Wireless Tools

Training materials for wireless trainers

The Abdus Salam
International Centre
for Theoretical Physics

UNESCO
United Nations
Educational, Scientific and
Cultural Organization

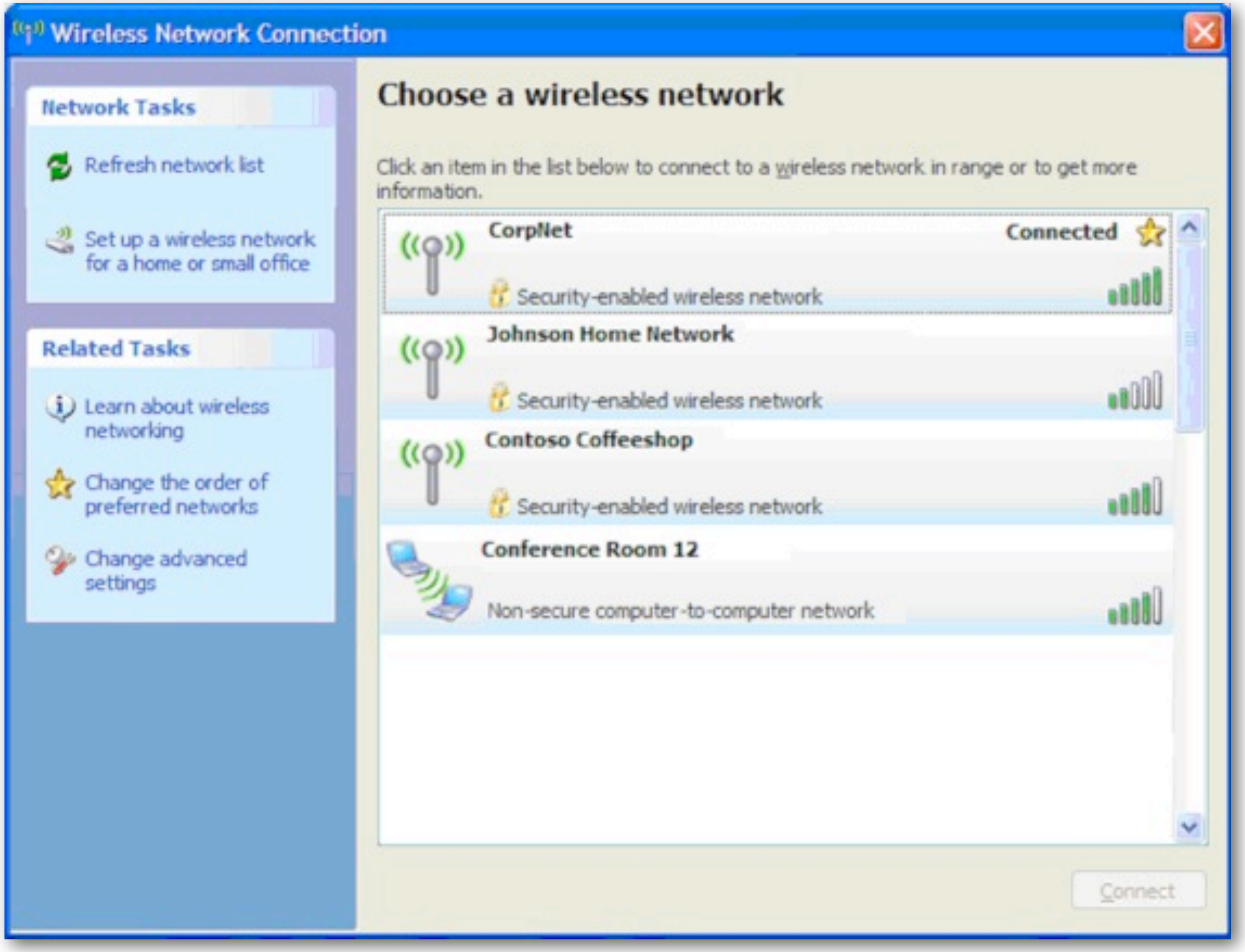
Goals

- The goal of this talk is to provide an introduction to a few software tools that will help you to:
    - monitor your WiFi network to identify problems
    - perform security audits and prevent attacks
    - observe the ongoing performance of your network and plan for future needs
    - detect interference

Types of wireless tools

- Network ESSID scanners
- Wireless protocol analyzers
- Encryption cracking tools
- Wireless device auditing and management
- “War driving” tools: network mapping
- Spectrum analysis

Built-in wireless clients



Wireless Network Connection

Network Tasks

- Refresh network list
- Set up a wireless network for a home or small office

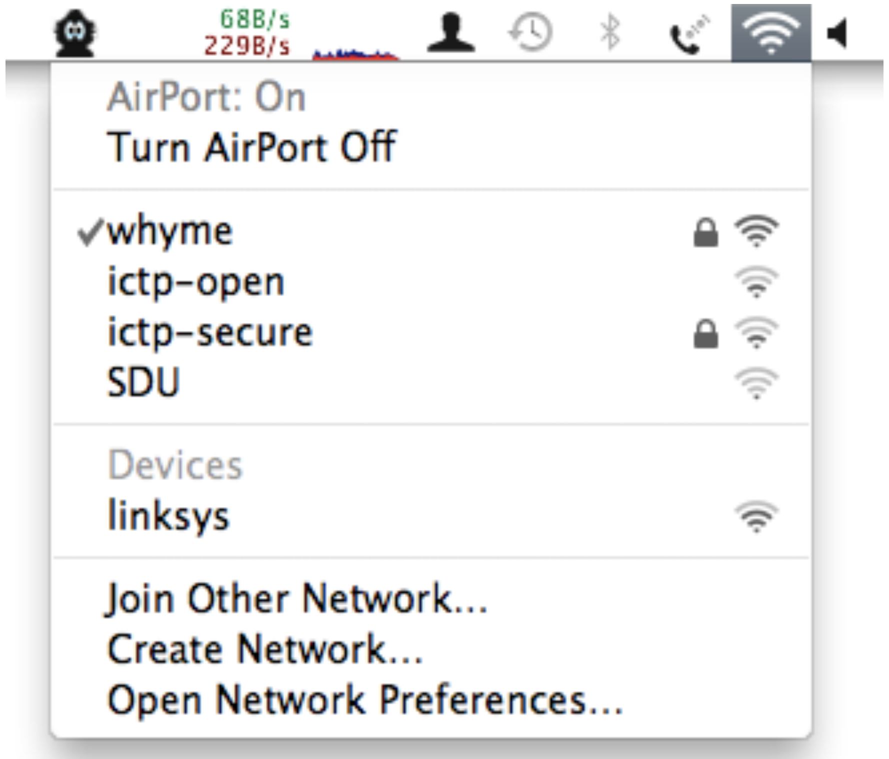
Related Tasks

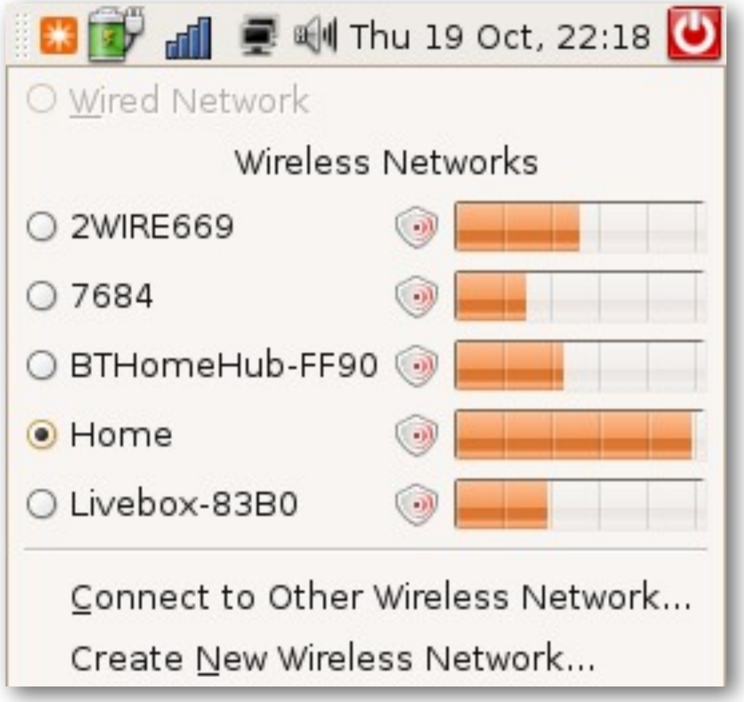
- Learn about wireless networking
- Change the order of preferred networks
- Change advanced settings

