

WiFi capture and injection on various Oses revisited

Thomas d'Otreppe

SharkFest '16 • Computer History Museum • June 13-16, 2016

whoami

- Security researcher
- Author of Aircrack-ng
- Created Offensive Security Wireless Attacks aka WiFu
- Software developer @ MainNerve



Agenda

- What's monitor mode?
- Linux
- Windows
- BSD
- OSX
- Android
- Demos



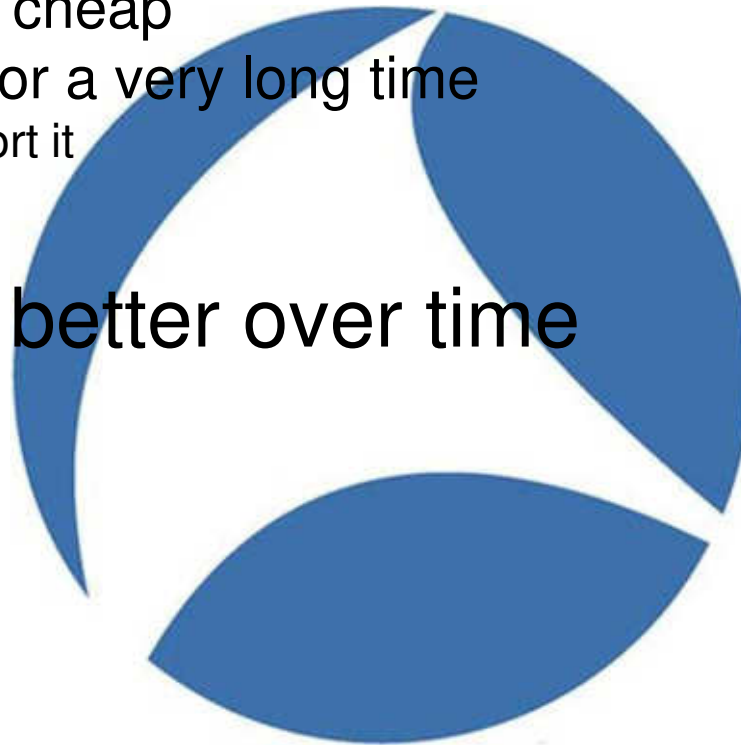
What's that?

- Monitor (aka RF Mon) mode is awesome
- Packet injection is awesomer



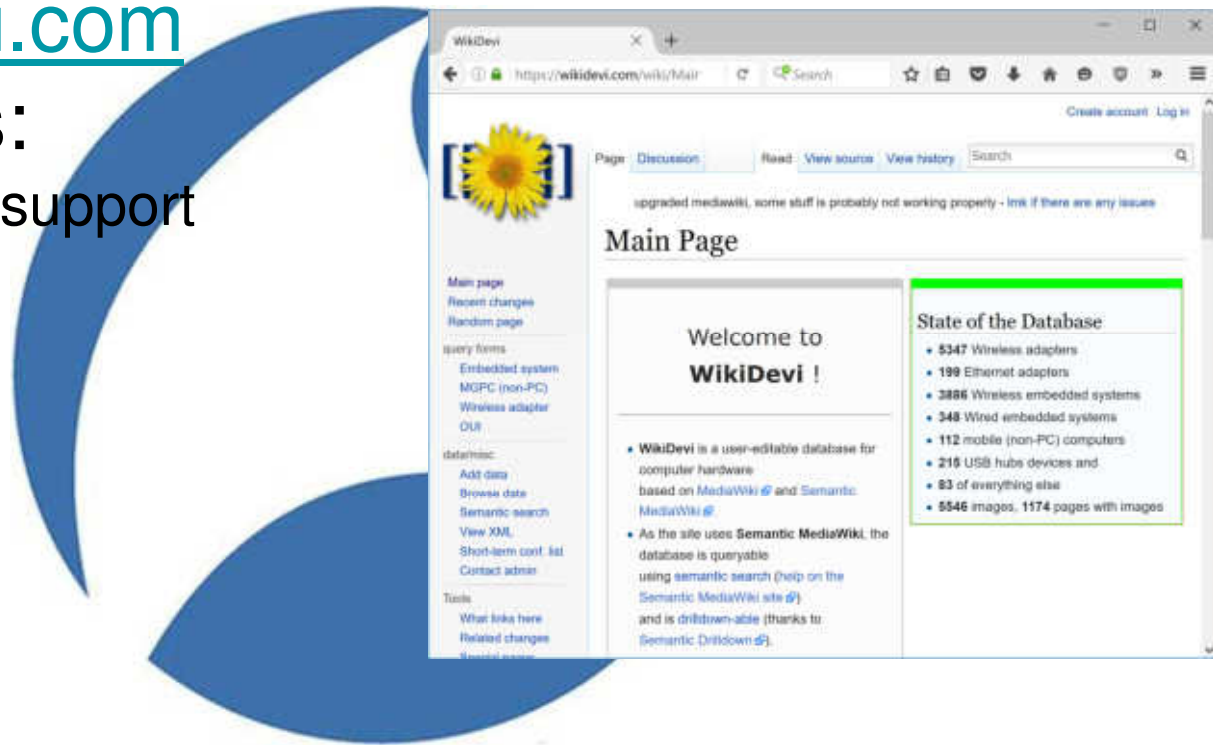
Linux

- **Most popular platform**
 - WiFi adapters are cheap
 - Has had support for a very long time
 - Lots of tools support it
- **WiFi stack got better over time**
 - Custom
 - ieee80211
 - mac80211



Adapter support

- Most of them (if not too new)
- <https://wikidevi.com>
- Vendor drivers:
 - No monitor mode support
 - **Never, ever**



Tools

- Aircrack-ng
- Wireshark
- Kismet
- Tcpdump
- Dumpcap
- A lot more...



