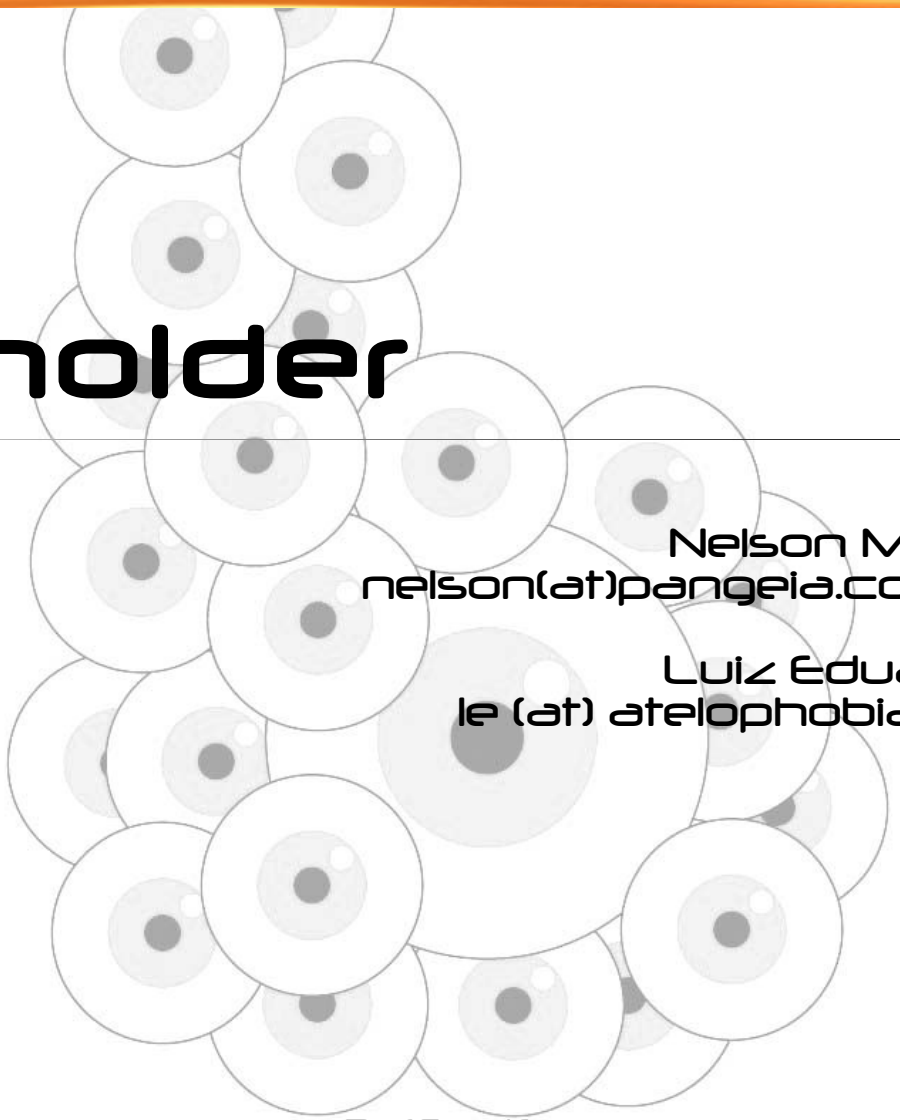


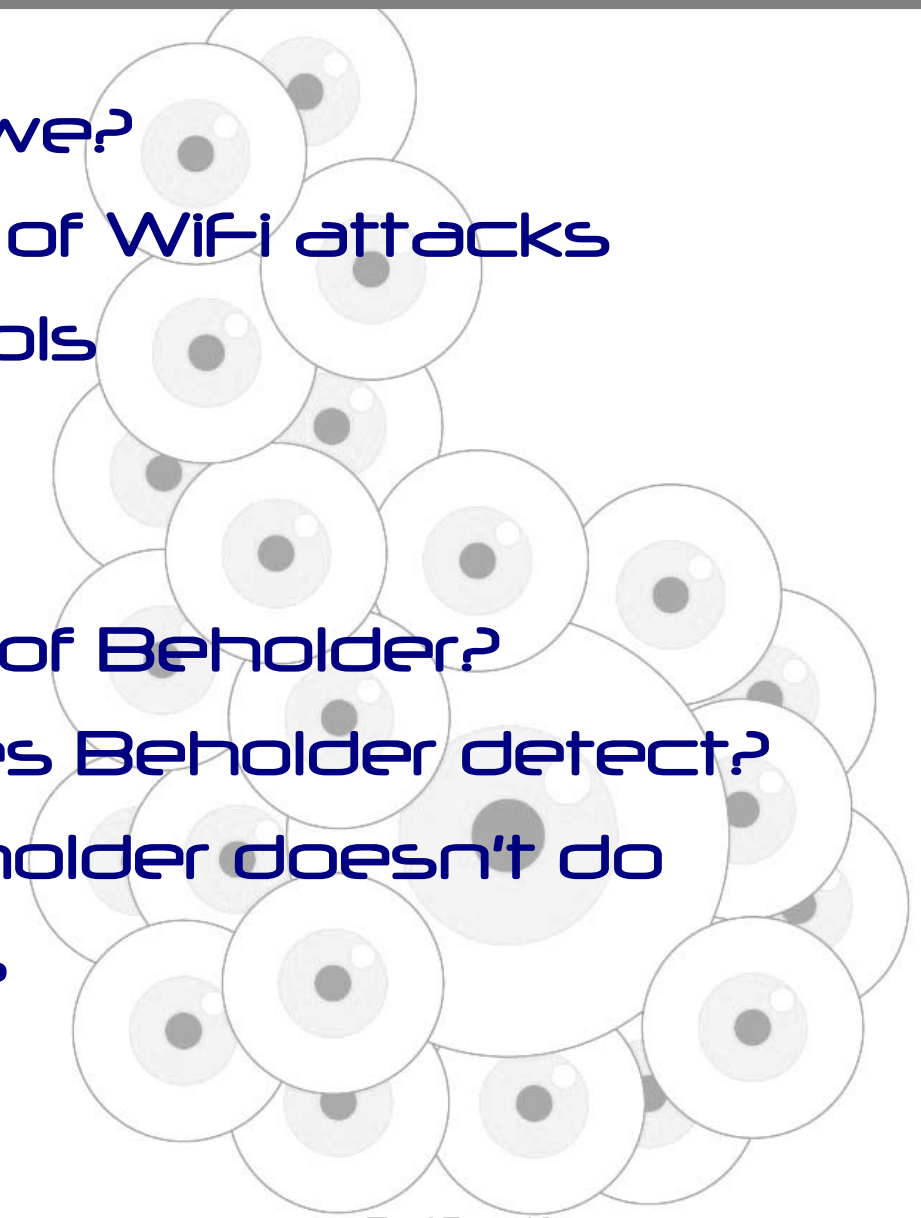
Beholder



Nelson Murilo
nelson(at)pangeia.com.br

Luiz Eduardo
le (at) atelophobia.net

Agenda



- Who are we?
- Evolution of WiFi attacks
- Attack tools
- Threats
- Solutions
- The inner of Beholder?
- What does Beholder detect?
- What Beholder doesn't do
- Scenarios
- Futures

