

Title:	How to Capture Packet via Tcpdump	Version:	v1.0	Date:	12/24/2019
Product:	IP Camera			Page:	1 of 6

Preparation

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

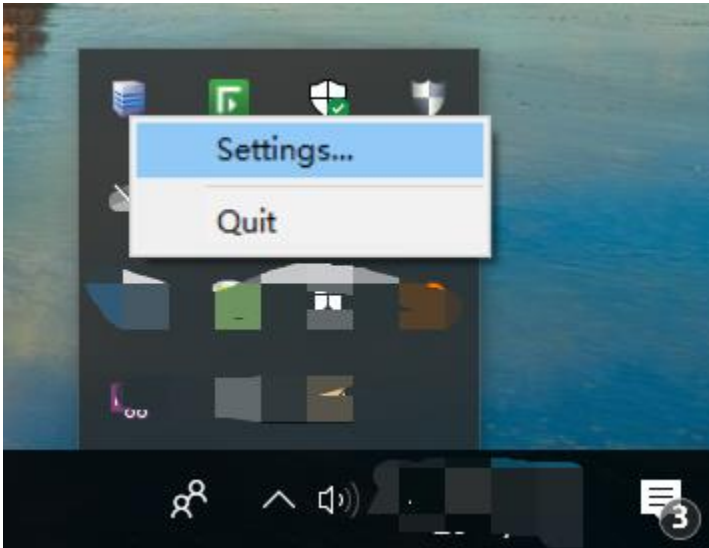
How to Capture Packet via Tcpdump

Title:	How to Capture Packet via Tcpdump	Version:	v1.0	Date:	12/24/2019
Product:	IP Camera			Page:	2 of 6

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.

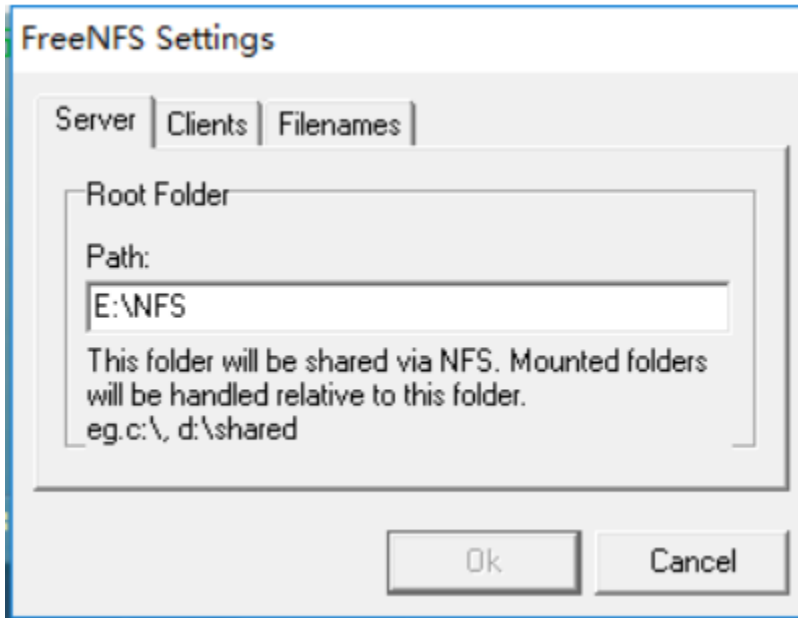
1. NFS mount capture

- 1) Create 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 created it in Disk E, fill in E:\NFS). And copy Tcpdump file to this folder.