Enable monitor mode

Enable monitor mode

1. `airmon-ng check kill`
2. `airmon-ng start wlan0`

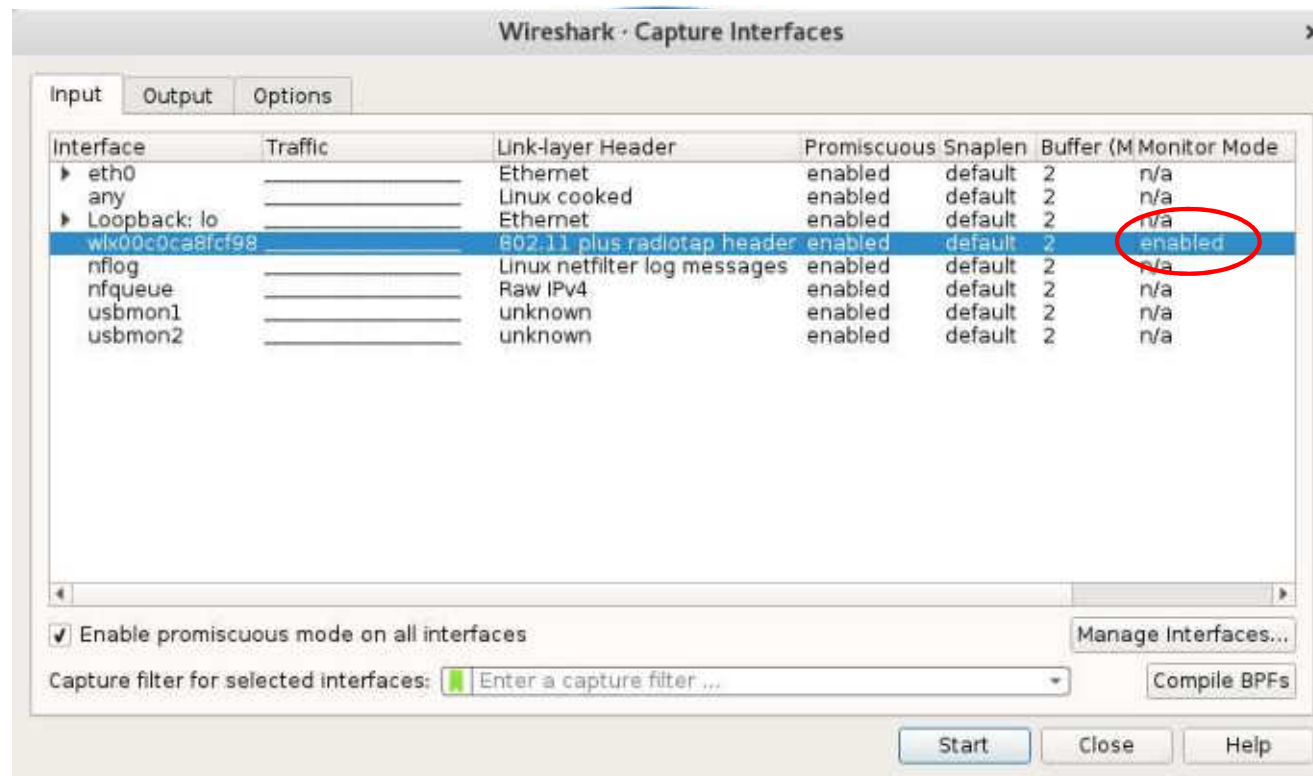
Start capturing

- `airodump-ng wlan0mon`



Wireshark

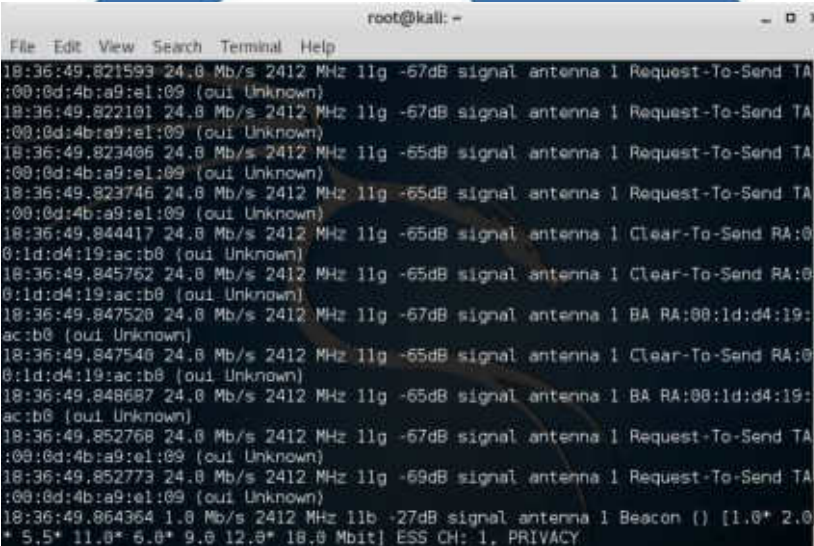
- Capture → Options



SharkFest '16 • Computer History Museum • June 13-16, 2016

tcpdump and others

- As root, use `-I` to put interface in monitor mode
 - `tcpdump -I -i wlan0`
 - `dumcap -I wlan0`
 - `tshark -I -i wlan0`



```
root@kali: ~  
File Edit View Search Terminal Help  
18:36:49.821593 24.8 Mb/s 2412 MHz 11g -67dB signal antenna 1 Request-To-Send TA  
:00:0d:4b:a9:e1:09 (oui Unknown)  
18:36:49.822101 24.8 Mb/s 2412 MHz 11g -67dB signal antenna 1 Request-To-Send TA  
:00:0d:4b:a9:e1:09 (oui Unknown)  
18:36:49.823406 24.8 Mb/s 2412 MHz 11g -65dB signal antenna 1 Request-To-Send TA  
:00:0d:4b:a9:e1:09 (oui Unknown)  
18:36:49.823746 24.8 Mb/s 2412 MHz 11g -65dB signal antenna 1 Request-To-Send TA  
:00:0d:4b:a9:e1:09 (oui Unknown)  
18:36:49.844417 24.8 Mb/s 2412 MHz 11g -65dB signal antenna 1 Clear-To-Send RA:0  
0:1d:d4:19:ac:b0 (oui Unknown)  
18:36:49.845762 24.8 Mb/s 2412 MHz 11g -65dB signal antenna 1 Clear-To-Send RA:0  
0:1d:d4:19:ac:b0 (oui Unknown)  
18:36:49.847520 24.8 Mb/s 2412 MHz 11g -67dB signal antenna 1 BA RA:00:1d:d4:19:  
ac:b0 (oui Unknown)  
18:36:49.847540 24.8 Mb/s 2412 MHz 11g -65dB signal antenna 1 Clear-To-Send RA:0  
0:1d:d4:19:ac:b0 (oui Unknown)  
18:36:49.848607 24.8 Mb/s 2412 MHz 11g -65dB signal antenna 1 BA RA:00:1d:d4:19:  
ac:b0 (oui Unknown)  
18:36:49.852768 24.8 Mb/s 2412 MHz 11g -67dB signal antenna 1 Request-To-Send TA  
:00:0d:4b:a9:e1:09 (oui Unknown)  
18:36:49.852773 24.8 Mb/s 2412 MHz 11g -69dB signal antenna 1 Request-To-Send TA  
:00:0d:4b:a9:e1:09 (oui Unknown)  
18:36:49.864364 1.0 Mb/s 2412 MHz 11b -27dB signal antenna 1 Beacon () [1.0* 2.0  
* 5.5* 11.0* 6.0* 9.0 12.0* 18.0 Mbit] ESS CH: 1, PRIVACY
```

