

# nexmon

Enable monitor mode for the  
Nexus 5

{dwegemer, mschulz} @ seemoo.de  
nexmon.org

32c3

Please don't sue us!

# Monitor what?

nexmon

We need:

**802.11 Management, Control and Data frames**

**Promisc Mode:** get all frames on the ether, not only the ones which are addressed to us

# Why monitor mode on mobile phones?

nexmon

... to that

Move from this ...



Image Source: [icanhas.cheezburger.com](http://icanhas.cheezburger.com)

# Related Work

nexmon

BCMON: bcm4329 + bcm4330



monmob: bcm4325 + bcm4329



nexmon: bcm4339

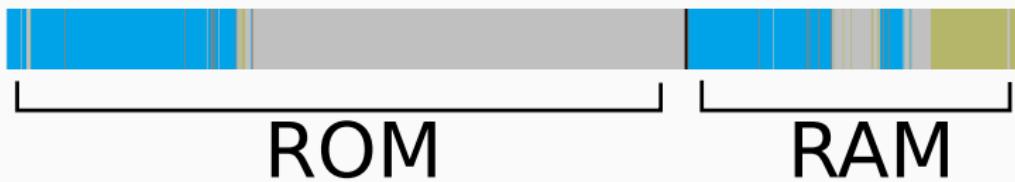


Image Source: ifixit.com

# DIY: 384 easy steps to enable monitor mode

nexmon

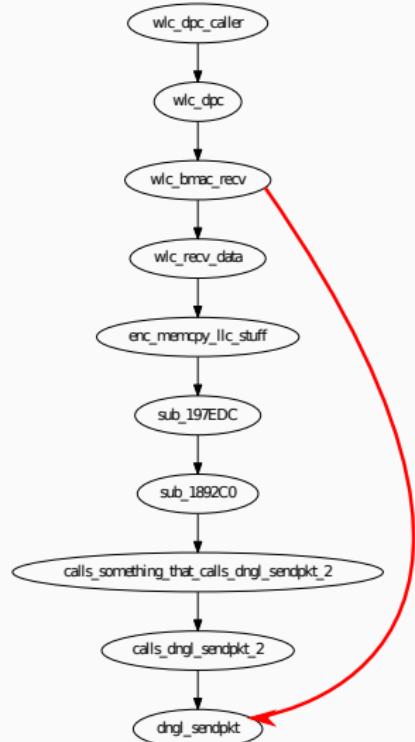
1. Extract ROM + RAM



# DIY: 384 easy steps to enable monitor mode

nexmon

## 2. Find the RX path



# DIY: 384 easy steps to enable monitor mode

nexmon

### 3. Patch necessary parts:

## Frame handler: **wlc\_bmac\_recv()**

## MAC control flags: `wlc_coreinit()`

# DIY: 384 easy steps to enable monitor mode

nexmon

## 379. Write binary patches in C:

```
int wlc_bmac_recv(struct wlc_hw_info *wlc_hw, uint fifo, bool bound, int *cnt) {
    struct sk_buff *p;
    while( (p = dma_rx (wlc_hw->di[fifo])) ) {
        dngl_sendpkt(SDIO_INFO_ADDR, p, 0xF);
    }
    dma_rxfill(wlc_hw->di[fifo]);
    return 0;
}
```

TX path: **injection support**

**Fix Radiotap header:** set RSSI / channel information

**Improve stability**

**Code + Android boot ROM:**  
[nexmon.org](http://nexmon.org)

**Read our technical report:**

*NexMon: A Cookbook for Firmware  
Modifications on Smartphones to Enable  
Monitor Mode* (available at [nexmon.org](http://nexmon.org))

**Contact:**

*Daniel Wegemer:*

dwegemer@seemoo.de; talk to me;  
call me via DECT/GSM (2412/2414)

*Matthias Schulz:*

mschulz@seemoo.de