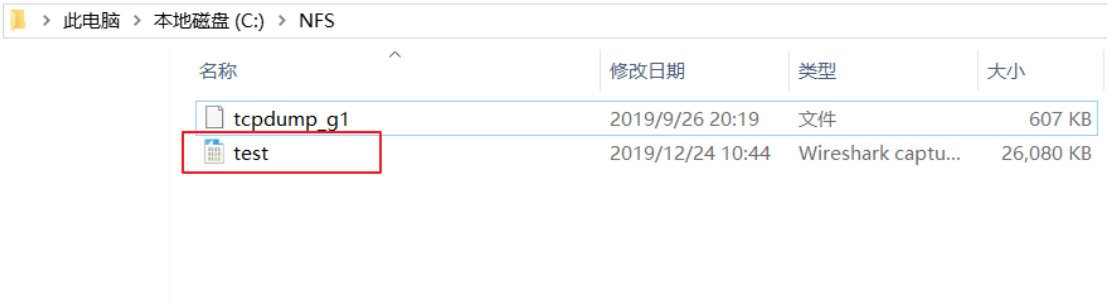
5) Copy the tcpdump file to "NFS" folder in step 1, following that, copy tcpdump to path "/home" of camera via command "**cp /mnt/nfs03/tcpdump /home**".

```
# cp /mnt/nfs03/tcpdump_g1 /home
# cd /home
# ls
alarm.ko        dlog            hikdsp          process         tcpdump_g1
applib          dsta            initrun.sh      script          vd_notify.ko
da_info         event_notify.ko motor.ko        serialCom       wifi
dalg            firmware        pidfile         sound
#
```

6) Input command "**/home/tcpdump -i eth0 -s0 -w /mnt/nfs03/test.cap**" to start capturing (test is packet name), and hit "**Ctrl+C**" to stop capturing.

If this command is no response, please input "**chmod 777 /home/tcpdump**" before capturing.

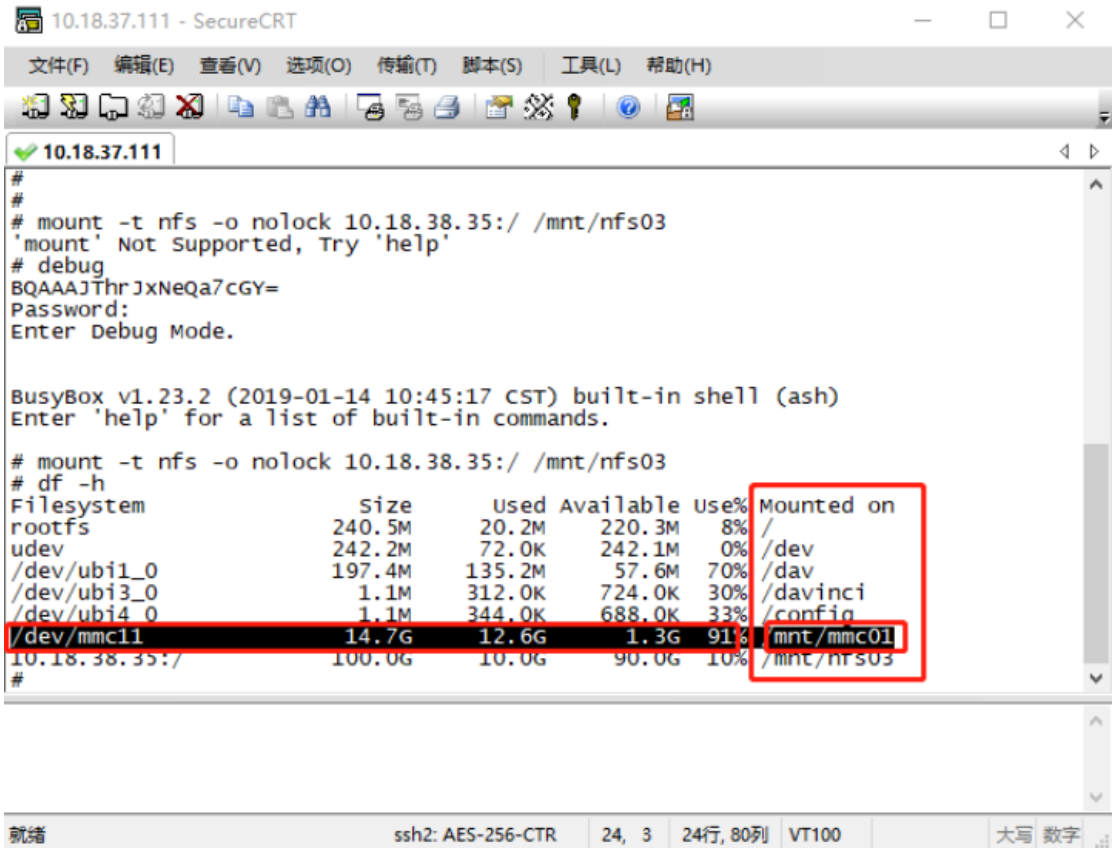
```
# chmod 777 /home/tcpdump_g1
# /home/tcpdump_g1 -i eth0 -s0 -w /mnt/nfs03/test.cap
tcpdump_g1: listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```



No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China • Tel: +86-571-8807-5998 • Fax: +1 909-595-0788
E-Mail: support@hikvision.com • www.hikvision.com

2. SD card capture

1) Copy tcpdump file to SD card on computer, plug SD card in camera.
   Note: Do not format SD card on IPC web.
2) Access CRT via SSH, than input zhimakaimen(debug) to enter debug mode.
3) Use the "df -h" command to confirm whether the SD card is successfully mounted and the location where the partition is mounted.



4) Enter this mount directory via "**cd /mnt/mmc01**".
   Use command "**tcpdump.dat -l eth0 -s0 -w test.cap**" to capture packets, and also hit "Ctrl + C" as the end packet capture instruction

No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China • Tel: +86-571-8807-5998 • Fax: +1 909-595-0788
E-Mail: support@hikvision.com • www.hikvision.com

First Choice for Security Professionals

***HIKVISION* Technical Support**

No.555 Qianmo Road, Binjiang District, Hangzhou 310052, China • Tel: +86-571-8807-5998 • Fax: +1 909-595-0788
E-Mail: support@hikvision.com • www.hikvision.com