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

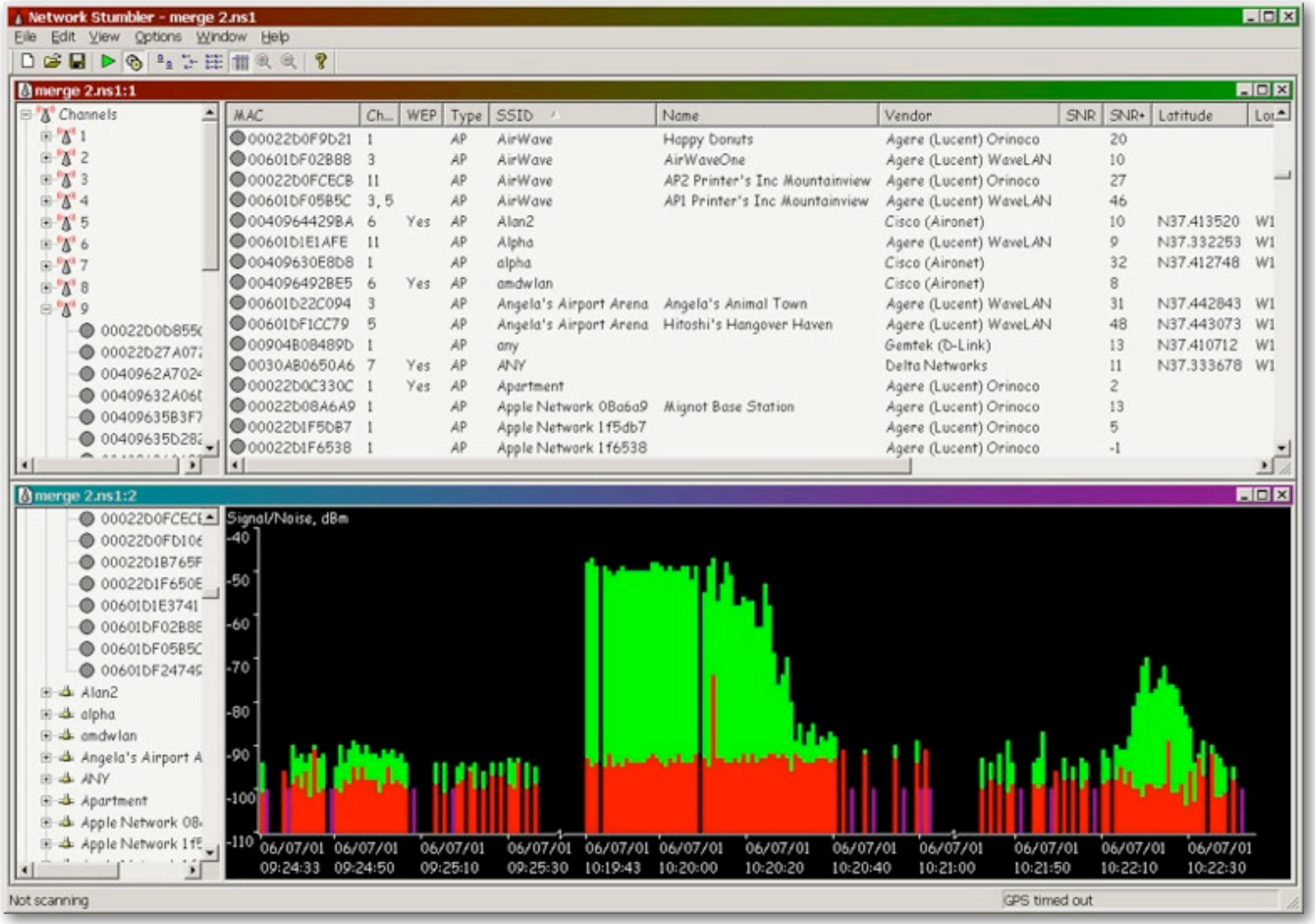
CorpNet	Security-enabled wireless network	Connected ☆
Johnson Home Network	Security-enabled wireless network	
Contoso Coffeeshop	Security-enabled wireless network	
Conference Room 12	Non-secure computer-to-computer network	





NetStumbler

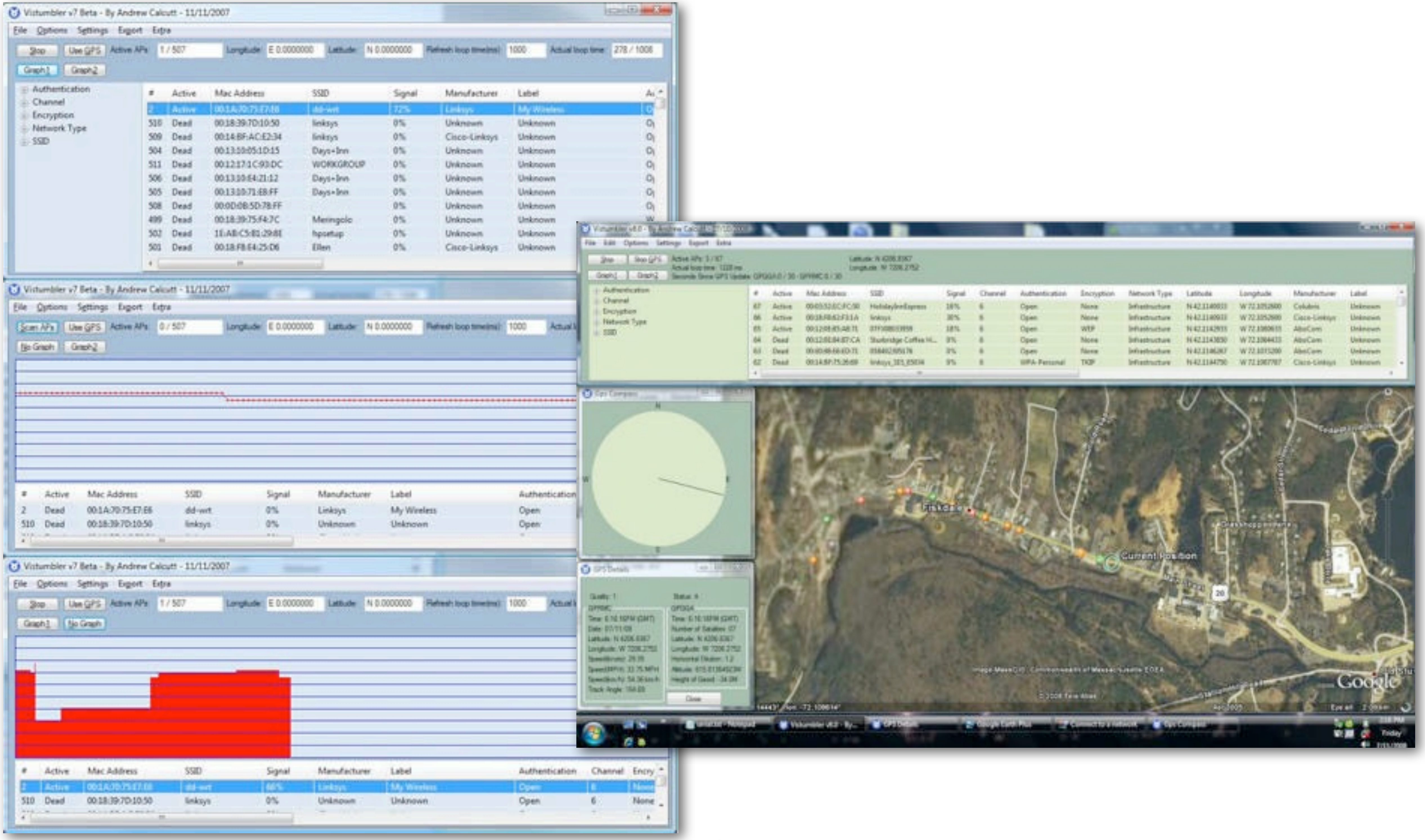
http://www.stumbler.net/



MAC	Ch...	WEP	Type	SSID	Name	Vendor	SNR	SNR+	Latitude	Lo
● 00022D0F9D21	1		AP	AirWave	Happy Donuts	Agere (Lucent) Orinoco		20		
● 00601DF02B88	3		AP	AirWave	AirWaveOne	Agere (Lucent) WaveLAN		10		
● 00022D0FCECB	11		AP	AirWave	AP2 Printer's Inc Mountainview	Agere (Lucent) Orinoco		27		
● 00601DF05B5C	3, 5		AP	AirWave	AP1 Printer's Inc Mountainview	Agere (Lucent) WaveLAN		46		
● 0040964429BA	6	Yes	AP	Alan2		Cisco (Aironet)		10	N37.413520	W1
● 00601D1E1AFE	11		AP	Alpha		Agere (Lucent) WaveLAN		9	N37.332253	W1
● 00409630E8D8	1		AP	alpha		Cisco (Aironet)		32	N37.412748	W1
● 004096492BE5	6	Yes	AP	amdwlan		Cisco (Aironet)		8		
● 00601D22C094	3		AP	Angela's Airport Arena	Angela's Animal Town	Agere (Lucent) WaveLAN		31	N37.442843	W1
● 00601DF1CC79	5		AP	Angela's Airport Arena	Hitoshi's Hangover Haven	Agere (Lucent) WaveLAN		48	N37.443073	W1
● 00904B08489D	1		AP	any		Gemtek (D-Link)		13	N37.410712	W1
● 0030AB0650A6	7	Yes	AP	ANY		Delta Networks		11	N37.333678	W1
● 00022D0C330C	1	Yes	AP	Apartment		Agere (Lucent) Orinoco		2		
● 00022D08A6A9	1		AP	Apple Network 0Ba6a9	Mignot Base Station	Agere (Lucent) Orinoco		13		
● 00022D1F5DB7	1		AP	Apple Network 1f5db7		Agere (Lucent) Orinoco		5		
● 00022D1F6538	1		AP	Apple Network 1f6538		Agere (Lucent) Orinoco		-1		