Title:	How to Capture Packet via Tcpcdump	Version:	v1.0	Date:	12/24/2019
Product:	IP Camera			Page:	3 of 6



- 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**”.

```
10.9.97.35 (9) - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)
10.9.97.35 (9)
BusyBox v1.19.3 (2019-06-25 10:00:13 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# mount -t nfs -o nolock 10.9.97.47:/ on /mnt/nfs03
BusyBox v1.19.3 (2019-06-25 10:00:13 CST) multi-call binary.

Usage: mount [OPTIONS] [-o OPTS] DEVICE NODE

Mount a filesystem. Filesystem autodetection requires /proc.

    -a          Mount all filesystems in fstab
    -f          Dry run
    -r          Read-only mount
    -w          Read-write mount (default)
    -t FSTYPE   Filesystem type
    -O OPT      Mount only filesystems with option OPT (-a only)

-o OPT:
[a]sync       writes are [a]synchronous
[no]atime     Disable/enable updates to inode access times
[no]diratime  Disable/enable atime updates to directories
[no]relatime  Disable/enable atime updates relative to modification time
[no]dev       (Dis)allow use of special device files
[no]exec      (Dis)allow use of executable files
[no]suid      (Dis)allow set-user-id-root programs
[r]shared     Convert [recursively] to a shared subtree
[r]slave      Convert [recursively] to a slave subtree
[r]private    Convert [recursively] to a private subtree
[un]bindable  Make mount point [un]able to be bind mounted
[r]bind       Bind a file or directory [recursively] to another location
move          Relocate an existing mount point
remount       Remount a mounted filesystem, changing flags
ro/rw        Same as -r/-w

There are filesystem-specific -o flags.

# df -h
Filesystem      Size      Used Available Use% Mounted on
devtmpfs        91.4M     4.0K      91.4M    0% /dev
udev            91.4M     4.0K      91.4M    0% /dev
/dev/ubi1_0     27.1M     22.5M      3.1M   88% /dav
/dev/ubi3_0     2.0M     272.0K    1.6M   14% /davinci
/dev/ubi4_0     2.0M     256.0K    1.6M   13% /config
/dev/ubi5_0     9.7M      4.2M      5.1M   45% /dav_web
10.9.97.47:/    119.2G    87.4G     31.9G   73% /mnt/nfs03
#
```

Title:	How to Capture Packet via Tcpdump	Version:	v1.0	Date:	12/24/2019
Product:	IP Camera			Page:	4 of 6

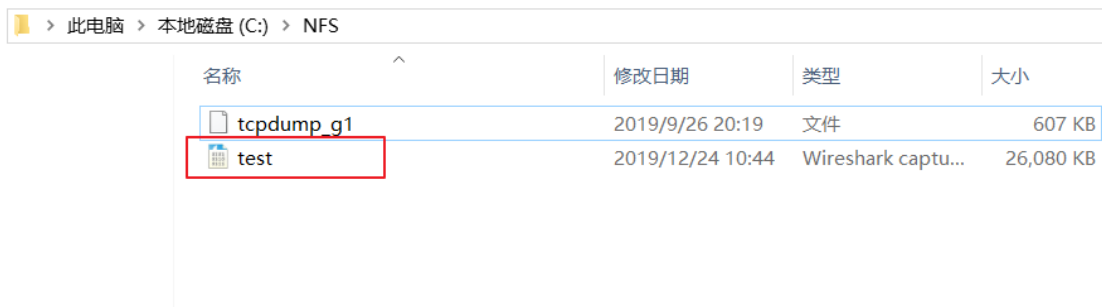
- 5) Copy the tcpdump file to “NFS” folder in step 1, following that, copy tcpdump to path “/home” of camera via command “**cp /mnt/nfs03/tcpdump /home**”.

```
# 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
```