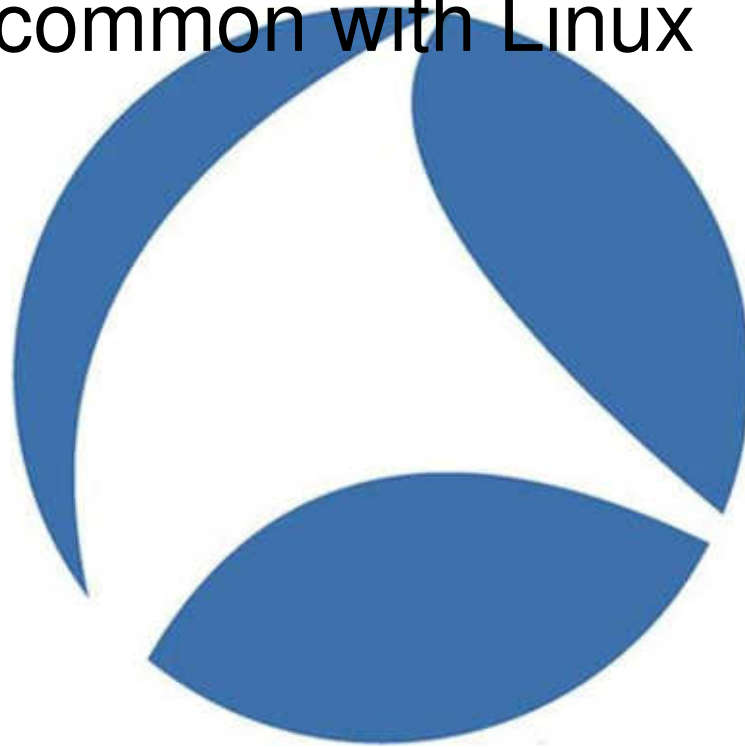
Wireshark, tcpdump and others

- Sometimes monitor mode/changing link layer (to 802.11) fails.
 - Exit and try again, it will work



Windows

- Getting better
- Some tools in common with Linux



Windows - Hardware

	Savvius aka Wildpackets	Riverbed Airpcap	Npcap	Acrylic WiFi Professional
API	No	Yes	Yes	No
License	Commercial	Commercial	Open source	Commercial
Adapter	Custom	Custom	Any*	Airpcap/Others**
Compatibility	Wildpackets only	Wireshark, commercial and open source	Wireshark	Airodump-ng
802.11	ac	n	depends	Depends
Packet injection	No	Yes	No	No
Monitor mode	GUI	GUI	Command line	Automatic (GUI)

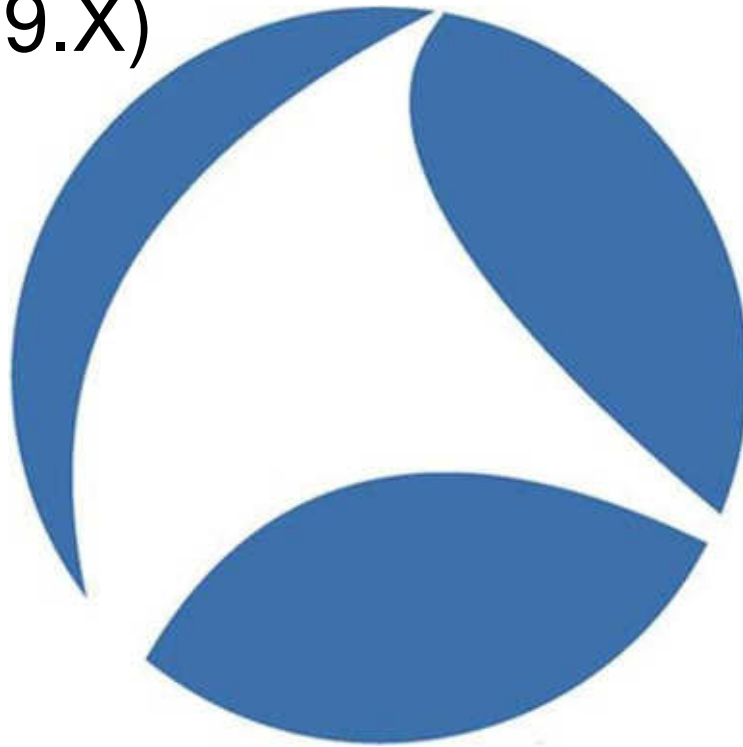
* All drivers have monitor mode but hit and miss