Wi-Fi Attacks





DoS



MiTM

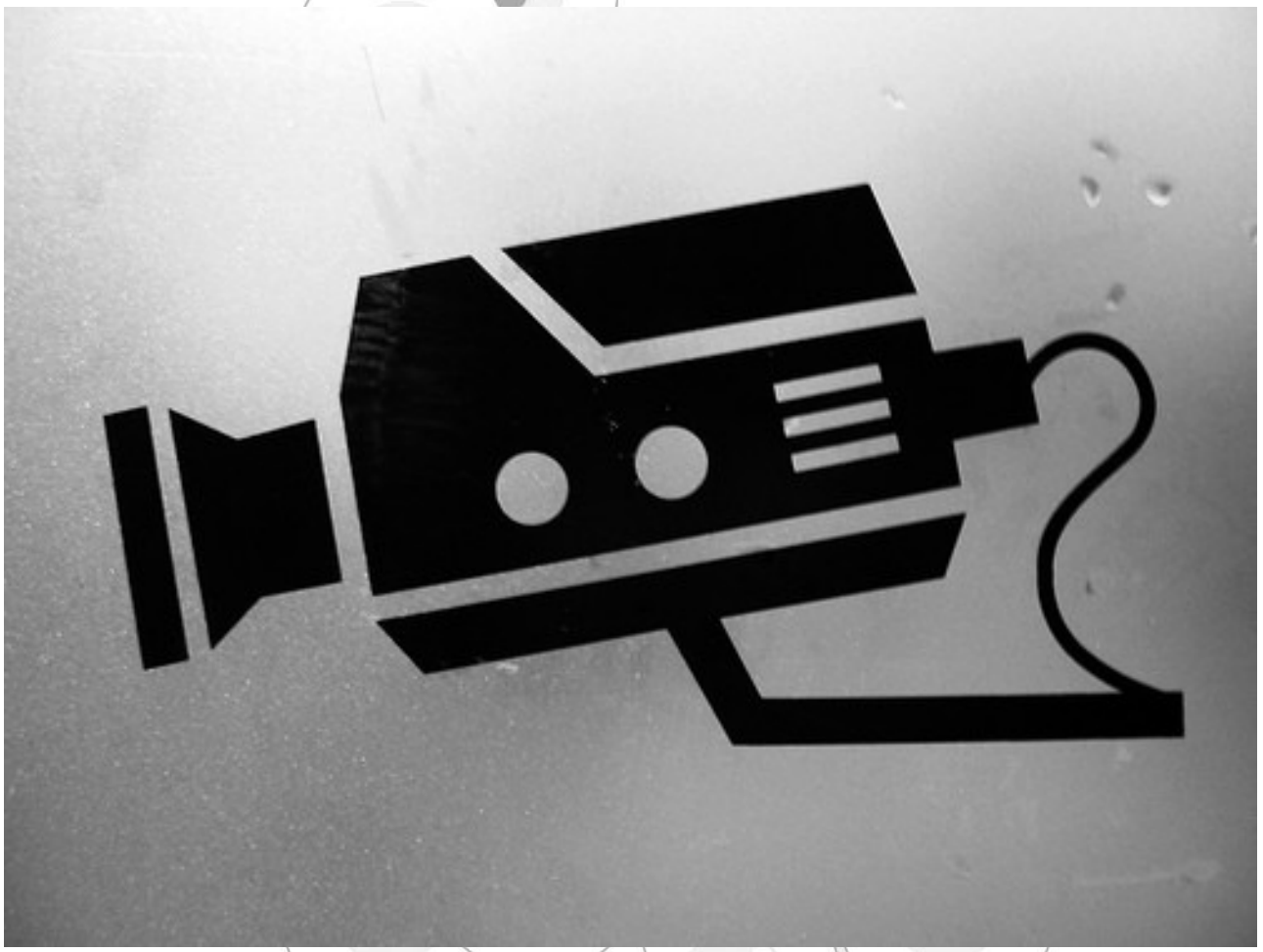


Impersonation





Surveillance

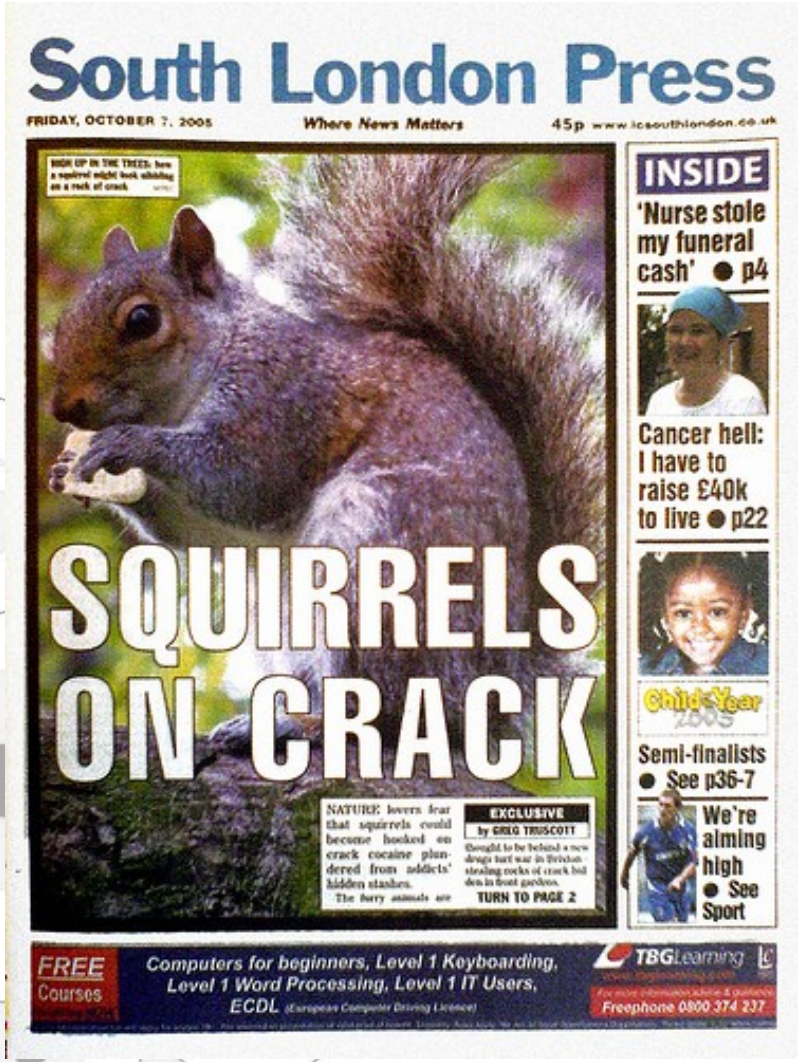


Packet Injection



Crypto Cracking

- WEP
- WPA



Client-Side

- AdHocs Circa

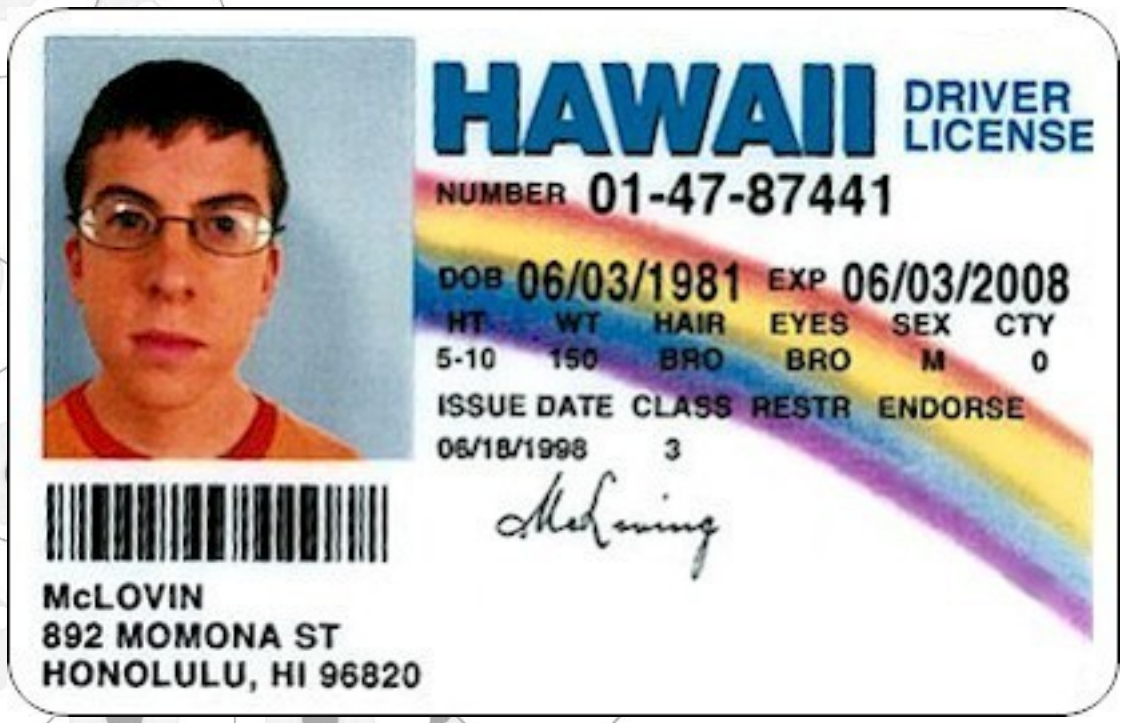


Rogue APs



Impersonation 2.0