Vistumbler

http://www.vistumbler.net/



Vistumbler v7 Beta - By Andrew Calcutt - 11/11/2007

Active APs: 1 / 507 · Longitude: E 0.0000000 · Latitude: N 0.0000000 · Refresh loop time(ms): 1000 · Actual loop time: 278 / 1008

#	Active	Mac Address	SSID	Signal	Manufacturer	Label
2	Active	00:1A:70:75:E7:E6	dd-wrt	72%	Linksys	My Wireless
510	Dead	00:18:39:7D:10:50	linksys	0%	Unknown	Unknown
509	Dead	00:14:BF:AC:E2:34	linksys	0%	Cisco-Linksys	Unknown
504	Dead	00:13:10:05:1D:15	Days+Inn	0%	Unknown	Unknown
511	Dead	00:12:17:1C:93:DC	WORKGROUP	0%	Unknown	Unknown
506	Dead	00:13:10:E4:21:12	Days+Inn	0%	Unknown	Unknown
505	Dead	00:13:10:71:E8:FF	Days+Inn	0%	Unknown	Unknown
508	Dead	00:0D:0B:5D:78:FF		0%	Unknown	Unknown
499	Dead	00:18:39:75:F4:7C	Meringolo	0%	Unknown	Unknown
502	Dead	11:AB:C5:81:29:81	hpsetup	0%	Unknown	Unknown
501	Dead	00:18:F8:E4:25:D6	Ellen	0%	Cisco-Linksys	Unknown

Vistumbler v7 Beta - By Andrew Calcutt - 11/11/2007

Active APs: 0 / 507 · Longitude: E 0.0000000 · Latitude: N 0.0000000 · Refresh loop time(ms): 1000

#	Active	Mac Address	SSID	Signal	Manufacturer	Label	Authentication
2	Dead	00:1A:70:75:E7:E6	dd-wrt	0%	Linksys	My Wireless	Open
510	Dead	00:18:39:7D:10:50	linksys	0%	Unknown	Unknown	Open

Vistumbler v7 Beta - By Andrew Calcutt - 11/11/2007

Active APs: 1 / 507 · Longitude: E 0.0000000 · Latitude: N 0.0000000 · Refresh loop time(ms): 1000

#	Active	Mac Address	SSID	Signal	Manufacturer	Label	Authentication	Channel	Encry
2	Active	00:1A:70:75:E7:E6	dd-wrt	66%	Linksys	My Wireless	Open	6	None
510	Dead	00:18:39:7D:10:50	linksys	0%	Unknown	Unknown	Open	6	None

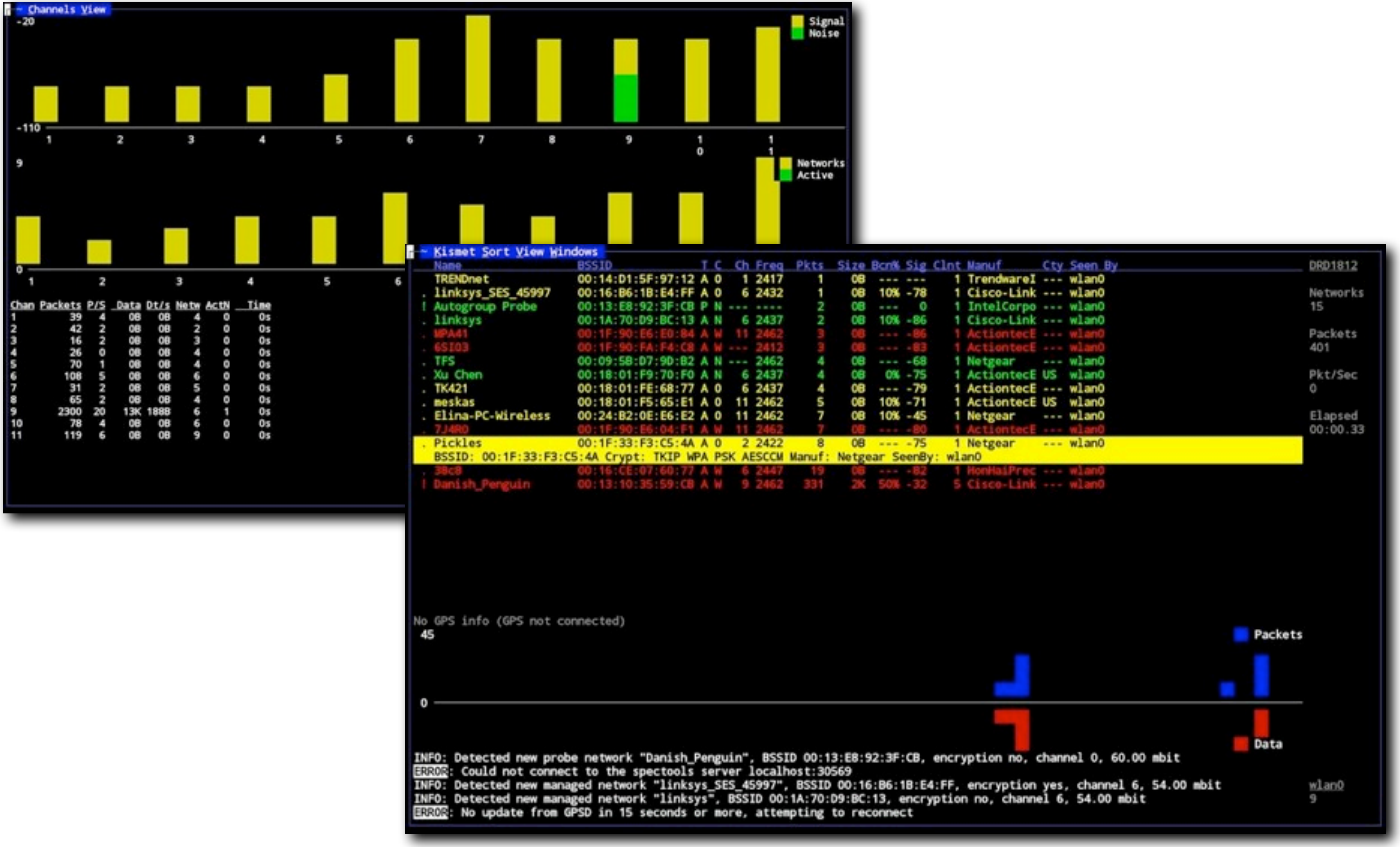
Vistumbler v8.0 - By Andrew Calcutt

Active APs: 3 / 67
Actual loop time: 1220 ms
Seconds Since GPS Update: GPGGA 0 / 30 - GPRMC 0 / 30
Latitude: N 4206.8367
Longitude: W 7206.2752

#	Active	Mac Address	SSID	Signal	Channel	Authentication	Encryption	Network Type	Latitude	Longitude	Manufacturer	Label
67	Active	00:03:52:EC:FC:50	HolidayInnExpress	18%	6	Open	None	Infrastructure	N 42.1140933	W 72.1052600	Colubris	Unknown
66	Active	00:18:F8:62:F3:1A	linksys	30%	6	Open	None	Infrastructure	N 42.1140933	W 72.1052600	Cisco-Linksys	Unknown
65	Active	00:12:0E:85:A8:71	07F108033958	18%	6	Open	WEP	Infrastructure	N 42.1142933	W 72.1060633	AboCom	Unknown
64	Dead	00:12:0E:84:87:CA	Sturbridge Coffee H...	0%	6	Open	None	Infrastructure	N 42.1143850	W 72.1064433	AboCom	Unknown
63	Dead	00:0D:88:66:ED:71	0584402005176	0%	6	Open	None	Infrastructure	N 42.1146267	W 72.1075200	AboCom	Unknown
62	Dead	00:14:BF:75:26:69	linksys_SES_05034	0%	6	WPA-Personal	TKIP	Infrastructure	N 42.1144750	W 72.1087787	Cisco-Linksys	Unknown

Kismet

http://www.kismetwireless.net/



```
Chan Packets P/S  Data Dt/s Netw ActN   Time
1         39   4    0B   0B    4    0     0s
2         42   2    0B   0B    2    0     0s
3         16   2    0B   0B    3    0     0s
4         26   0    0B   0B    4    0     0s
5         70   1    0B   0B    4    0     0s
6        108   5    0B   0B    6    0     0s
7         31   2    0B   0B    5    0     0s
8         65   2    0B   0B    4    0     0s
9       2300  20   13K 188B    6    1     0s
10        78   4    0B   0B    6    0     0s
11       119   6    0B   0B    9    0     0s
```