** <https://www.acrylicwifi.com/en/support/compatible-hardware/>

SharkFest '16 • Computer History Museum • June 13-16, 2016

Windows – Open source

- Wireshark
- Aircrack-ng (0.9.X)
- Kismet
- Cain and Abel

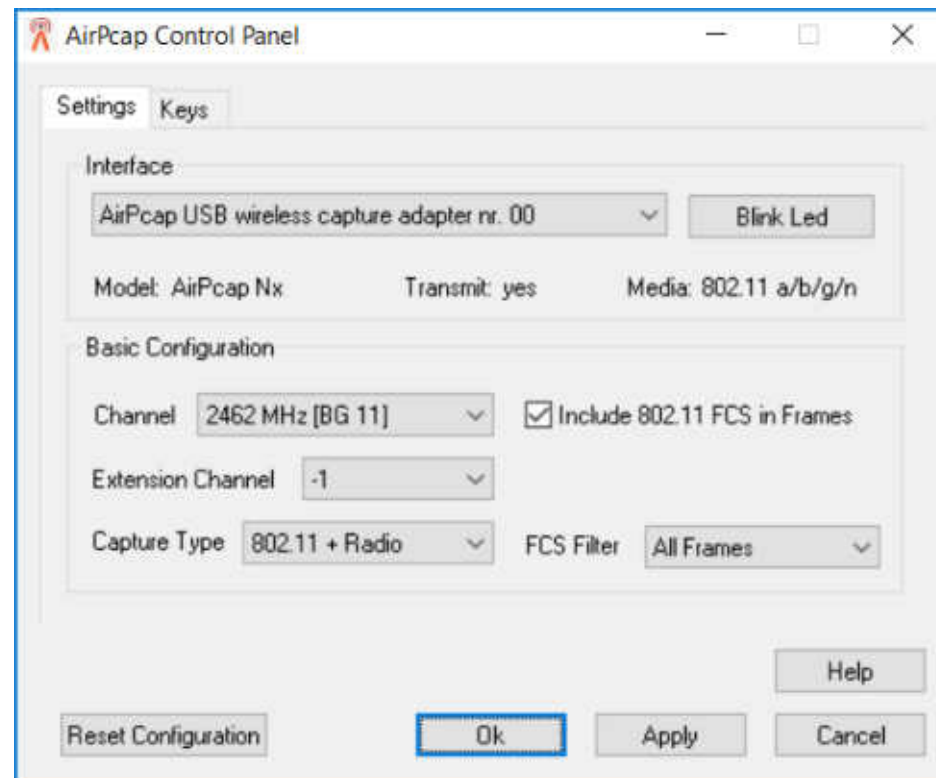


Windows – Closed source

- Riverbed Steelcentral
- Microsoft Network Monitor
- Elcomsoft Wireless Network Auditor
- Commview For WiFi



Enable monitor mode - Airpcap



SharkFest '16 • Computer History Museum • June 13-16, 2016

Wireshark on Windows - Airpcap

Capturing from AirPcap USB wireless capture adapter nr. 00

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

*Apply a display filter ... <Ctrl-/> Expression...

Interface airpcap00 Channel 11 · 2.462 HT 40- FCS Filter AirPcap Control Panel 802.11 Preferences

No.	Time	Source	Destination	Protocol	Length	Info
5085	74.246939	Azurewav_7d:b8:e1	Broadcast	802.11	242	Beacon frame, SN=3657, FN=0, Flags=.....C, BI=100, SSID...
5086	74.249560	Azurewav_7d:b8:e1	Broadcast	802.11	54	Null function (No data), SN=3658, FN=0, Flags=.....F.C
5087	74.269081	Azurewav_7d:b8:e1	Broadcast	802.11	54	Null function (No data), SN=3659, FN=0, Flags=.....F.C
5088	74.289356	Azurewav_7d:b8:e1	Broadcast	802.11	54	Null function (No data), SN=3660, FN=0, Flags=.....F.C
5089	74.308826	Azurewav_7d:b8:e1	Broadcast	802.11	54	Null function (No data), SN=3661, FN=0, Flags=.....F.C
5090	74.328473	Azurewav_7d:b8:e1	Broadcast	802.11	54	Null function (No data), SN=3662, FN=0, Flags=.....F.C
5091	74.347613	Azurewav_7d:b8:e1	Broadcast	802.11	242	Beacon frame, SN=3663, FN=0, Flags=.....C, BI=100, SSID...
5092	74.350251	Azurewav_7d:b8:e1	Broadcast	802.11	54	Null function (No data), SN=3664, FN=0, Flags=.....F.C
5093	74.369730	Azurewav_7d:b8:e1	Broadcast	802.11	54	Null function (No data), SN=3665, FN=0, Flags=.....F.C
5094	74.389256	Azurewav_7d:b8:e1	Broadcast	802.11	54	Null function (No data), SN=3666, FN=0, Flags=.....F.C
5095	74.408674	Azurewav_7d:b8:e1	Broadcast	802.11	54	Null function (No data), SN=3667, FN=0, Flags=.....F.C

>Frame 3515: 54 bytes on wire (432 bits), 54 bytes captured on interface airpcap00

>Radiotap Header v0, Length 26

>802.11 radio information

>IEEE 802.11 Null function (No data), Flags:F.C

```
0000 00 00 1a 00 6f 18 00 00 bc 8f ce 5f 00 00 00 00 .....0... ..
0010 10 02 9e 09 a0 00 cc a7 00 25 48 02 68 42 ff ff .....%H.
0020 ff ff ff ff 80 d2 1d 7d b8 e1 80 d2 1d 7d b8 e1 .....} ....
0030 f0 88 e9 c1 cf bb .....

```

AirPcap USB wireless capture adapter nr. 00: <live capture in progress> Packets: 5095 · Displayed: 5095 (100.0%) Profile: Default