- Evil-twin
- More rogue-aps



Drive-By Pharming



Faster Crypto-Cracking



Rogue Radius Servers



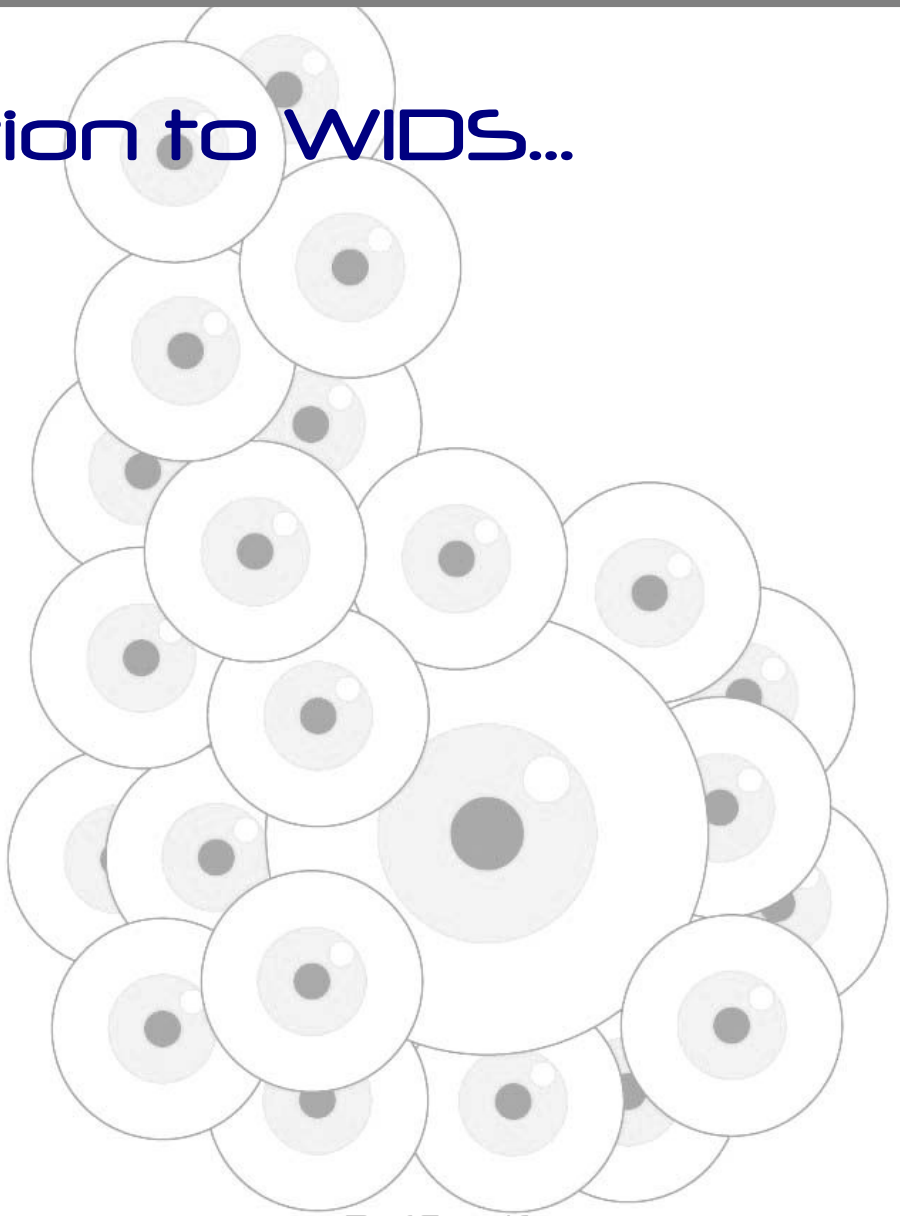
Tools

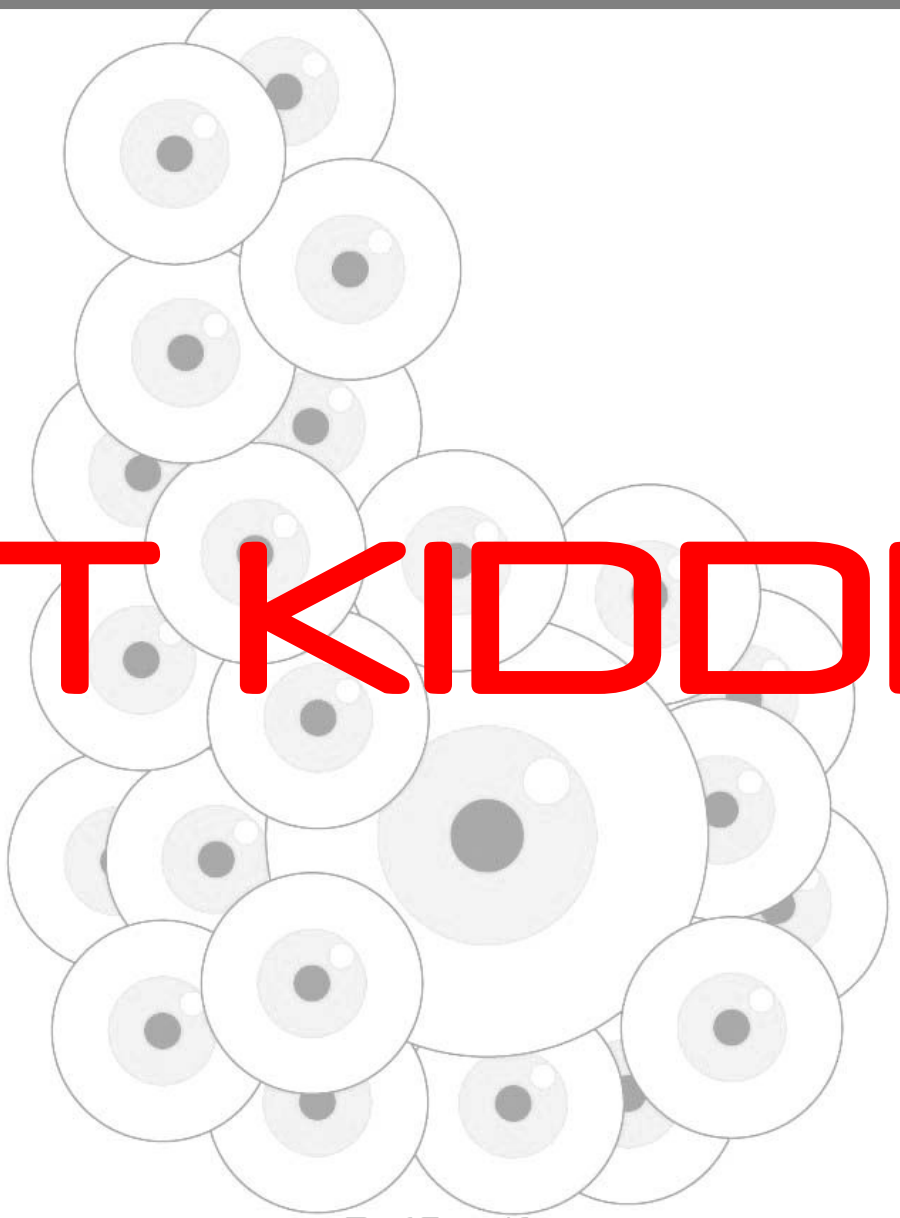



©2002 DRAGONICAHN

Solutions?

- Introduction to WIDS...





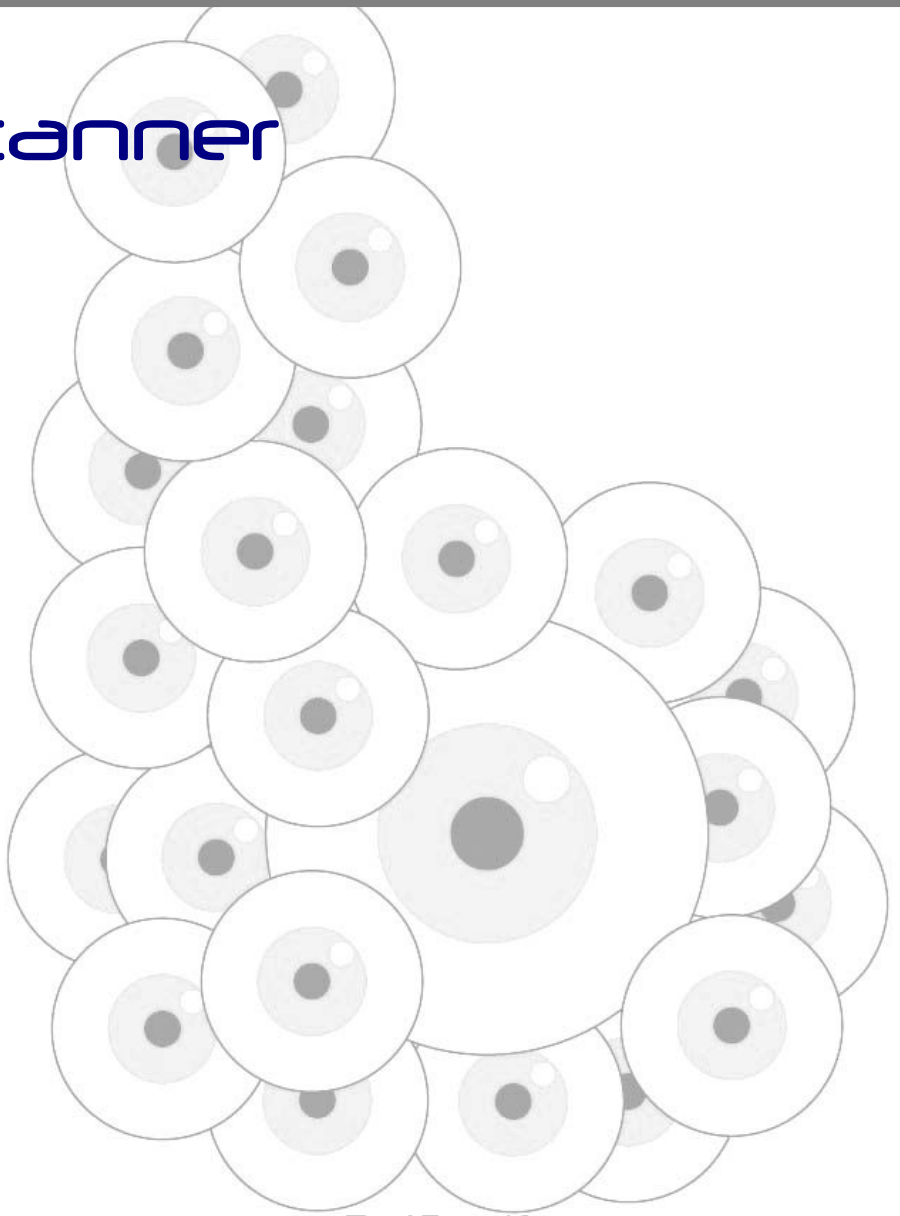
JUST KIDDING!