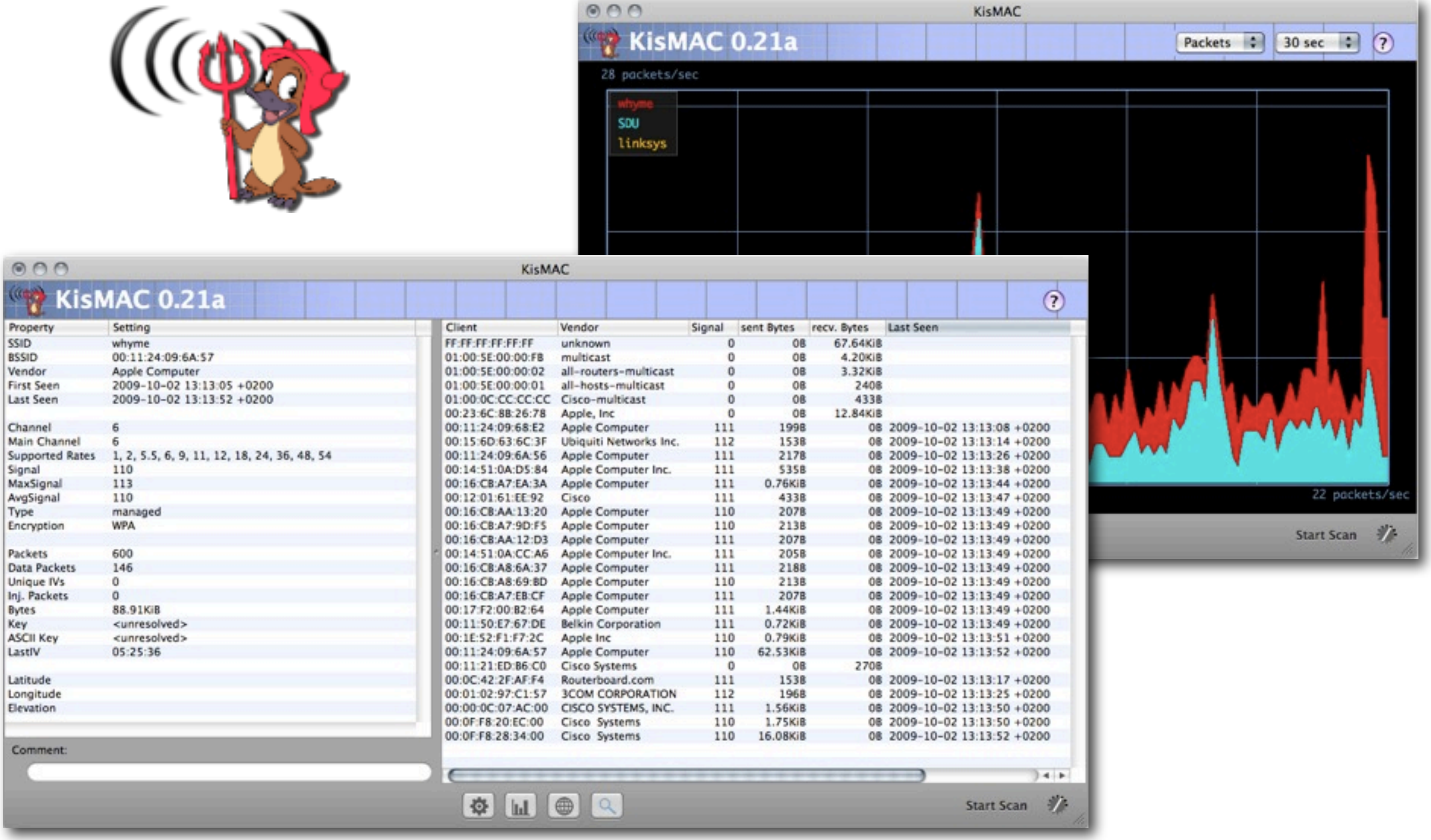
```
~ Kismet Sort View Windows
  Name                BSSID             T C  Ch Freq  Pkts  Size Bcn% Sig Clnt Manuf       Cty Seen By       DRD1812
  TRENDnet            00:14:D1:5F:97:12 A 0   1 2417     1    0B ---  ---    1 TrendwareI  --- wlan0
. linksys_SES_45997   00:16:B6:1B:E4:FF A 0   6 2432     1    0B 10%  -78    1 Cisco-Link  --- wlan0         Networks
! Autogroup Probe     00:13:E8:92:3F:CB P N --- ----     2    0B ---    0    1 IntelCorpo  --- wlan0         15
. linksys             00:1A:70:D9:BC:13 A N   6 2437     2    0B 10%  -86    1 Cisco-Link  --- wlan0
. WPA41               00:1F:90:E6:E0:B4 A W  11 2462     3    0B ---  -86    1 ActiontecE  --- wlan0         Packets
. 6SI03               00:1F:90:FA:F4:C8 A W --- 2412     3    0B ---  -83    1 ActiontecE  --- wlan0         401
. TFS                 00:09:5B:D7:9D:B2 A N --- 2462     4    0B ---  -68    1 Netgear     --- wlan0
. Xu Chen             00:18:01:F9:70:F0 A N   6 2437     4    0B  0%  -75    1 ActiontecE  US  wlan0         Pkt/Sec
. TK421               00:18:01:FE:68:77 A 0   6 2437     4    0B ---  -79    1 ActiontecE  --- wlan0         0
. meskas              00:18:01:F5:65:E1 A 0  11 2462     5    0B 10%  -71    1 ActiontecE  US  wlan0
. Elina-PC-Wireless   00:24:B2:0E:E6:E2 A 0  11 2462     7    0B 10%  -45    1 Netgear     --- wlan0         Elapsed
. 7J4R0               00:1F:90:E6:04:F1 A W  11 2462     7    0B ---  -80    1 ActiontecE  --- wlan0         00:00.33
. Pickles             00:1F:33:F3:C5:4A A 0   2 2422     8    0B ---  -75    1 Netgear     --- wlan0
  BSSID: 00:1F:33:F3:C5:4A Crypt: TKIP WPA PSK AESCCM Manuf: Netgear SeenBy: wlan0
. 38c8                00:16:CE:07:60:77 A W   6 2447    19    0B ---  -82    1 HonHaiPrec  --- wlan0
! Danish_Penguin      00:13:10:35:59:CB A W   9 2462   331    2K 50%  -32    5 Cisco-Link  --- wlan0

No GPS info (GPS not connected)

INFO: Detected new probe network "Danish_Penguin", BSSID 00:13:E8:92:3F:CB, encryption no, channel 0, 60.00 mbit
ERROR: Could not connect to the spectools server localhost:30569
INFO: Detected new managed network "linksys_SES_45997", BSSID 00:16:B6:1B:E4:FF, encryption yes, channel 6, 54.00 mbit   wlan0
INFO: Detected new managed network "linksys", BSSID 00:1A:70:D9:BC:13, encryption no, channel 6, 54.00 mbit             9
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
```