SharkFest '16 • Computer History Museum • June 13-16, 2016

Enable monitor mode - Npcap

```
Command Prompt
WlanHelper for Npcap 0.0/ ( http://npcap.org )
Usage: WlanHelper [Commands]
       or: WlanHelper {Interface Name or GUID} [Options]

OPTIONS:
mode                                     : Get interface operation mode
mode <managed|monitor|master|..>       : Set interface operation mode
modes                                    : Get all operation modes supported by the interface, comma separated
channel                                  : Get interface channel
channel <1-14>                           : Set interface channel (only works in monitor mode)
freq                                      : Get interface frequency
freq <VAIUHF>                             : Set interface frequency (only works in monitor mode)

COMMANDS:
-i                                       : Enter the interactive mode
-h                                       : Print this help summary page

OPERATION MODES:
managed      : The Extensible Station (ExtSTA) operation mode
monitor      : The Network Monitor (NetMon) operation mode
master       : The Extensible Access Point (ExtAP) operation mode (supported from Windows 7 and later)
wfd_device   : The Wi-Fi Direct Device operation mode (supported from Windows 8 and later)
wfd_owner    : The Wi-Fi Direct Group Owner operation mode (supported from Windows 8 and later)
wfd_client   : The Wi-Fi Direct Client operation mode (supported from Windows 8 and later)

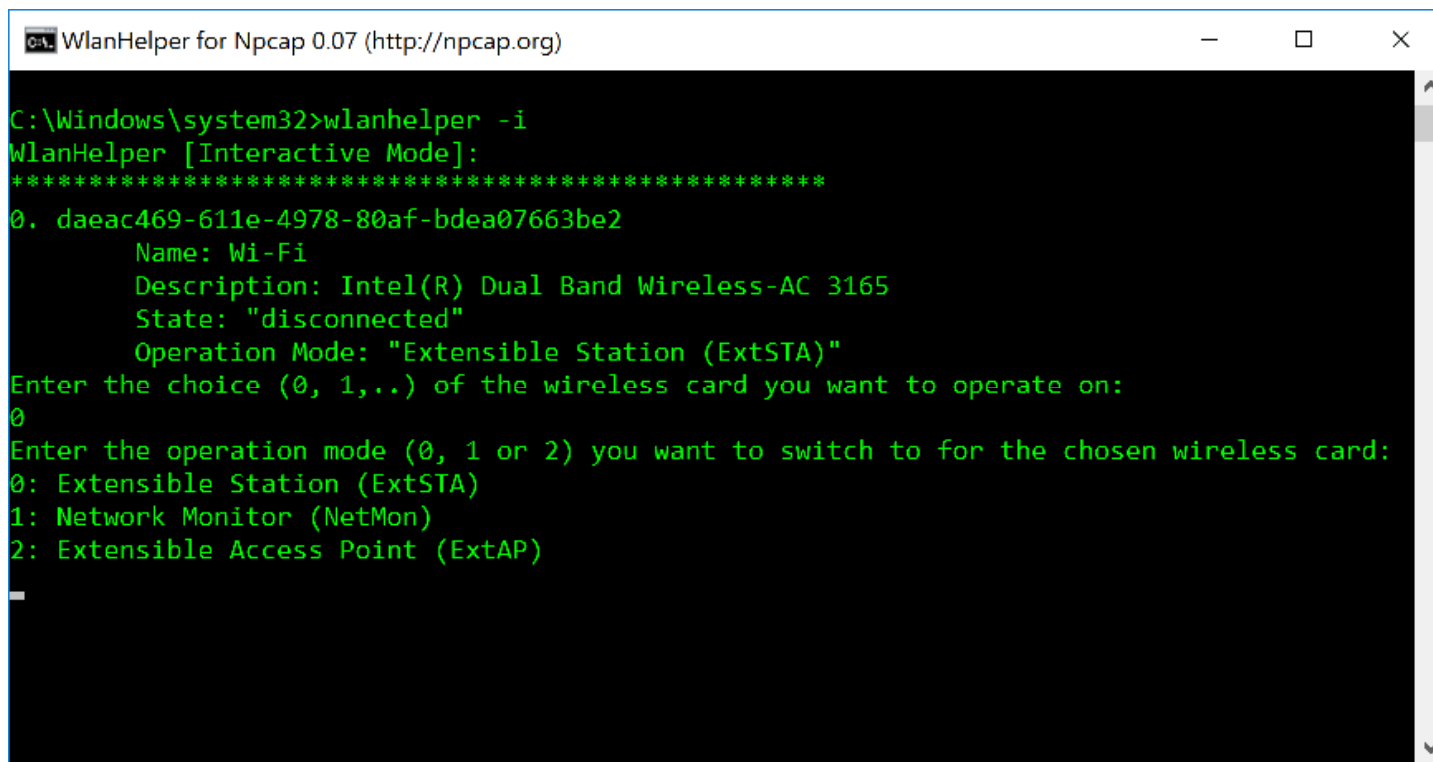
EXAMPLES:
WlanHelper Wi-Fi mode
WlanHelper 42dfd47a-2764-43ac-b58e-3df569c447da channel 11
WlanHelper 42dfd47a-2764-43ac-b58e-3df569c447da freq 7
WlanHelper "Wireless Network Connection" mode monitor

SEE THE MAN PAGE (https://github.com/nmap/ncap) FOR MORE OPTIONS AND EXAMPLES

C:\Users\Thomas>
```

Enable monitor mode - NPcap

- Run Command Prompt as Administrator



```
C:\Windows\system32>wlanhelper -i
WlanHelper [Interactive Mode]:
*****
0. daeac469-611e-4978-80af-bdea07663be2
   Name: Wi-Fi
   Description: Intel(R) Dual Band Wireless-AC 3165
   State: "disconnected"
   Operation Mode: "Extensible Station (ExtSTA)"
Enter the choice (0, 1,..) of the wireless card you want to operate on:
0
Enter the operation mode (0, 1 or 2) you want to switch to for the chosen wireless card:
0: Extensible Station (ExtSTA)
1: Network Monitor (NetMon)
2: Extensible Access Point (ExtAP)
-
```

NPcap - Notes

- Command line must be run as Administrator
- WiFi card must be enabled
- There can be only one
 - Airpcap or Npcap, you have to choose
- Still in beta, and releases often

BSD

- Similar support as in Linux in the mid-2000
- Limited driver and adapter support
 - Mostly old 802.11bg
- Not very well documented
- Different support depending on BSD flavor



FreeBSD/DragonflyBSD

- Use ifconfig to put interface in monitor mode
 - `ifconfig wlan create wlandev ${IFACE} wlanmode monitor`
- Monitor interface name has to be wlanX



FreeBSD/DragonflyBSD

- Use your favorite tool (Wireshark, Tcpdump, Aircrack-ng, Kismet)
- Airmon-ng has support for *ath* and *urtwn* drivers
 - Atheros
 - Realtek USB



FreeBSD - Notes

- Load drivers in */boot/loader.conf*
 - Realtek: `if_urtn_load="YES"`
 - Atheros: `if_ath_load="YES"`
- Accept Realtek license (*/boot/loader.conf*):
 - `legal.realtek.license_ack=1`
- Might not complain if firmware is not loaded
 - But will not give any packet
- For other drivers, look in man pages for info