State of WIDS
(not the one below)



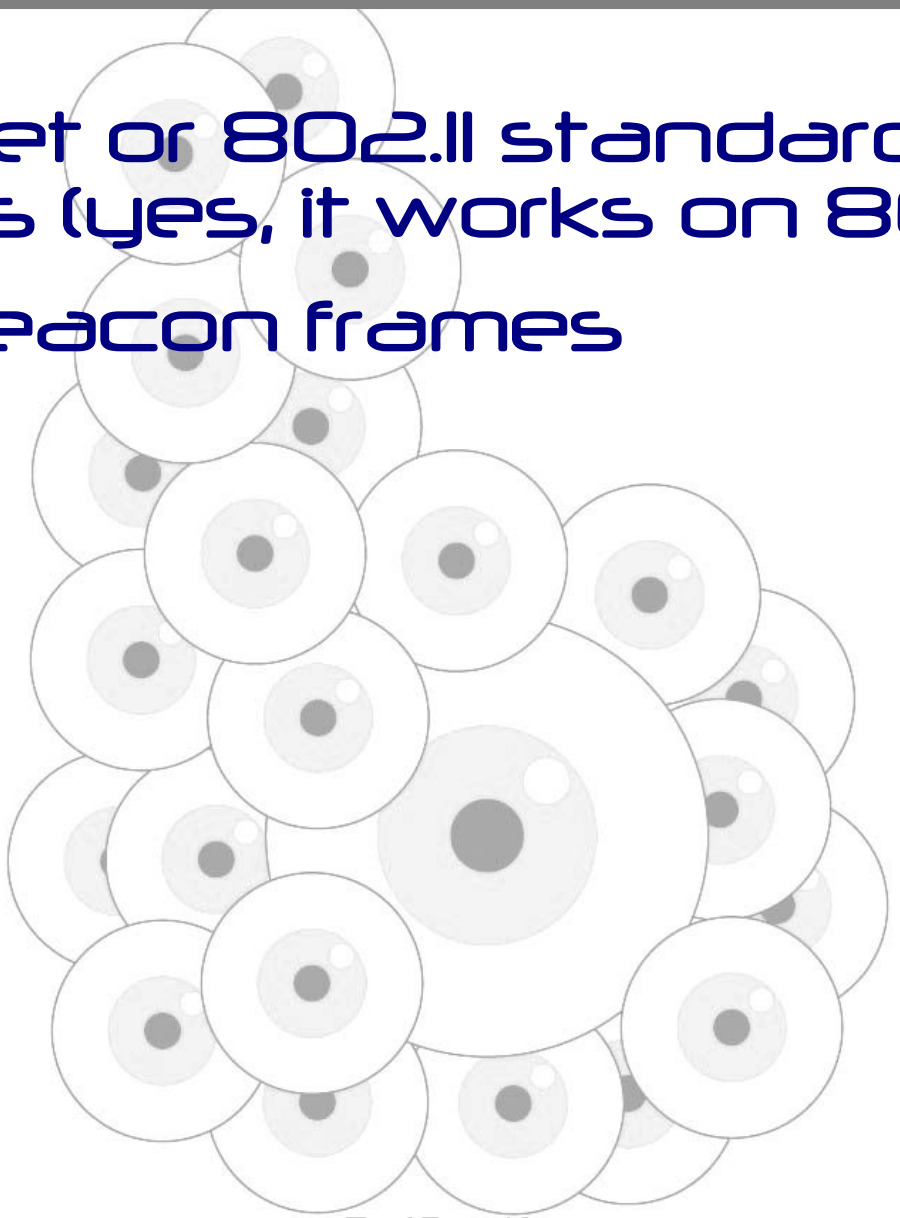
Any free tools at all?

- Roguescanner
- ??



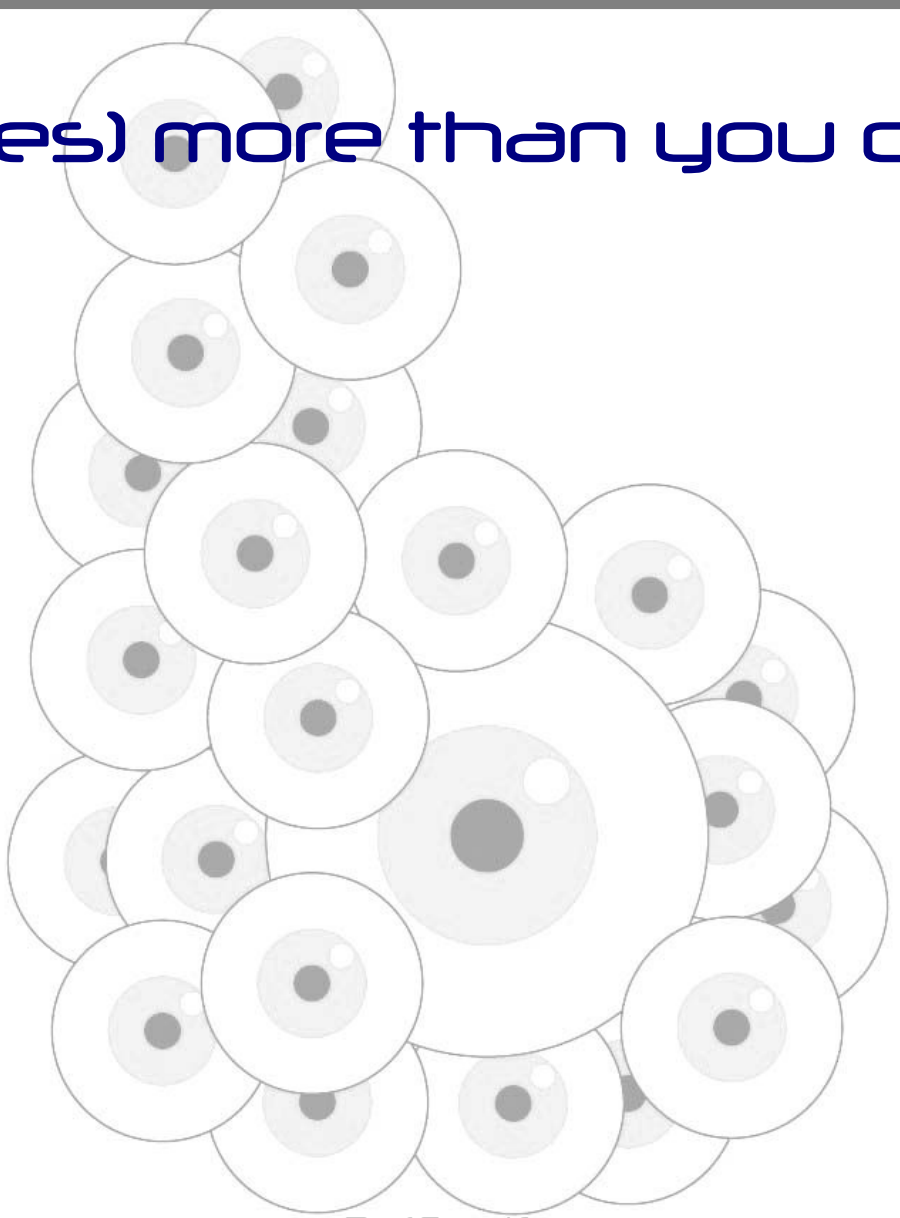
Here comes Beholder

- No chipset or 802.11 standard limitations (yes, it works on 802.11n)
- Based beacon frames



802.11 Beacons

- (sometimes) more than you can expect



OmniPeek - [cancun-direct.pkt - Packet #62]

File Edit View Capture Send Monitor Tools Window Help

Packet: 62

- Packet Info
  - Packet Number: 62
  - Flags: 0x00000000
  - Status: 0x00000000
  - Packet Length: 175
  - Timestamp: 18:09:52.897220000 04/24/2008
  - Data Rate: 11 *5.5 Mbps*
  - Channel: 6 *2437MHz 802.11n 20MHz*
  - 802.11n Flags: %00000000000000000000000000010001
    - ....1 .... *Full GI*
    - ....1 *20MHz Lower*
  - Signal Level: 18%
  - Signal dBm: -73
  - Noise Level: 16%
  - Noise dBm: -84
- 802.11 MAC Header
  - Version: 0
  - Type: %00 *Management*
  - Subtype: %1000 *Beacon*
  - Frame Control Flags: %00000000
    - 0... .... *Non-strict order*
    - .0.. .... *Non-Protected Frame*
    - ..0. .... *No More Data*
    - ...0 .... *Power Management - active mode*
    - .... 0... *This is not a Re-Transmission*
    - .... .0.. *Last or Unfragmented Frame*
    - .... ..0. *Not an Exit from the Distribution System*
    - ....0 *Not to the Distribution System*
  - Duration: 0 *Microseconds*
  - Destination: FF:FF:FF:FF:FF:FF *Ethernet Broadcast*