KisMAC

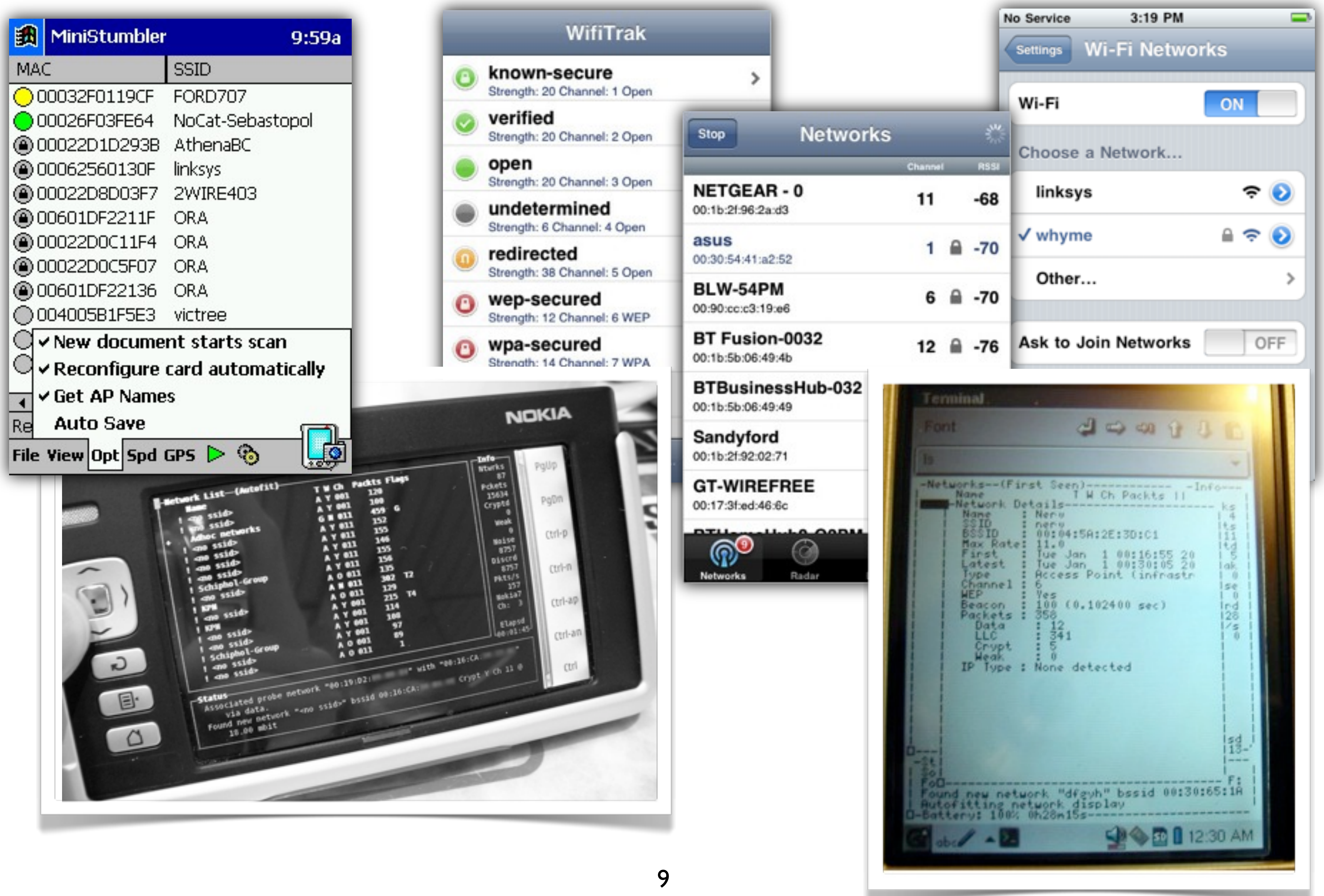
http://www.kismac-ng.org/



Property	Setting
SSID	whyme
BSSID	00:11:24:09:6A:57
Vendor	Apple Computer
First Seen	2009-10-02 13:13:05 +0200
Last Seen	2009-10-02 13:13:52 +0200
Channel	6
Main Channel	6
Supported Rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54
Signal	110
MaxSignal	113
AvgSignal	110
Type	managed
Encryption	WPA
Packets	600
Data Packets	146
Unique IVs	0
Inj. Packets	0
Bytes	88.91KiB
Key	<unresolved>
ASCII Key	<unresolved>
LastIV	05:25:36
Latitude	
Longitude	
Elevation	

Client	Vendor	Signal	sent Bytes	recv. Bytes	Last Seen
FF:FF:FF:FF:FF:FF	unknown	0	0B	67.64KiB	
01:00:5E:00:00:FB	multicast	0	0B	4.20KiB	
01:00:5E:00:00:02	all-routers-multicast	0	0B	3.32KiB	
01:00:5E:00:00:01	all-hosts-multicast	0	0B	240B	
01:00:0C:CC:CC:CC	Cisco-multicast	0	0B	433B	
00:23:6C:8B:26:78	Apple, Inc	0	0B	12.84KiB	
00:11:24:09:68:E2	Apple Computer	111	199B	0B	2009-10-02 13:13:08 +0200
00:15:6D:63:6C:3F	Ubiquiti Networks Inc.	112	153B	0B	2009-10-02 13:13:14 +0200
00:11:24:09:6A:56	Apple Computer	111	217B	0B	2009-10-02 13:13:26 +0200
00:14:51:0A:D5:84	Apple Computer Inc.	111	535B	0B	2009-10-02 13:13:38 +0200
00:16:CB:A7:EA:3A	Apple Computer	111	0.76KiB	0B	2009-10-02 13:13:44 +0200
00:12:01:61:EE:92	Cisco	111	433B	0B	2009-10-02 13:13:47 +0200
00:16:CB:AA:13:20	Apple Computer	110	207B	0B	2009-10-02 13:13:49 +0200
00:16:CB:A7:9D:F5	Apple Computer	110	213B	0B	2009-10-02 13:13:49 +0200
00:16:CB:AA:12:D3	Apple Computer	111	207B	0B	2009-10-02 13:13:49 +0200
00:14:51:0A:CC:A6	Apple Computer Inc.	111	205B	0B	2009-10-02 13:13:49 +0200
00:16:CB:A8:6A:37	Apple Computer	111	218B	0B	2009-10-02 13:13:49 +0200
00:16:CB:A8:69:BD	Apple Computer	110	213B	0B	2009-10-02 13:13:49 +0200
00:16:CB:A7:EB:CF	Apple Computer	111	207B	0B	2009-10-02 13:13:49 +0200
00:17:F2:00:B2:64	Apple Computer	111	1.44KiB	0B	2009-10-02 13:13:49 +0200
00:11:50:E7:67:DE	Belkin Corporation	111	0.72KiB	0B	2009-10-02 13:13:49 +0200
00:1E:52:F1:F7:2C	Apple Inc	110	0.79KiB	0B	2009-10-02 13:13:51 +0200
00:11:24:09:6A:57	Apple Computer	110	62.53KiB	0B	2009-10-02 13:13:52 +0200
00:11:21:ED:B6:C0	Cisco Systems	0	0B	270B	
00:0C:42:2F:AF:F4	Routerboard.com	111	153B	0B	2009-10-02 13:13:17 +0200
00:01:02:97:C1:57	3COM CORPORATION	112	196B	0B	2009-10-02 13:13:25 +0200
00:00:0C:07:AC:00	CISCO SYSTEMS, INC.	111	1.56KiB	0B	2009-10-02 13:13:50 +0200
00:0F:F8:20:EC:00	Cisco Systems	110	1.75KiB	0B	2009-10-02 13:13:50 +0200
00:0F:F8:28:34:00	Cisco Systems	110	16.08KiB	0B	2009-10-02 13:13:52 +0200

Handheld wireless clients



MiniStumbler 9:59a

MAC	SSID
● 00032F0119CF	FORD707
● 00026F03FE64	NoCat-Sebastopol
00022D1D293B	AthenaBC
00062560130F	linksys
00022D8D03F7	2WIRE403
00601DF2211F	ORA
00022D0C11F4	ORA
00022D0C5F07	ORA
00601DF22136	ORA
○ 004005B1F5E3	victree

✓ New document starts scan
✓ Reconfigure card automatically
✓ Get AP Names
Auto Save

WifiTrak

known-secure
Strength: 20 Channel: 1 Open

verified
Strength: 20 Channel: 2 Open

open
Strength: 20 Channel: 3 Open

undetermined
Strength: 6 Channel: 4 Open

redirected
Strength: 38 Channel: 5 Open

wep-secured
Strength: 12 Channel: 6 WEP

wpa-secured
Strength: 14 Channel: 7 WPA

	Channel	RSSI
NETGEAR - 0 00:1b:2f:96:2a:d3	11	-68
asus 00:30:54:41:a2:52	1 🔒	-70
BLW-54PM 00:90:cc:c3:19:e6	6 🔒	-70
BT Fusion-0032 00:1b:5b:06:49:4b	12 🔒	-76
BTBusinessHub-032 00:1b:5b:06:49:49		
Sandyford 00:1b:2f:92:02:71		
GT-WIREFREE 00:17:3f:ed:46:6c		

No Service 3:19 PM

Wi-Fi Networks

Wi-Fi ON

Choose a Network...

linksys
✓ whyme 🔒
Other...