FreeBSD/DragonflyBSD - Problems

- Injection is supposed to work in FreeBSD
- DragonflyBSD unstable
- Lots of other adapters supported but lots discontinued (or too old to be useful)



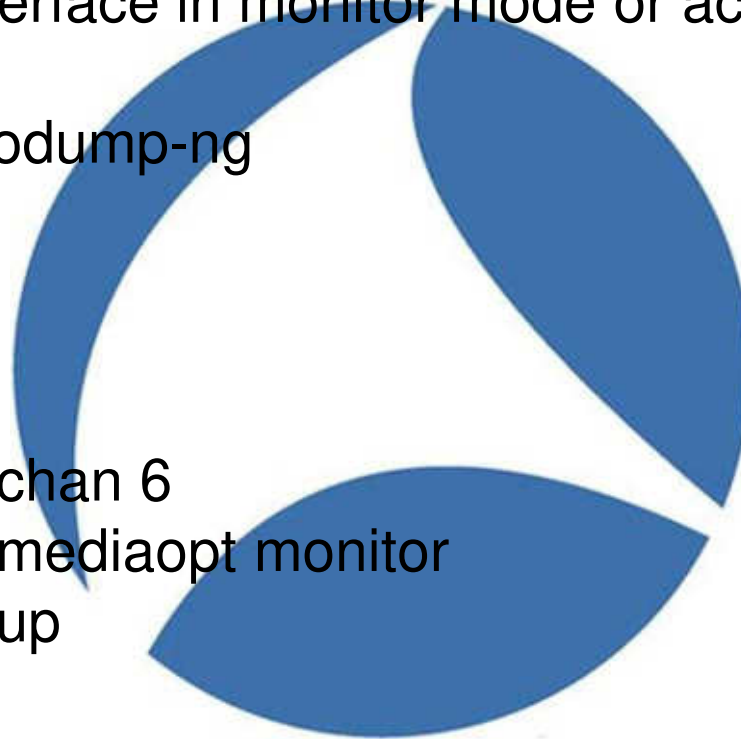
Other BSD flavor

- **NetBSD**

- No need to put interface in monitor mode or accept license and load driver
- Kinda laggy in Airodump-ng

- **OpenBSD**

- Seems unstable
- `ifconfig ${IFACE} chan 6`
- `ifconfig ${IFACE} mediaopt monitor`
- `ifconfig ${IFACE} up`



OS X

- Started in Tiger (10.4.0) and improved over time



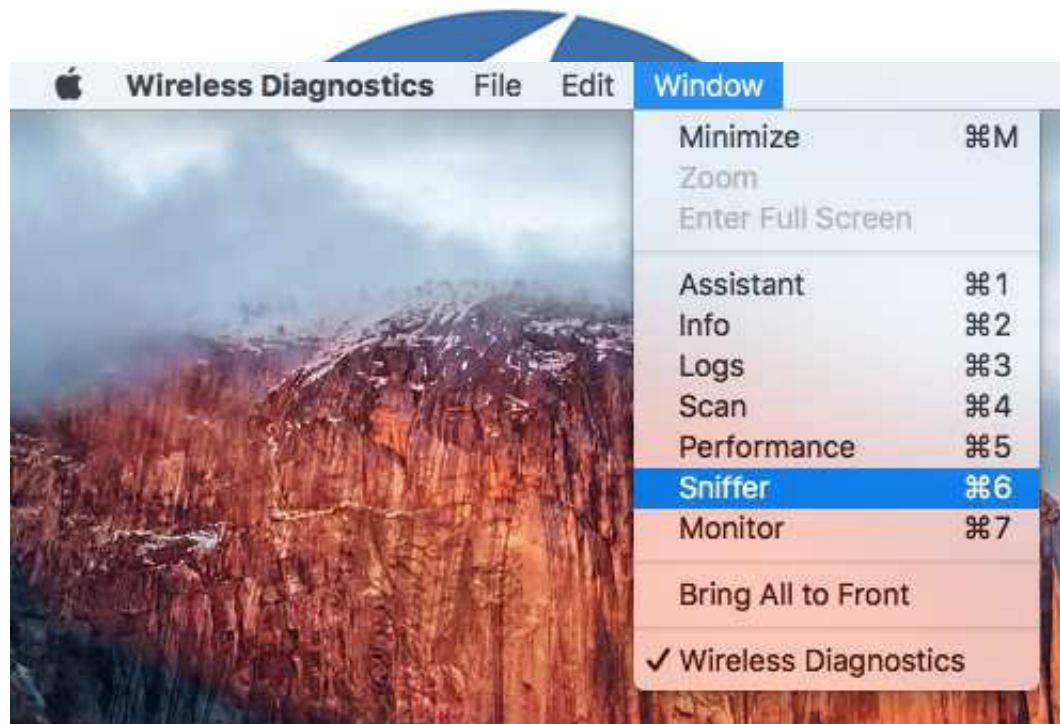
OS X – GUI

- Hold 'Option' key and click on the wireless icon
- Select 'Open Wireless Diagnostics...'



OS X – GUI

- Select ‘Sniffer’ in the ‘Window’ menu



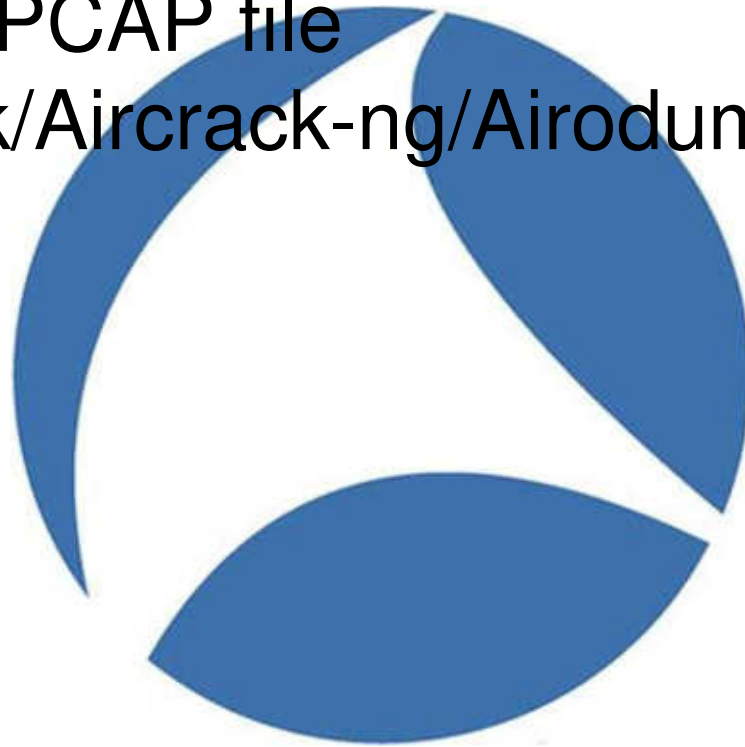
OS X – GUI



SharkFest '16 • Computer History Museum • June 13-16, 2016

OS X - GUI

- .wcap file on your desktop
- Just a regular PCAP file
- Use Wireshark/Aircrack-ng/Airodump-ng/...