File Edit View Capture Send Monitor Tools Window Help

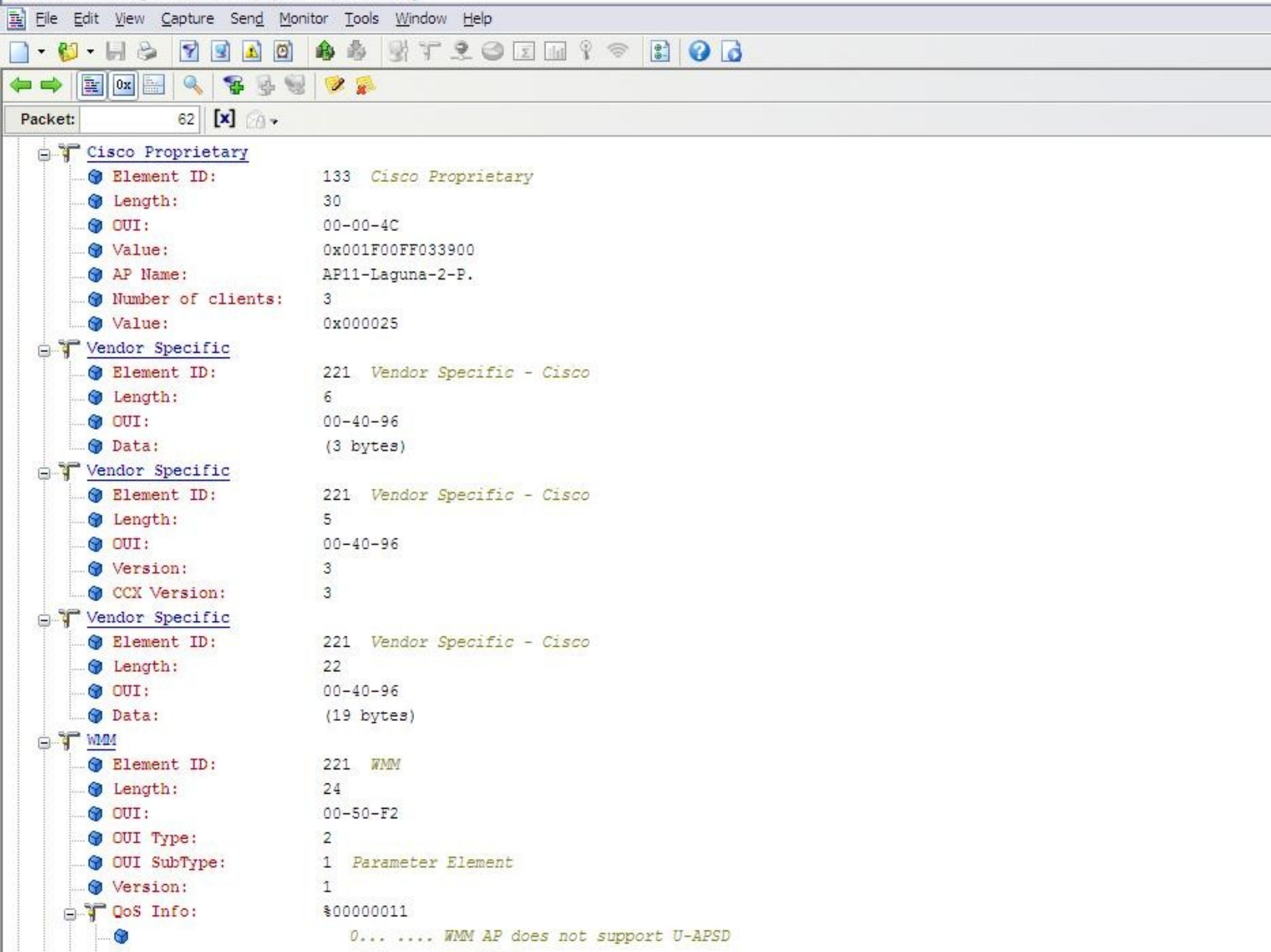
Packet: 62

802.11 Management - Beacon
- Timestamp: 1587170406644 Microseconds
- Beacon Interval: 100
- Capability Info: %0000000000000001
  - 0....... .... Immediate Block Ack Not Allowed
  - .0...... .... Delayed Block Ack Not Allowed
  - ..0..... .... DSSS-OFDM is Not Allowed
  - ...0.... .... Reserved
  - ....0... .... APSD is not supported
  - .....0.. .... G Mode Short Slot Time [20 microseconds]
  - ......0. .... QoS is Not Supported
  - ....0 .... Spectrum Mgmt Disabled
  - .... 0....... Channel Agility Not Used
  - .... .0...... PBCC Not Allowed
  - ....0..... Short Preamble Not Allowed
  - ....0.... Privacy Disabled
  - ....0... CF Poll Not Requested
  - ....0.. CF Not Pollable
  - ....0. Not an IBSS Type Network
  - ....1 ESS Type Network

SSID
- Element ID: 0 SSID
- Length: 13
- SSID: Westin Cancun

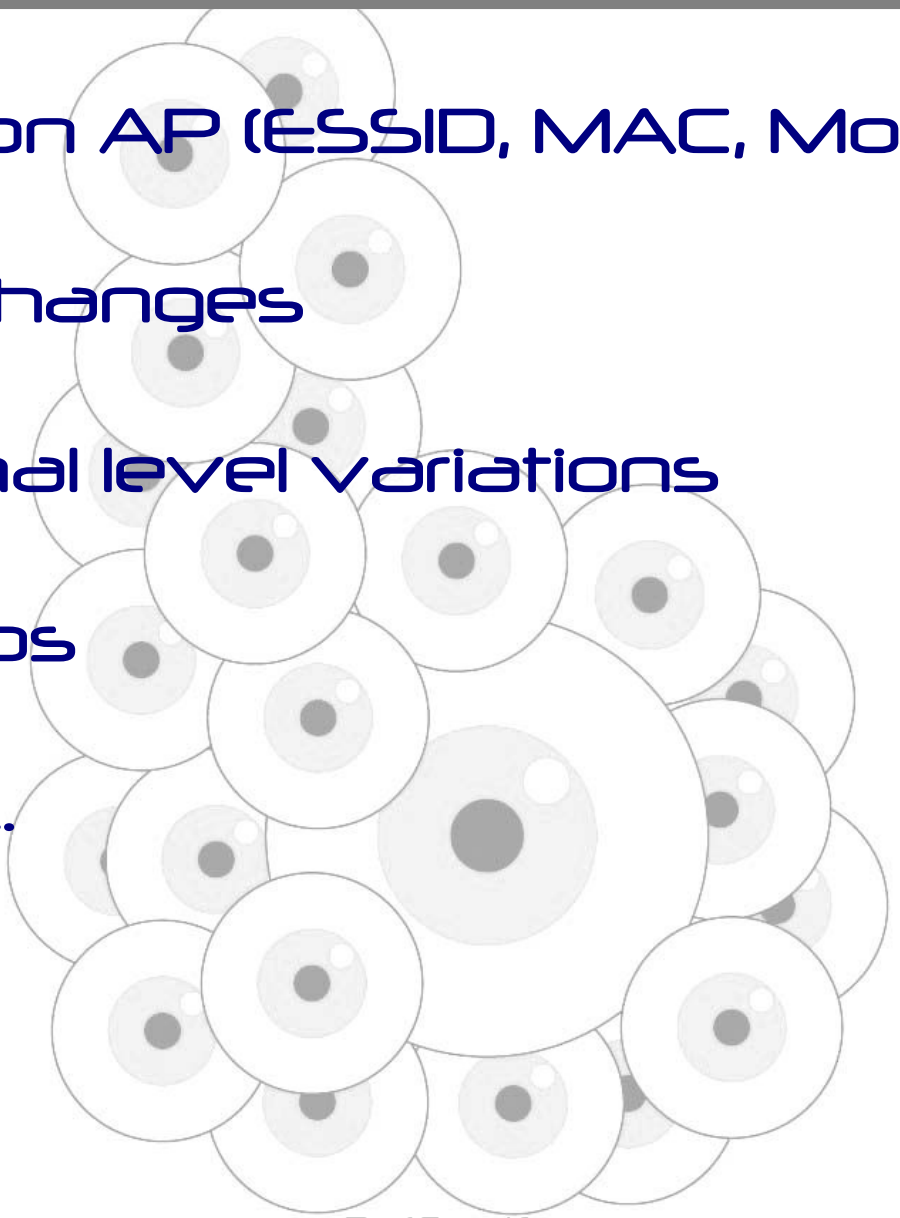
Supported Rates
- Element ID: 1 Supported Rates
- Length: 2
- Supported Rate: 5.5 Mbps (BSS Basic Rate)
- Supported Rate: 11.0 Mbps (BSS Basic Rate)

Direct Sequence Parameter Set
- Element ID: 3 Direct Sequence Parameter Set


File Edit View Capture Send Monitor Tools Window Help
Packet: 62
Cisco Proprietary
Element ID: 133 Cisco Proprietary
Length: 30
OUI: 00-00-4C
Value: 0x001F00FF033900
AP Name: AP11-Laguna-2-P.
Number of clients: 3
Value: 0x000025
Vendor Specific
Element ID: 221 Vendor Specific - Cisco
Length: 6
OUI: 00-40-96
Data: (3 bytes)
Vendor Specific
Element ID: 221 Vendor Specific - Cisco
Length: 5
OUI: 00-40-96
Version: 3
CCX Version: 3
Vendor Specific
Element ID: 221 Vendor Specific - Cisco
Length: 22
OUI: 00-40-96
Data: (19 bytes)
WMM
Element ID: 221 WMM
Length: 24
OUI: 00-50-F2
OUI Type: 2
OUI SubType: 1 Parameter Element
Version: 1
QoS Info: %00000011
0... .... WMM AP does not support U-APSD

Beholder Detects and Reports

- Changes on AP (ESSID, MAC, Mode)
- Channel changes
- Huge signal level variations
- Missing Aps
- And more...