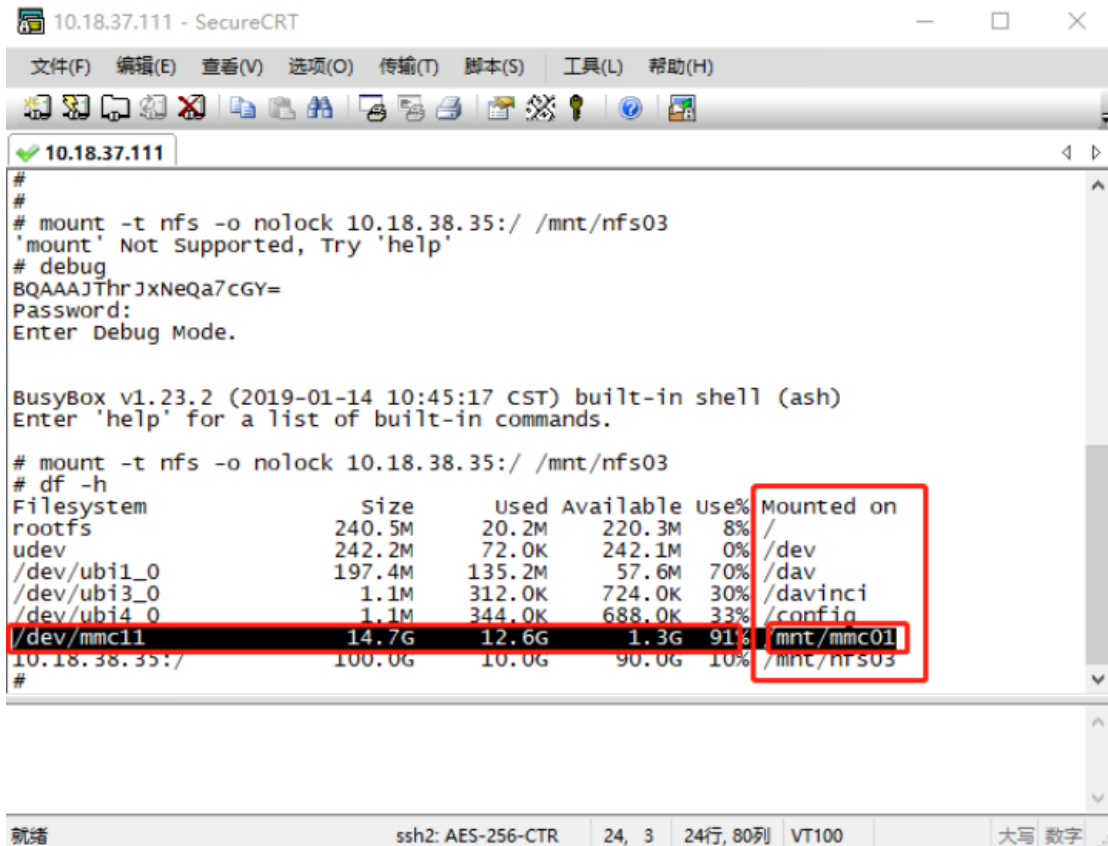


名称	修改日期	类型	大小
tcpdump_g1	2019/9/26 20:19	文件	607 KB
test	2019/12/24 10:44	Wireshark captu...	26,080 KB

Title:	How to Capture Packet via Tcpcdump	Version:	v1.0	Date:	12/24/2019
Product:	IP Camera			Page:	5 of 6

2. SD card capture

- 1) Copy tcpcdump 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.



```
10.18.37.111 - SecureCRT
文件(F) 编辑(E) 查看(V) 选项(O) 传输(T) 脚本(S) 工具(L) 帮助(H)
10.18.37.111
#
# mount -t nfs -o nolock 10.18.38.35:/ /mnt/nfs03
'mount' Not Supported, Try 'help'
# debug
BQAAAjThrjXNeQa7cGY=
Password:
Enter Debug Mode.

BusyBox v1.23.2 (2019-01-14 10:45:17 CST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

# mount -t nfs -o nolock 10.18.38.35:/ /mnt/nfs03
# df -h
Filesystem          Size      Used Available Use% Mounted on
rootfs              240.5M    20.2M    220.3M    8% /
udev                242.2M    72.0K    242.1M    0% /dev
/dev/ubi1_0         197.4M   135.2M    57.6M   70% /dav
/dev/ubi3_0          1.1M    312.0K    724.0K   30% /davinci
/dev/ubi4_0          1.1M    344.0K    688.0K   33% /config
/dev/mmc11          14.7G    12.6G     1.3G   91% /mnt/mmc01
10.18.38.35:/       100.0G    10.0G    90.0G   10% /mnt/nfs03
#
```

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



Title:	How to Capture Packet via Tcpdump	Version:	v1.0	Date:	12/24/2019
Product:	IP Camera			Page:	6 of 6

First Choice for Security Professionals
HIKVISION Technical Support