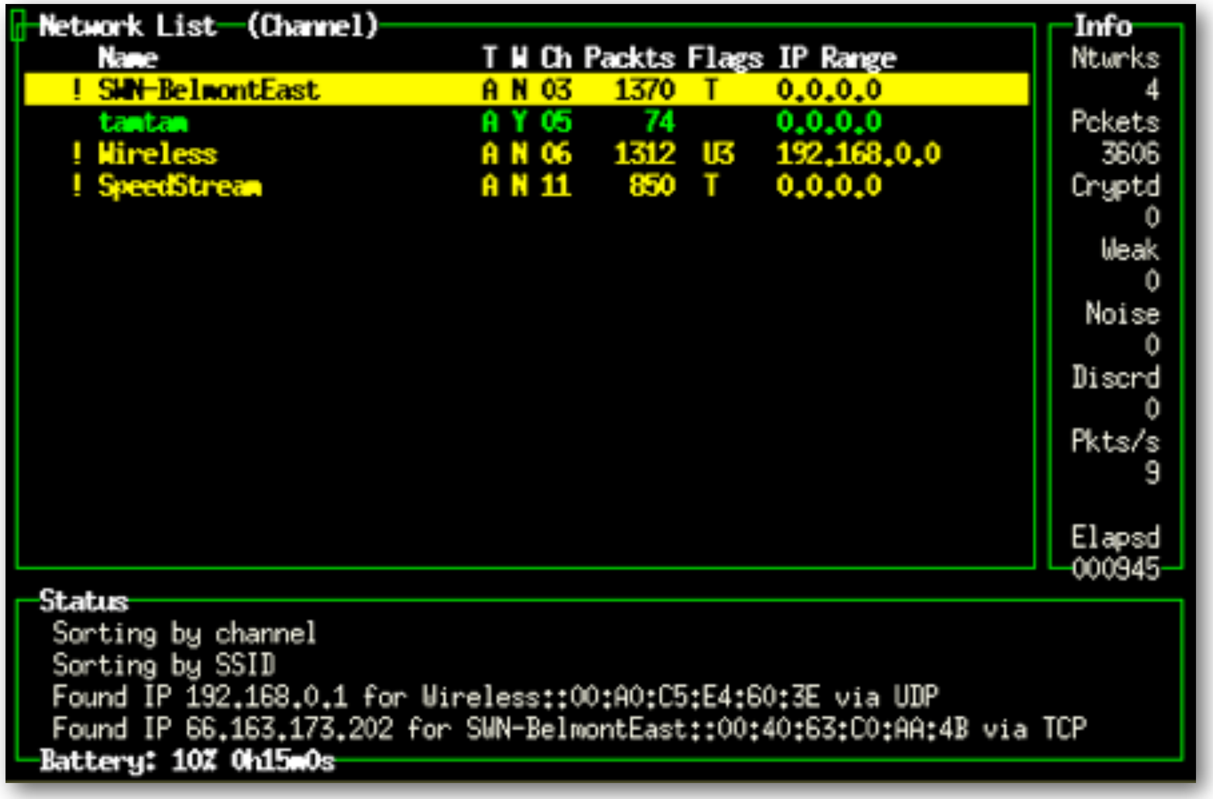
Ask to Join Networks OFF

```
-Network List--(Autofit)--------------- T W Ch  Packts Flags   Info
   Name                                  A Y 001   120          Ntwrks
 ! <no ssid>                             A Y 001   100            87
 ! <no ssid>                             G N 011   459   G      Pckets
 Adhoc networks                          A Y 011   152           15634
 ! <no ssid>                             A Y 011   155          Cryptd
 ! <no ssid>                             A Y 011   146             0
 ! <no ssid>                             A Y 011   155          Weak
 ! <no ssid>                             A Y 011   156             0
 ! Schiphol-Group                        A Y 011   135          Noise
 ! <no ssid>                             A O 011   302   T2      8757
 ! KPN                                   A N 011   129          Discrd
 ! <no ssid>                             A O 011   215   T4      8757
 ! KPN                                   A Y 001   114          Pkts/s
 ! <no ssid>                             A Y 001   108            157
 ! <no ssid>                             A Y 001    97          Nokia7
 ! Schiphol-Group                        A Y 001    89          Ch:  3
 ! <no ssid>                             A O 001     1
 ! <no ssid>                             A O 011                Elapsd
                                                                00:01:45
-Status
 Associated probe network "00:19:02:[redacted]" with "00:16:CA:[redacted]"
     via data.
 Found new network "<no ssid>" bssid 00:16:CA:[redacted] Crypt Y Ch 11 @
     10.00 mbit
```

```
-Networks--(First Seen)------------ -Info---
   Name                 T W Ch Packts !!
  -Network Details----------------------- ks
     Name     : Nero                       4
     SSID     : nero                      ts
     BSSID    : 00:04:5A:2E:3D:C1         11
     Max Rate : 11.0                      td
     First    : Tue Jan  1 00:16:55 20     5
     Latest   : Tue Jan  1 00:30:05 20    ak
     Type     : Access Point (infrastr     0
     Channel  : 6                         se
     WEP      : Yes                        0
     Beacon   : 100 (0.102400 sec)        rd
     Packets  : 358                       28
       Data     : 12                      /s
       LLC      : 341                      0
       Crypt    : 5
       Weak     : 0
     IP Type  : None detected

                                          sd
                                          13-
 Found new network "dfgyh" bssid 00:30:65:1A
 Autofitting network display
-Battery: 100% 0h28m15s--------------------
```

KISMET

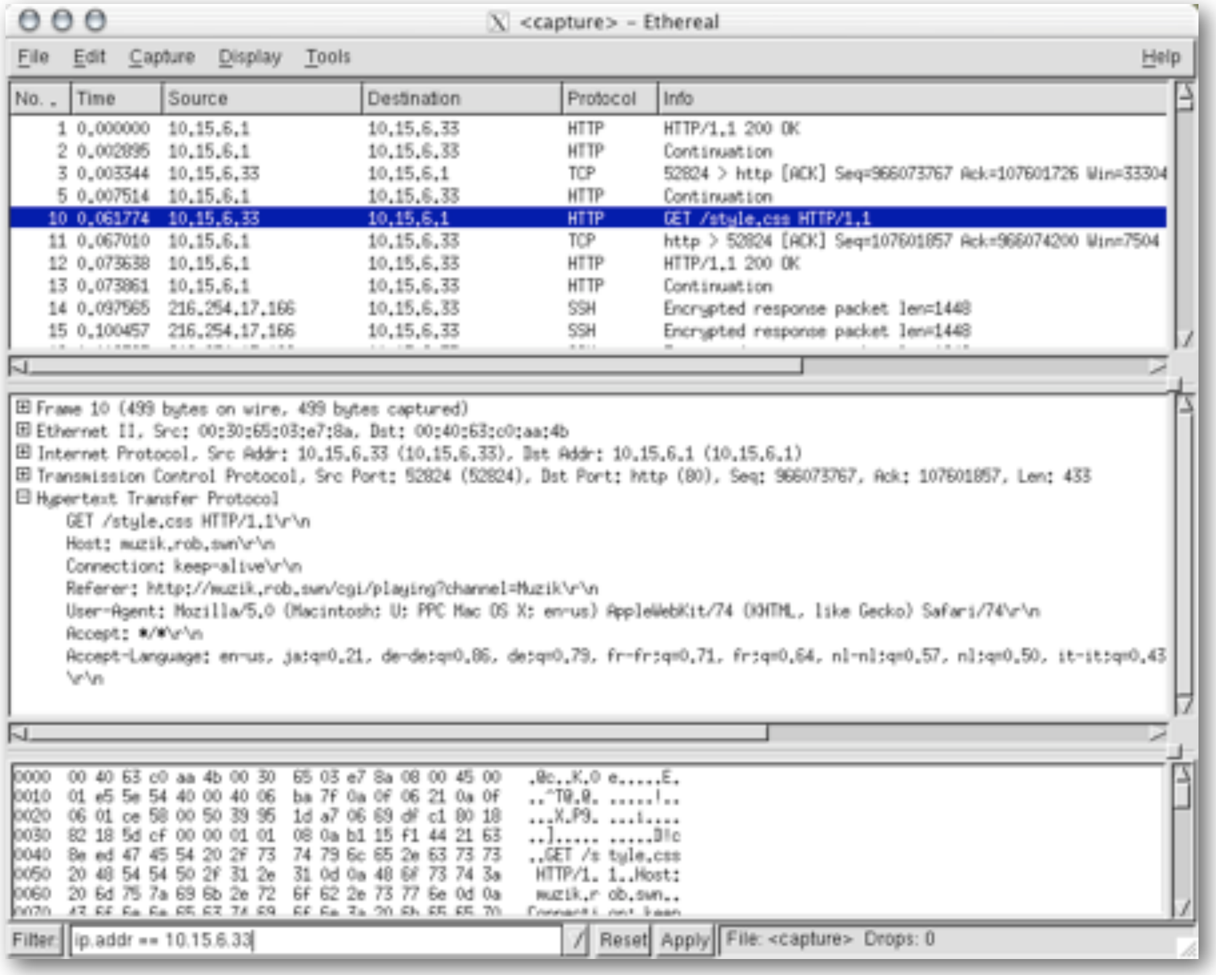


```
Network List—(Channel)                                      Info
   Name                              T W Ch Packts Flags IP Range   Ntwrks
 ! SWN-BelmontEast                   A N 03  1370   T    0.0.0.0        4
   tamtam                            A Y 05    74        0.0.0.0    Pckets
 ! Wireless                          A N 06  1312   U3   192.168.0.0  3606
 ! SpeedStream                       A N 11   850   T    0.0.0.0    Cryptd
                                                                         0
                                                                      Weak
                                                                         0
                                                                     Noise
                                                                         0
                                                                    Discrd
                                                                         0
                                                                    Pkts/s
                                                                         9

                                                                    Elapsd
                                                                    000945
Status
 Sorting by channel
 Sorting by SSID
 Found IP 192.168.0.1 for Wireless::00:A0:C5:E4:60:3E via UDP
 Found IP 66.163.173.202 for SWN-BelmontEast::00:40:63:C0:AA:4B via TCP
Battery: 10% 0h15m0s
```

+

WIRESHARK



```
No. . Time      Source          Destination   Protocol Info
    1 0.000000  10.15.6.1       10.15.6.33    HTTP     HTTP/1.1 200 OK
    2 0.002895  10.15.6.1       10.15.6.33    HTTP     Continuation
    3 0.003344  10.15.6.33      10.15.6.1     TCP      52824 > http [ACK] Seq=966073767 Ack=107601726 Win=33304
    5 0.007514  10.15.6.1       10.15.6.33    HTTP     Continuation
   10 0.061774  10.15.6.33      10.15.6.1     HTTP     GET /style.css HTTP/1.1
   11 0.067010  10.15.6.1       10.15.6.33    TCP      http > 52824 [ACK] Seq=107601857 Ack=966074200 Win=7504
   12 0.073638  10.15.6.1       10.15.6.33    HTTP     HTTP/1.1 200 OK
   13 0.073861  10.15.6.1       10.15.6.33    HTTP     Continuation
   14 0.097565  216.254.17.166  10.15.6.33    SSH      Encrypted response packet len=1448
   15 0.100457  216.254.17.166  10.15.6.33    SSH      Encrypted response packet len=1448
```