Your
karma
is leaking.

Other cool stuff



RegEx

Regular Expression

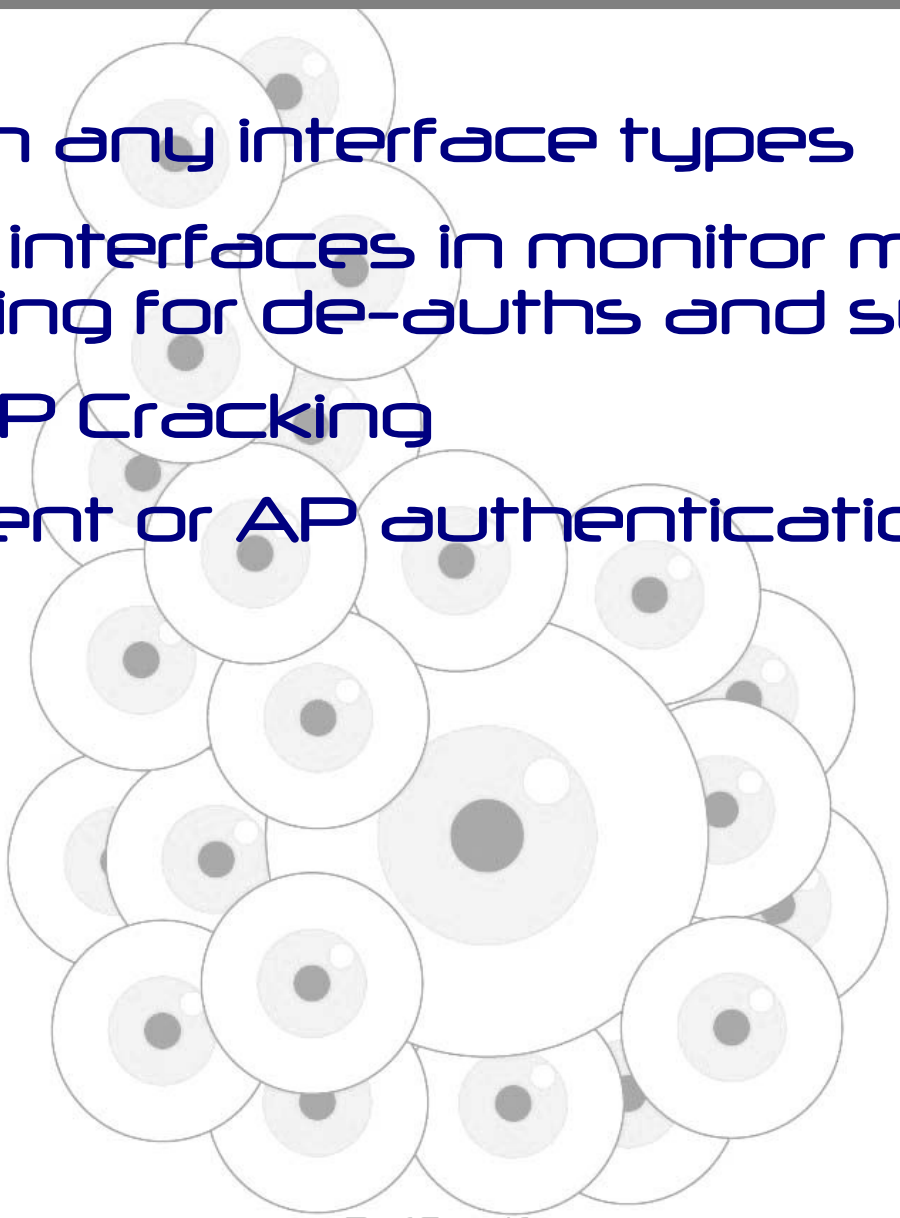
```
/h[a4@](([c<](k)|(\|<)))|((k)|(\|<))|(x))\s+\
((d)|([t\+]h))[3ea4@]\s+p[l1][a4@]n[3e][t\+]/i
```

(C)2006 FTS Conventures - www.ftsconventures.com



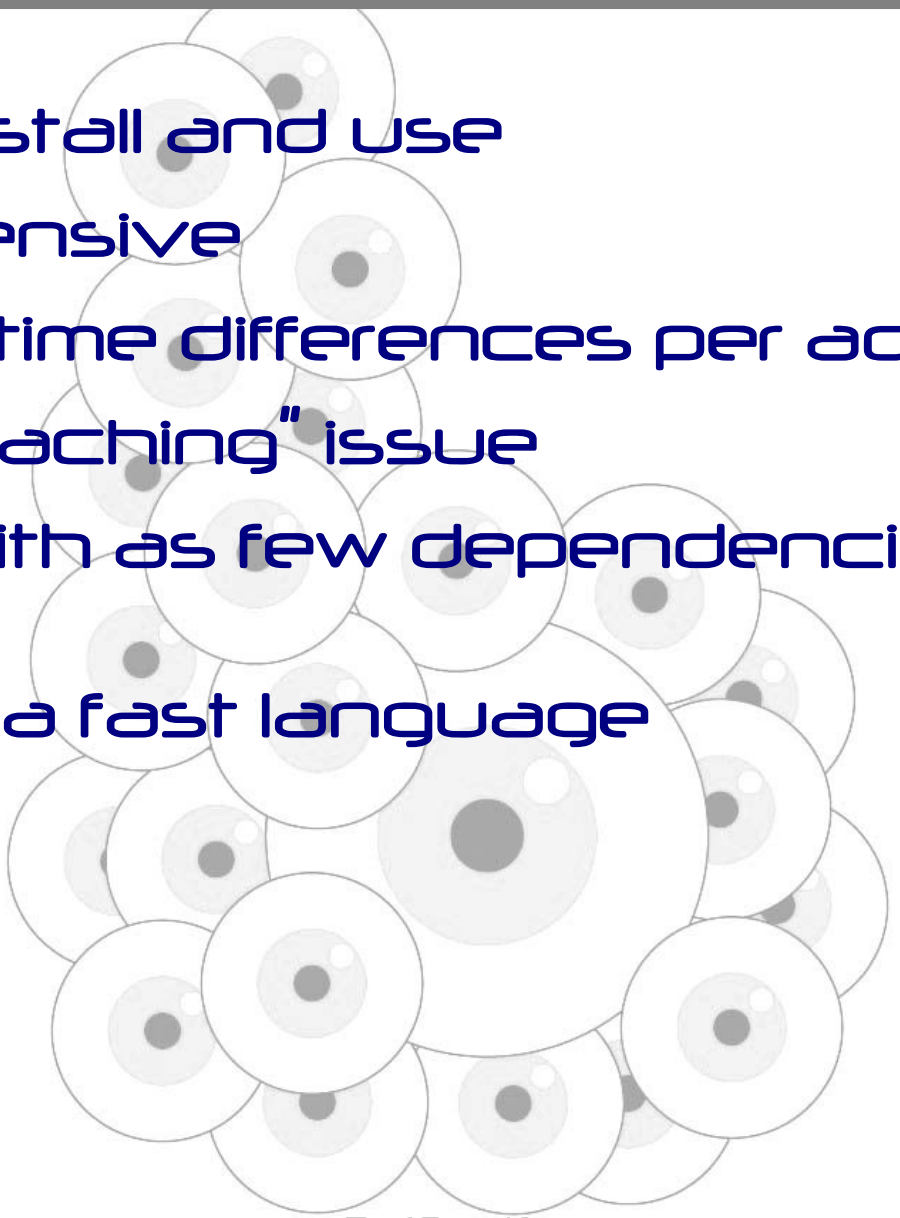
Things we DON'T do

- Sniffing on any interface types
- Put 802.11 interfaces in monitor mode (hence not checking for de-auths and such)
- WPA/WEP Cracking
- Detect client or AP authentication failed



(some of the) design challenges

- Easy to install and use
- Comprehensive
- Scanning time differences per adapter
- Madwifi "caching" issue
- Make it with as few dependencies as possible
- Written in a fast language
  - C Ansi