OS X – Command line

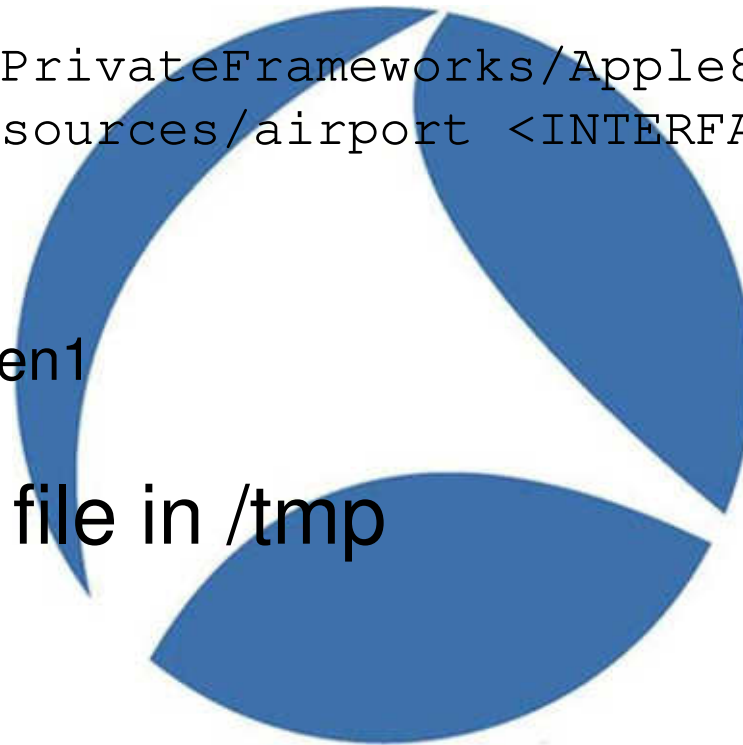
- **Command:**

```
sudo  
/System/Library/PrivateFrameworks/Apple80211.framework/Ver  
sions/Current/Resources/airport <INTERFACE> sniff  
<CHANNEL>
```