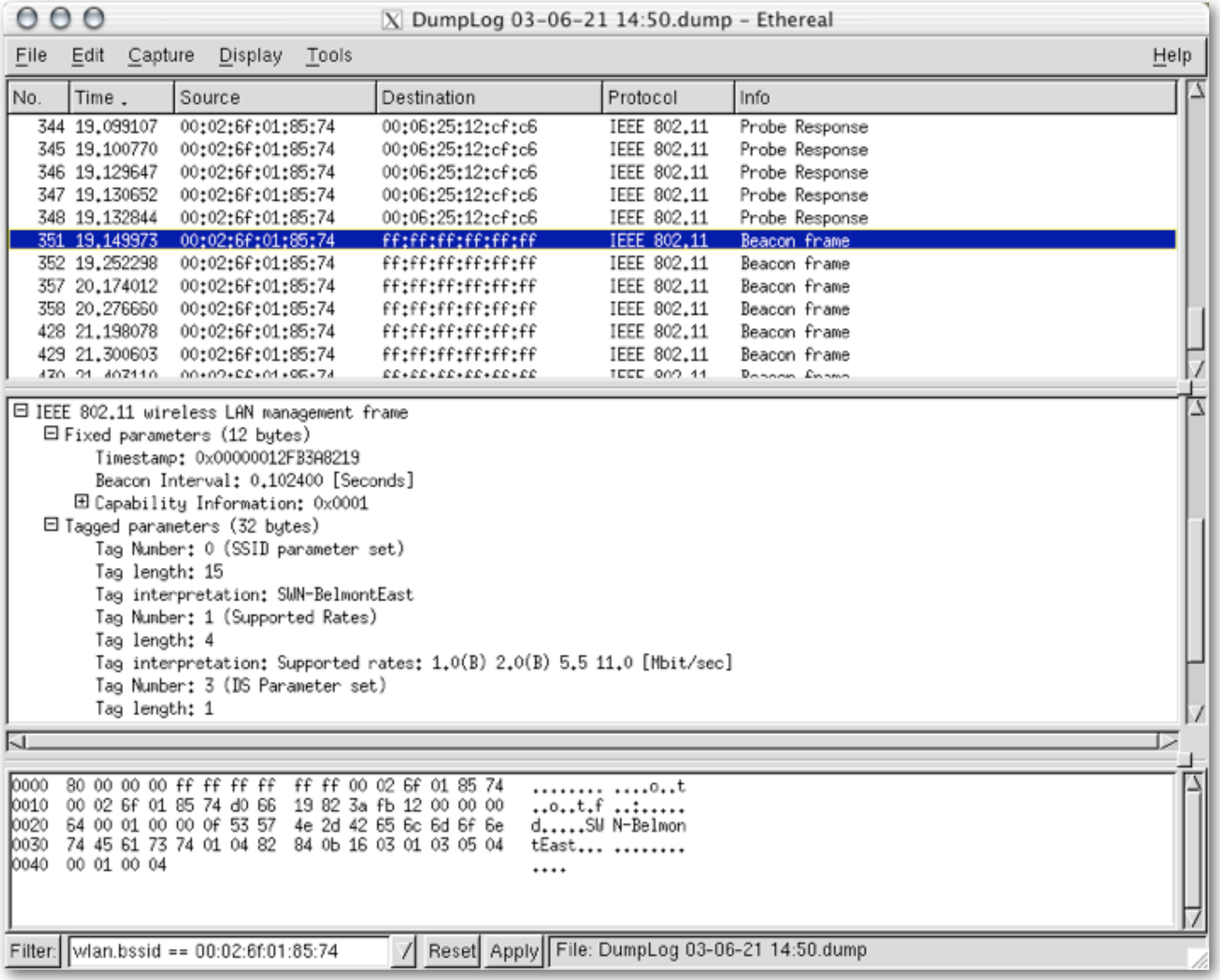
```
⊞ Frame 10 (499 bytes on wire, 499 bytes captured)
⊞ Ethernet II, Src: 00:30:65:03:e7:8a, Dst: 00:40:63:c0:aa:4b
⊞ Internet Protocol, Src Addr: 10.15.6.33 (10.15.6.33), Dst Addr: 10.15.6.1 (10.15.6.1)
⊞ Transmission Control Protocol, Src Port: 52824 (52824), Dst Port: http (80), Seq: 966073767, Ack: 107601857, Len: 433
⊟ Hypertext Transfer Protocol
    GET /style.css HTTP/1.1\r\n
    Host: muzik.rob.swn\r\n
    Connection: keep-alive\r\n
    Referer: http://muzik.rob.swn/cgi/playing?channel=Muzik\r\n
    User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en-us) AppleWebKit/74 (KHTML, like Gecko) Safari/74\r\n
    Accept: */*\r\n
    Accept-Language: en-us, ja;q=0.21, de-de;q=0.86, de;q=0.79, fr-fr;q=0.71, fr;q=0.64, nl-nl;q=0.57, nl;q=0.50, it-it;q=0.43
    \r\n
```

```
0000  00 40 63 c0 aa 4b 00 30  65 03 e7 8a 08 00 45 00   .@c..K.0 e.....E.
0010  01 e5 5e 54 40 00 40 06  ba 7f 0a 0f 06 21 0a 0f   ..^T@.@. .....!..
0020  06 01 ce 58 00 50 39 95  1d a7 06 69 df c1 80 18   ...X.P9. ...i....
0030  82 18 5d cf 00 00 01 01  08 0a b1 15 f1 44 21 63   ..]..... .....D!c
0040  8e ed 47 45 54 20 2f 73  74 79 6c 65 2e 63 73 73   ..GET /s tyle.css
0050  20 48 54 54 50 2f 31 2e  31 0d 0a 48 6f 73 74 3a    HTTP/1. 1..Host:
0060  20 6d 75 7a 69 6b 2e 72  6f 62 2e 73 77 6e 0d 0a    muzik.r ob.swn..
```

Filter: ip.addr == 10.15.6.33

=

extremely powerful wireless protocol analyzer



DumpLog 03-06-21 14:50.dump - Ethereal

```
No.  Time .     Source             Destination        Protocol     Info
 344 19.099107  00:02:6f:01:85:74  00:06:25:12:cf:c6  IEEE 802.11  Probe Response
 345 19.100770  00:02:6f:01:85:74  00:06:25:12:cf:c6  IEEE 802.11  Probe Response
 346 19.129647  00:02:6f:01:85:74  00:06:25:12:cf:c6  IEEE 802.11  Probe Response
 347 19.130652  00:02:6f:01:85:74  00:06:25:12:cf:c6  IEEE 802.11  Probe Response
 348 19.132844  00:02:6f:01:85:74  00:06:25:12:cf:c6  IEEE 802.11  Probe Response
 351 19.149973  00:02:6f:01:85:74  ff:ff:ff:ff:ff:ff  IEEE 802.11  Beacon frame
 352 19.252298  00:02:6f:01:85:74  ff:ff:ff:ff:ff:ff  IEEE 802.11  Beacon frame
 357 20.174012  00:02:6f:01:85:74  ff:ff:ff:ff:ff:ff  IEEE 802.11  Beacon frame
 358 20.276660  00:02:6f:01:85:74  ff:ff:ff:ff:ff:ff  IEEE 802.11  Beacon frame
 428 21.198078  00:02:6f:01:85:74  ff:ff:ff:ff:ff:ff  IEEE 802.11  Beacon frame
 429 21.300603  00:02:6f:01:85:74  ff:ff:ff:ff:ff:ff  IEEE 802.11  Beacon frame
```