Caveats

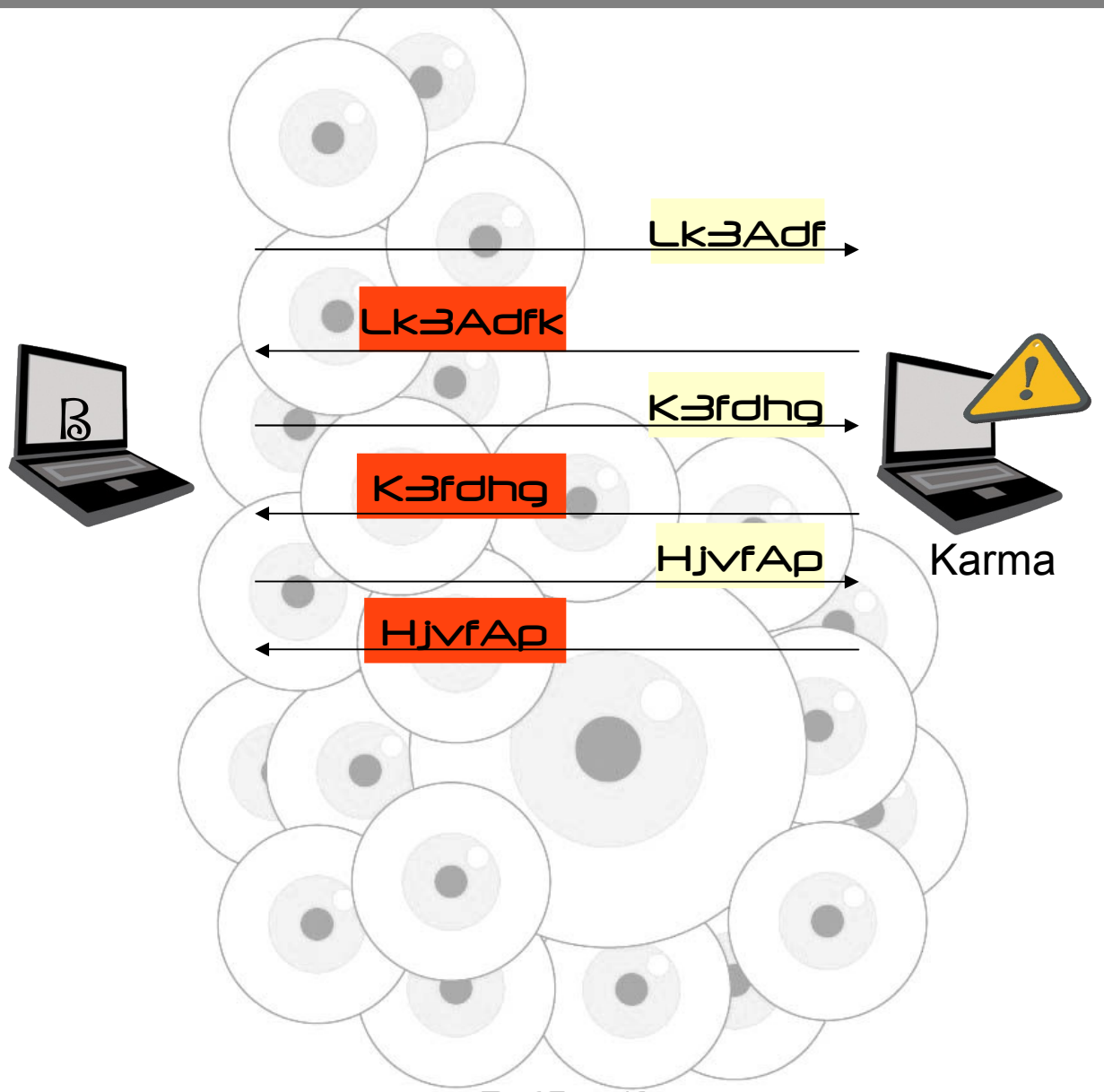
- For now...



Futures of Beholder

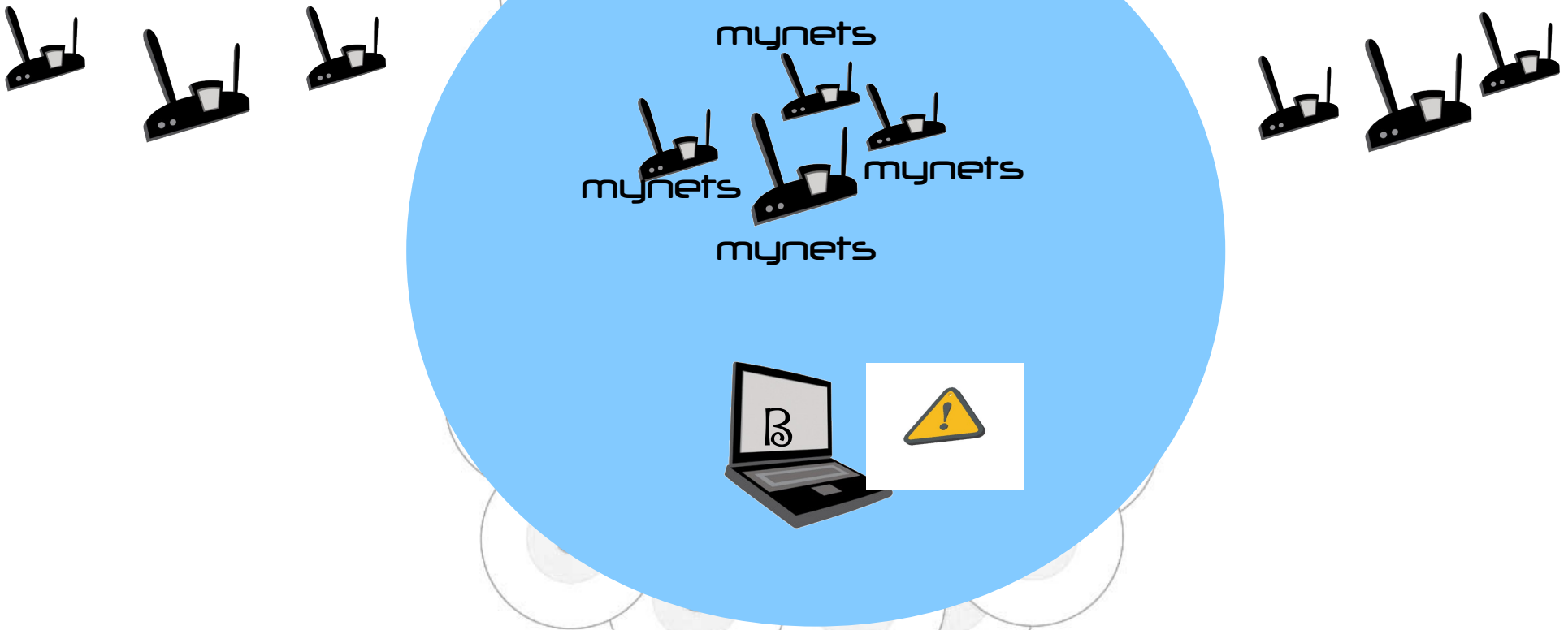


Karma Detection



Scenarios
Alerting for missing APs

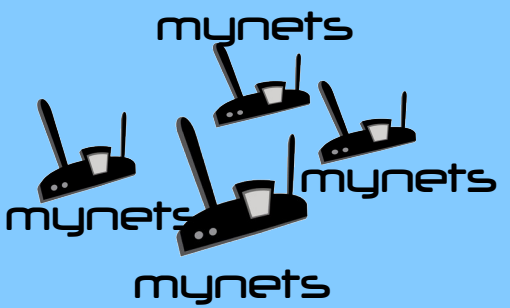
beholder -m "mynets" wifidev

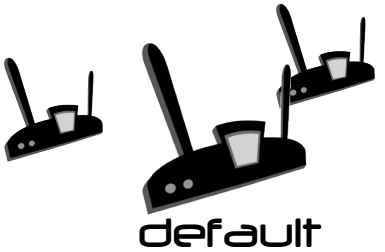


Scenarios
checking for similar essids via RegEX

```
beholder -r "mynet[t7]s.*" wifidev
```