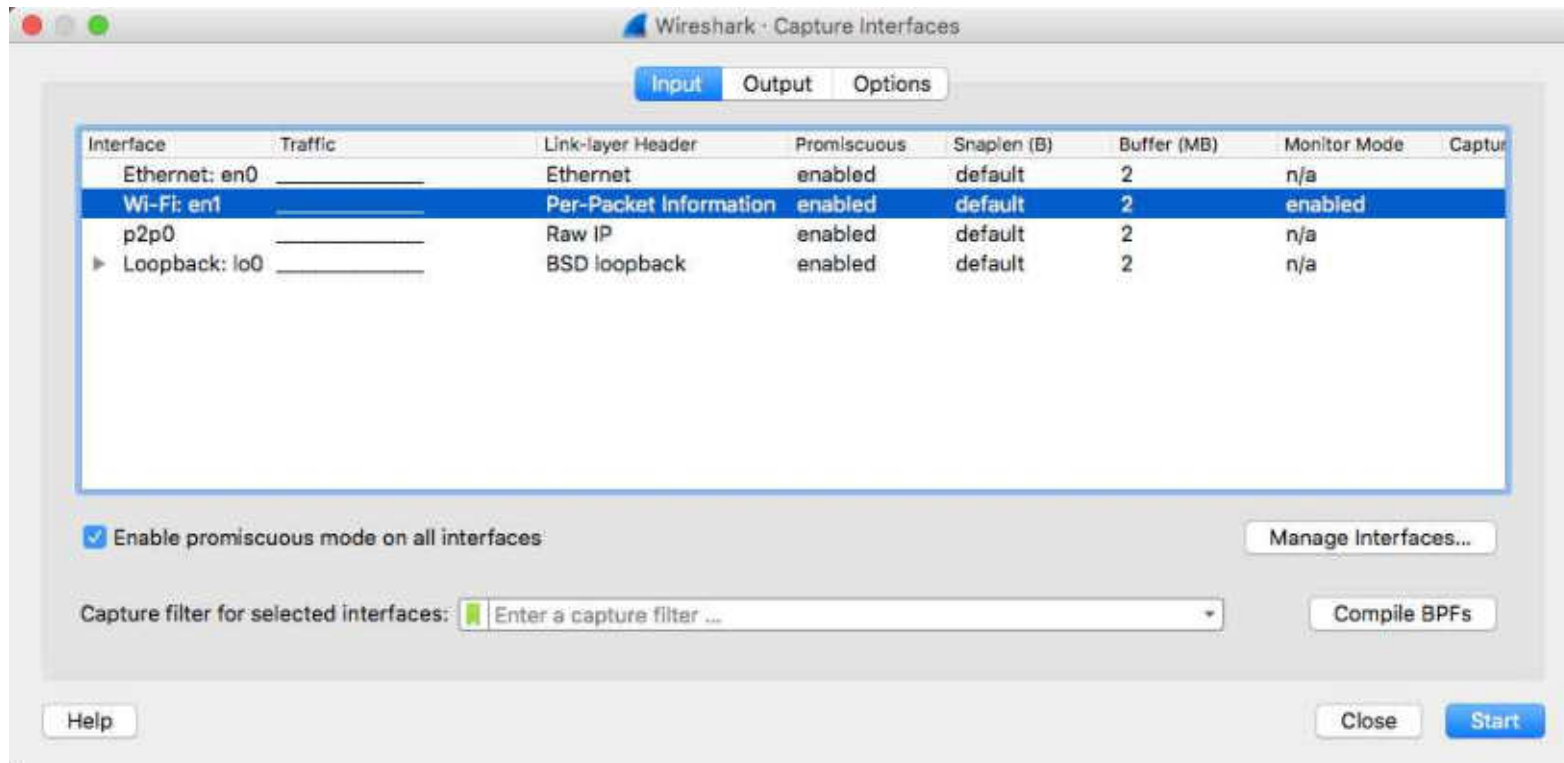
- **Parameters:**

- Interface: usually en1
- Channel

- **Output: PCAP file in /tmp**



OS X - Wireshark



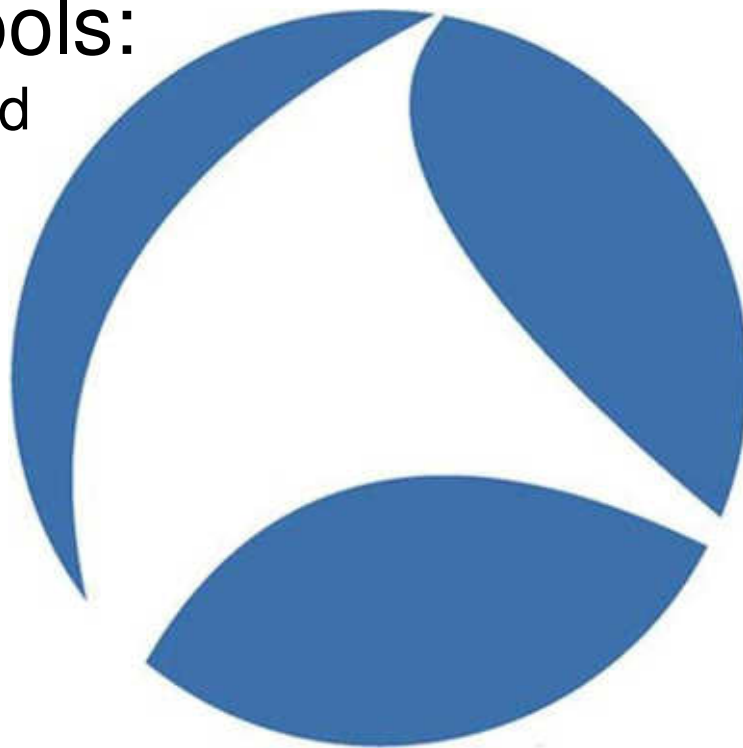
SharkFest '16 • Computer History Museum • June 13-16, 2016

OS X - Notes

- Wireshark Wireless toolbar doesn't allow changing settings → command line
- No live display or channel change while capturing with built-in GUI tools
- **Change channel:** `airport -cCHANNEL`
 - No channel validation/list in command line
 - No space between **c** and channel number

Android

- Wi-Fi PCAP Capture
- Other useful tools:
 - CloudShark upload
 - PCAP reader

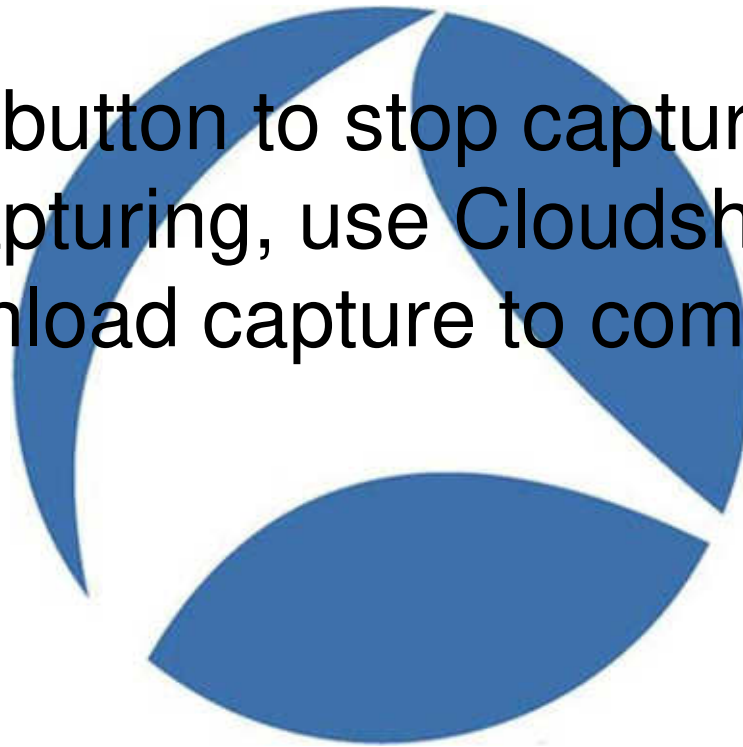


Android - Set-up

- Connect AWUS036H to a micro USB to USB female adapter to the device
- It will ask if you want to start the app when connecting adapter. Answer Yes.
- First time might fail. Exit, unplug adapter then plug it back

Android - Capture

- Select channel(s) then click on capture at the bottom.
- Use the same button to stop capture
- When done capturing, use Cloudshark, PCAP reader or download capture to computer



Demo

- **Windows**
 - Aircap
 - Npcap
- **Linux**
- **BSD**
- **Android**



Which OS has best support?

- One thing to remember:

- Even if a card says 802.11n or ac, it might not support capturing packets in this mode

- Ranked

1. Linux – Widest range of adapters/tools supported
2. Windows – Best adapter
3. OSX
4. FreeBSD (> DragonflyBSD > OpenBSD/NetBSD)
Android

What's the best adapter?

- Windows: Aircap
- Linux:
 - TP-Link WN722N
 - Alfa AWUS051NH v2
- FreeBSD
 - PCI/MiniPCI: Atheros 5xxx
 - USB: TEW-648UBM
- Android: Alfa AWUS036H



Resource

- Driver comparison:
https://en.wikipedia.org/wiki/Comparison_of_open-source_wireless_drivers
- Wireshark documentation:
<https://wiki.wireshark.org/CaptureSetup/WLAN>



That's all Folks!