**Linux 802.11n Csi Tool**

**官方文档地址：**http://dhalperi.github.io/linux-80211n-csitool/

**硬件环境：**

华硕笔记本A（接收端）：

处理器：Inter® Core™ i5-4200

内存：8G

网卡：Inter5300

华硕笔记本B（发送端）：

处理器：Inter® Core™ i7-4720

内存：4G

网卡：Inter5300

**软件环境：**

Ubuntu Server14.04系统（内核版本在3.2-4.2之间）

查看Linux内核版本命令：**$ uname -a**

Linux 802.11n CSI Tool（包含编译安装过Ubuntu系统内核对应版本的网卡驱动与编译过的固件）

**配置过程：**

1、安装当前版本的GCC：

**$ sudo apt-get install gcc make linux-headers-$(uname -r) git-core**

2、编译并安装修改过的驱动程序：

**$ CSITOOL\_KERNEL\_TAG=csitool-$(uname -r | cut -d . -f 1-2)**

**$ git clone <https://github.com/dhalperi/linux-80211n-csitool.git>**

**$ cd linux-80211n-csitool**

**$ git checkout ${CSITOOL\_KERNEL\_TAG}**

**Tip:** Git下载速度慢，你也可以在Github上下载适用你当前内核版本的源码压缩包（如果下载错误将无法编译）。编译并安装驱动。

编译：

**$ sudo make -C /lib/modules/$(uname -r)/build M=$(pwd)/drivers/net/wireless/iwlwifi modules**

安装：

**$ sudo make -C /lib/modules/$(uname -r)/build M=$(pwd)/drivers/net/wireless/iwlwifi INSTALL\_MOD\_DIR=updates \**

**modules\_install**

**$ sudo depmod**

**$ cd ..**

**Tip**：如果编译出现 "Can't read private key"错误，请在**/etc/default/grub**文件内将**GRUB\_CMDLINE\_LINUX\_DEFAULT=””**改为**GRUB\_CMDLINE\_LINUX\_DEFAULT=”enforcemodulesig=0”**

3、安装修改过的固件：

**$ git clone <https://github.com/dhalperi/linux-80211n-csitool-supplementary.git>**

备份当前固件：

**$ for file in /lib/firmware/iwlwifi-5000-\*.ucode; do sudo mv $file $file.orig; done**

**安装：**

**$ sudo cp linux-80211n-csitool-supplementary/firmware/iwlwifi-5000-2.ucode.sigcomm2010 /lib/firmware/**

**$ sudo ln -s iwlwifi-5000-2.ucode.sigcomm2010 /lib/firmware/iwlwifi-5000-2.ucode**

4、安装编译injection工具：

安装libcap-dev：

**$ sudo apt-get install libpcap-dev**

克隆编译LORCON：

**$ git clone <https://github.com/dhalperi/lorcon-old.git>**

**$ cd lorcon-old**

**$ sudo make install**

**$ sudo cd ..**

**$ cd linux-80211n-csitool-supplementary/injection/**

**$ sudo make**

**开始injection与monitor模式实验：**

笔记本A（接收端）：

卸载当前驱动：

**$ modprobe -r iwlwifi mac80211 cfg80211**

重新加载驱动：

**$ modprobe iwlwifi connector\_log=0x1**

接收端网络配置：

**$ iwconfig wlan0 mode monitor 2>/dev/null 1>/dev/null**

**$ ifconfig wlan0 up**

**$ iw wlan0 set channel 64 HT20**

开始接收数据：

**$ cd linux-80211n-csitool-supplementary/injection/**

**$ sudo ../netlink/log\_to\_file log.dat**

**Tip**：log.dat用来存接收的数据，可以自行修改，格式为\*.dat。

笔记本B（发送端）：

卸载当前驱动：

**$ modprobe -r iwlwifi mac80211 cfg80211**

重新加载驱动：

**$ modprobe iwlwifi debug=0x40000**

发送端网络配置：

**$ ifconfig wlan0 2>/dev/null 1>/dev/null**

**$ iw dev wlan0 interface add mon0 type monitor**

**$ ifconfig mon0 up**

**Tip**：“mon0”不可修改。

**$ iw mon0 set channel 64 HT20**

开始发送数据：

**$ cd linux-80211n-csitool-supplementary/injection/**

echo 0x4101 | sudo tee `find /sys -name monitor\_tx\_rate`

**$ sudo ./rander\_packets 360 100 1 500000**

**Tip**：”360”是包的数量，100是包的Size，500000是微秒数，每0.5秒发送一次数据，整个实验持续3分钟。