

wireshark + rvictl 配合 ios 抓包

[evil77](#) / 2017-10-23 09:11:39 / 浏览数 3950 [安全技术](#) [技术讨论](#) [顶\(0\)](#) [踩\(0\)](#)

作者：天才小三斤

```
sanjin — sanjin@SanJin-MacBook — ~ — -zsh — 80x24
Last login: Mon Jun 19 11:38:14 on ttys003
[➔ ~ rvictl -h]

Remote Virtual Interface Tool starts and stops a remote packet capture instance
for any set of attached mobile devices. It can also provide feedback on any atta
ched
devices that are currently relaying packets back to this host.

Options:
    -l, -L      List currently active devices
    -s, -S      Start a device or set of devices
    -x, -X      Stop a device or set of devices

➔ ~ _
```

命令介绍

```
-l , -L ■■■■■■■■
-s , -S ■■■■
-x , -X ■■■■
```

使用说明

添加设备

```
# ■■■■ usb ■ ■■■■
# UDID ■■■■ iTunes ■■■■
rvictl -s c32c775e43ed1fde9b5f475db6299062eb9911f3
```

查看设备

```
rvictl -l
```

ifconfig

设备一般 rvi 开头

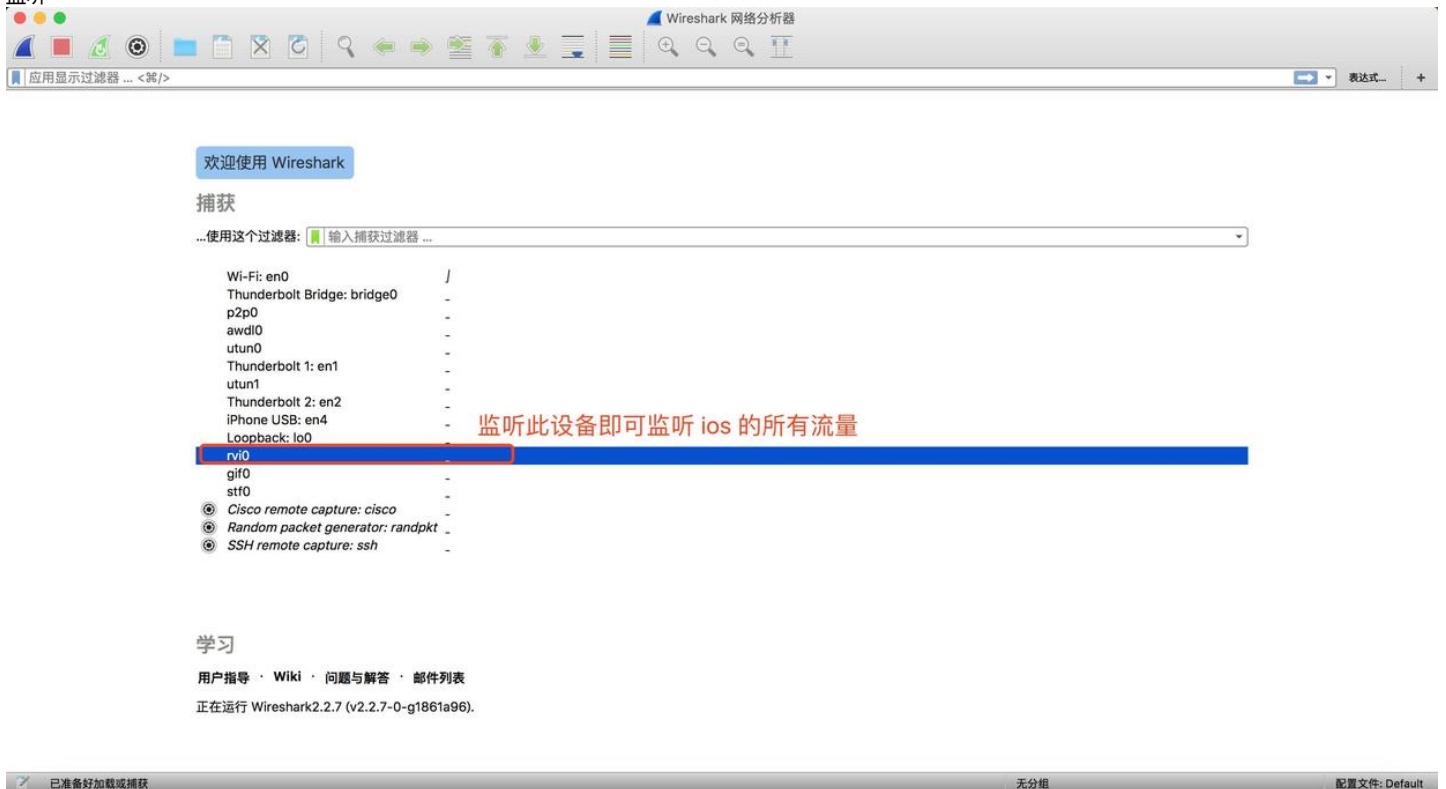
```
sanjin — sanjin@SanJin-MacBook — ~ — -zsh — 80x24
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    ether 0e:bc:32:c7:84:2d
    media: autoselect
    status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
    ether 62:62:a0:6e:c2:cf
    inet6 fe80::6062:a0ff:fe6e:c2cf%awdl0 prefixlen 64 scopeid 0x9
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect
    status: active
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
    inet6 fe80::6584:678f:f7d4:194f%utun0 prefixlen 64 scopeid 0xa
    nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
    inet6 fe80::f2f2:c5d3:adf2:d221%utun1 prefixlen 64 scopeid 0xd
    nd6 options=201<PERFORMNUD,DAD>
rvi0: flags=3005<UP,DEBUG,LINK0,LINK1> mtu 0
en4: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 66:b0:a6:bc:80:e5
    inet6 fe80::1ca4:7c52:9d11:1937%en4 prefixlen 64 secured scopeid 0xc
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect (100baseTX <full-duplex>)
    status: active
```

移除设备

UDID

rvictl -x c32c775e43ed1fde9b5f475db6299062eb9911f3

监听



点击收藏 | 0 关注 | 0

[上一篇：蜜罐与内网安全从0到1（三）](#) [下一篇：运用 iptables 限制同一I...](#)

1. 0 条回复
- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

目录

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)