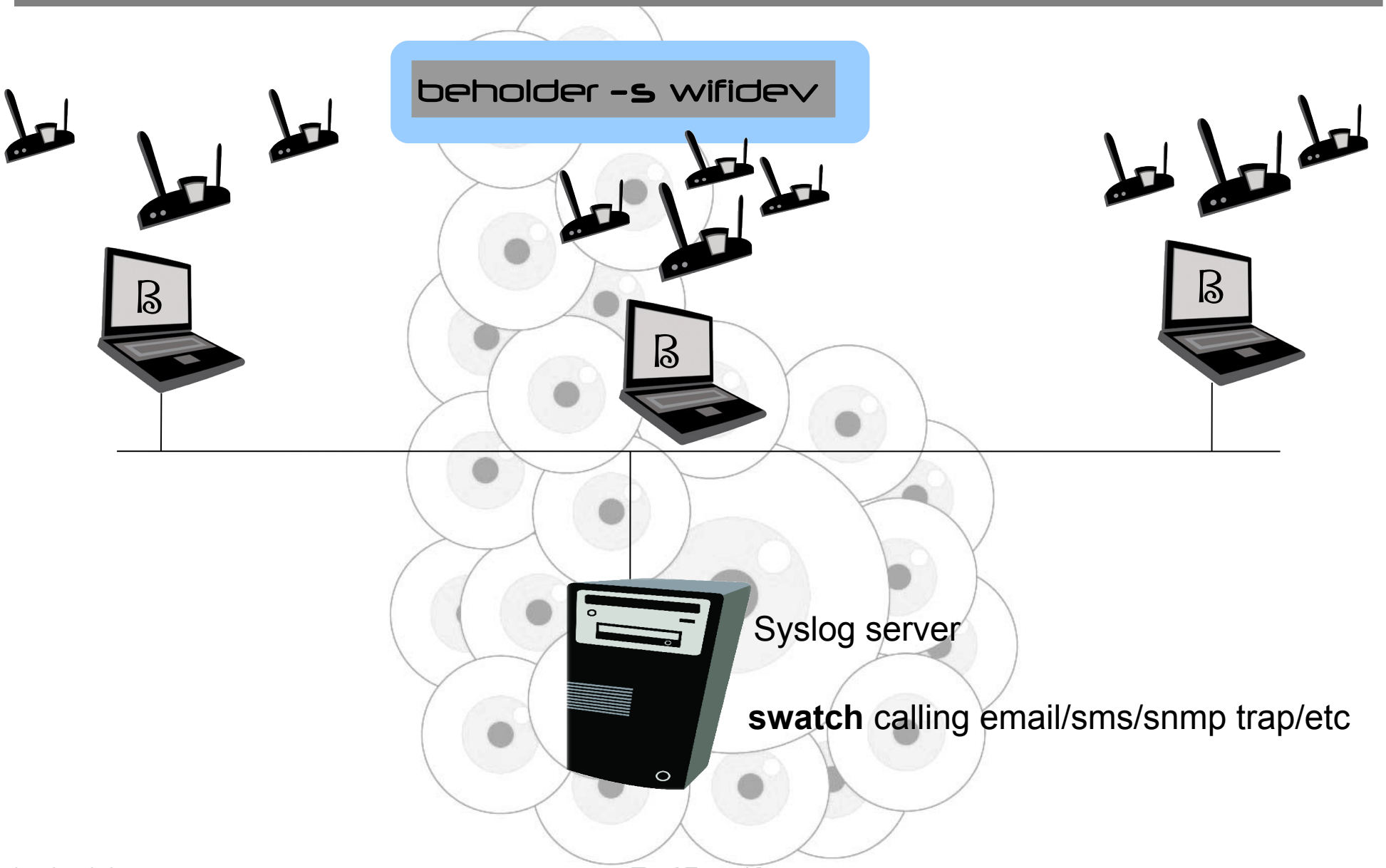








Scenarios
Huge environments



Demo?



And remember

- Even great tools might not help in all situations

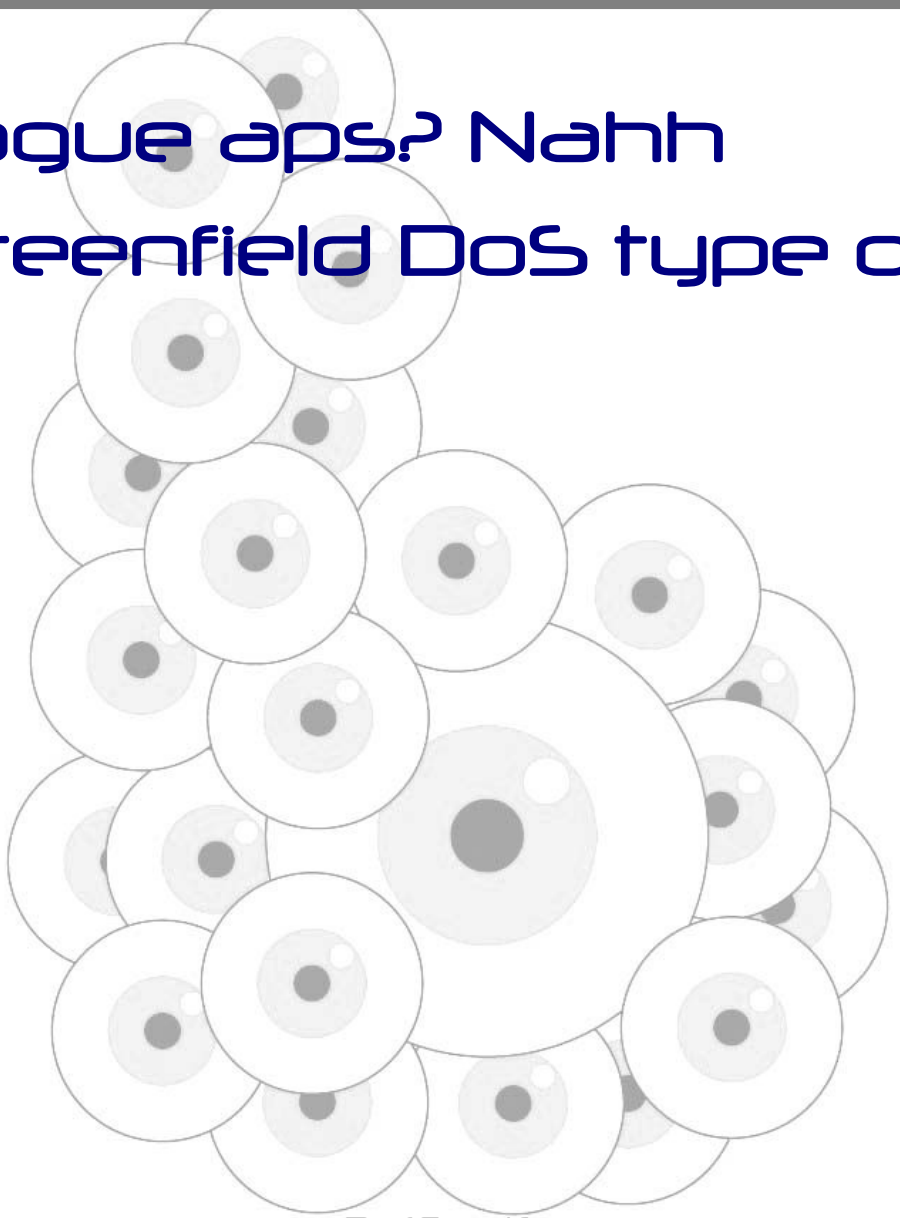


Beholder could help a bit though



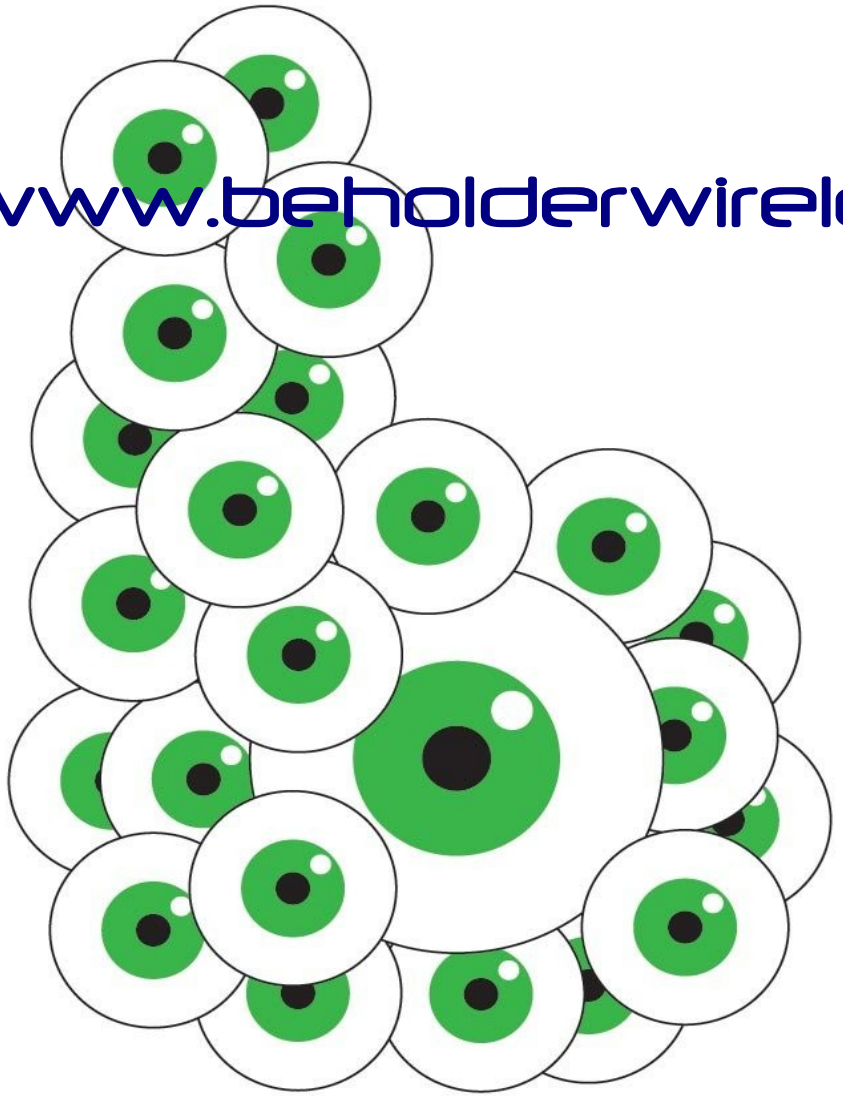
What's next on wifi attacks?

- 802.11n rogue aps? Nahh
- 802.11n greenfield DoS type of attacks? (maybe)



Now available at

http://www.beholderwireless.org




12

thanks!