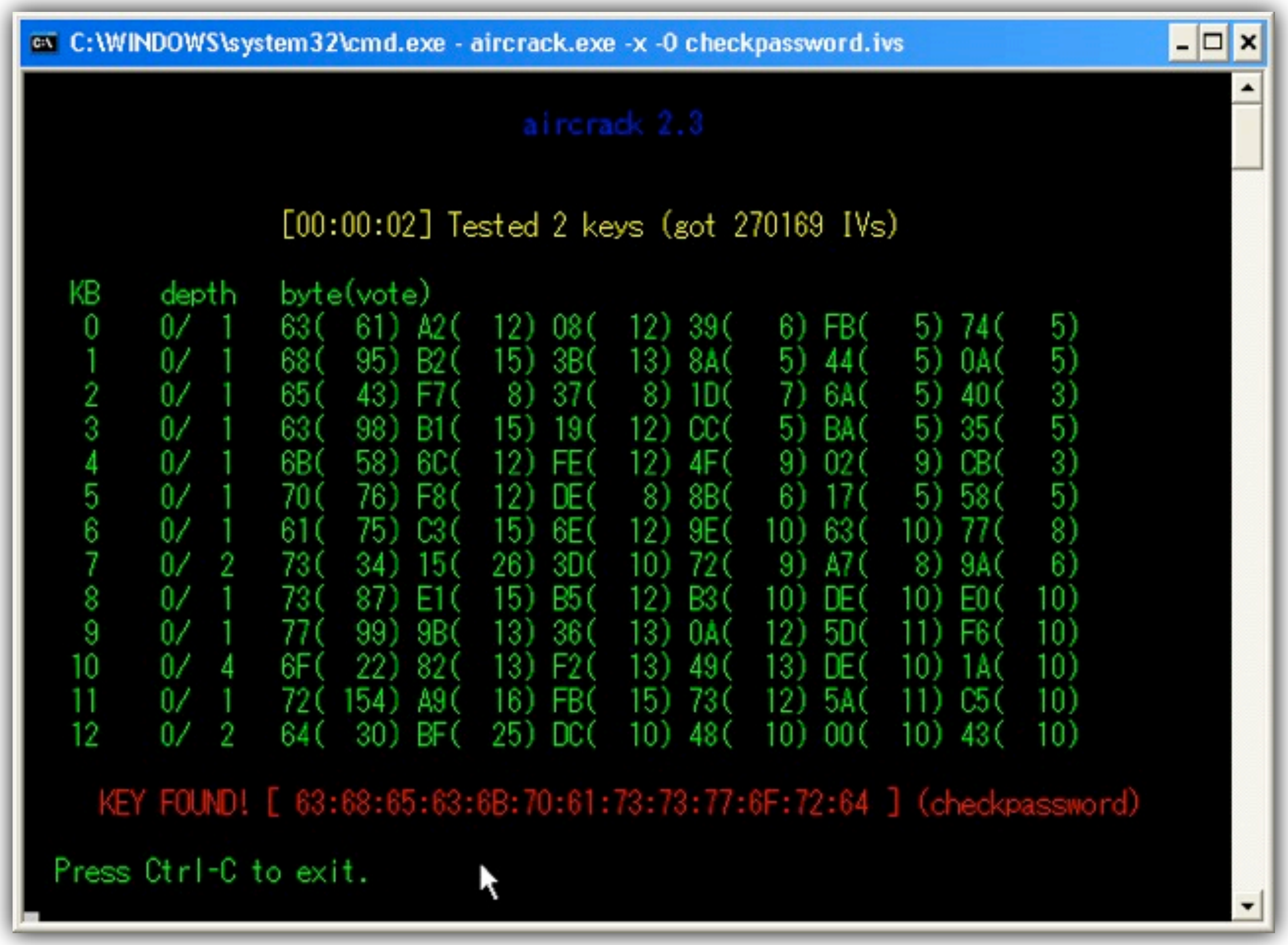
```
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters (12 bytes)
      Timestamp: 0x00000012FB3A8219
      Beacon Interval: 0.102400 [Seconds]
    ⊞ Capability Information: 0x0001
  ⊟ Tagged parameters (32 bytes)
      Tag Number: 0 (SSID parameter set)
      Tag length: 15
      Tag interpretation: SWN-BelmontEast
      Tag Number: 1 (Supported Rates)
      Tag length: 4
      Tag interpretation: Supported rates: 1.0(B) 2.0(B) 5.5 11.0 [Mbit/sec]
      Tag Number: 3 (DS Parameter set)
      Tag length: 1
```

```
0000  80 00 00 00 ff ff ff ff  ff ff 00 02 6f 01 85 74   ........ ....o..t
0010  00 02 6f 01 85 74 d0 66  19 82 3a fb 12 00 00 00   ..o..t.f ..:.....
0020  64 00 01 00 00 0f 53 57  4e 2d 42 65 6c 6d 6f 6e   d.....SW N-Belmon
0030  74 45 61 73 74 01 04 82  84 0b 16 03 01 03 05 04   tEast... ........
0040  00 01 00 04                                        ....
```

Filter: wlan.bssid == 00:02:6f:01:85:74

File: DumpLog 03-06-21 14:50.dump

AIRCRACK-NG



C:\WINDOWS\system32\cmd.exe - aircrack.exe -x -0 checkpassword.ivs

```
                              aircrack 2.3


             [00:00:02] Tested 2 keys (got 270169 IVs)

 KB    depth   byte(vote)
  0    0/  1   63(  61) A2(  12) 08(  12) 39(   6) FB(   5) 74(   5)
  1    0/  1   68(  95) B2(  15) 3B(  13) 8A(   5) 44(   5) 0A(   5)
  2    0/  1   65(  43) F7(   8) 37(   8) 1D(   7) 6A(   5) 40(   3)
  3    0/  1   63(  98) B1(  15) 19(  12) CC(   5) BA(   5) 35(   5)
  4    0/  1   6B(  58) 6C(  12) FE(  12) 4F(   9) 02(   9) CB(   3)
  5    0/  1   70(  76) F8(  12) DE(   8) 8B(   6) 17(   5) 58(   5)
  6    0/  1   61(  75) C3(  15) 6E(  12) 9E(  10) 63(  10) 77(   8)
  7    0/  2   73(  34) 15(  26) 3D(  10) 72(   9) A7(   8) 9A(   6)
  8    0/  1   73(  87) E1(  15) B5(  12) B3(  10) DE(  10) E0(  10)
  9    0/  1   77(  99) 9B(  13) 36(  13) 0A(  12) 5D(  11) F6(  10)
 10    0/  4   6F(  22) 82(  13) F2(  13) 49(  13) DE(  10) 1A(  10)
 11    0/  1   72( 154) A9(  16) FB(  15) 73(  12) 5A(  11) C5(  10)
 12    0/  2   64(  30) BF(  25) DC(  10) 48(  10) 00(  10) 43(  10)

   KEY FOUND! [ 63:68:65:63:6B:70:61:73:73:77:6F:72:64 ] (checkpassword)

Press Ctrl-C to exit.
```

COWPATTY - ATTACKING WPA/WPA2-PSK EXCHANGES

http://www.willhackforsushi.com/Cowpatty.html

- Implementation of an offline dictionary attack against WPA-PSK and WPA2-PSK networks

CHURCH OF WIFI

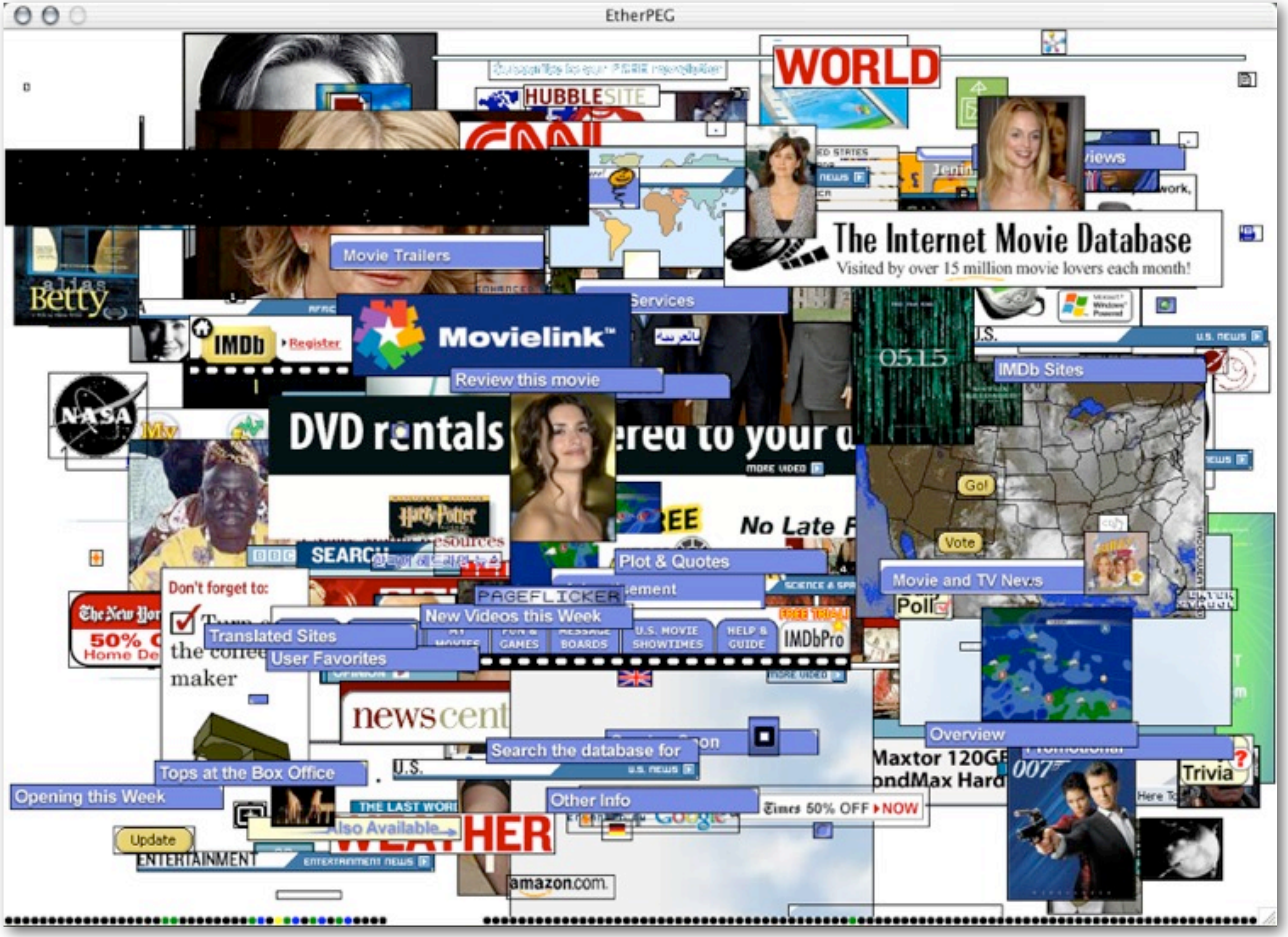
TIME TO PLAY

http://www.renderlab.net/projects/WPA-tables/

- WPA2-PSK Rainbow Tables: 1 million common passwords x 1,000 common SSIDs. 40 GB of lookup tables available on DVDs.

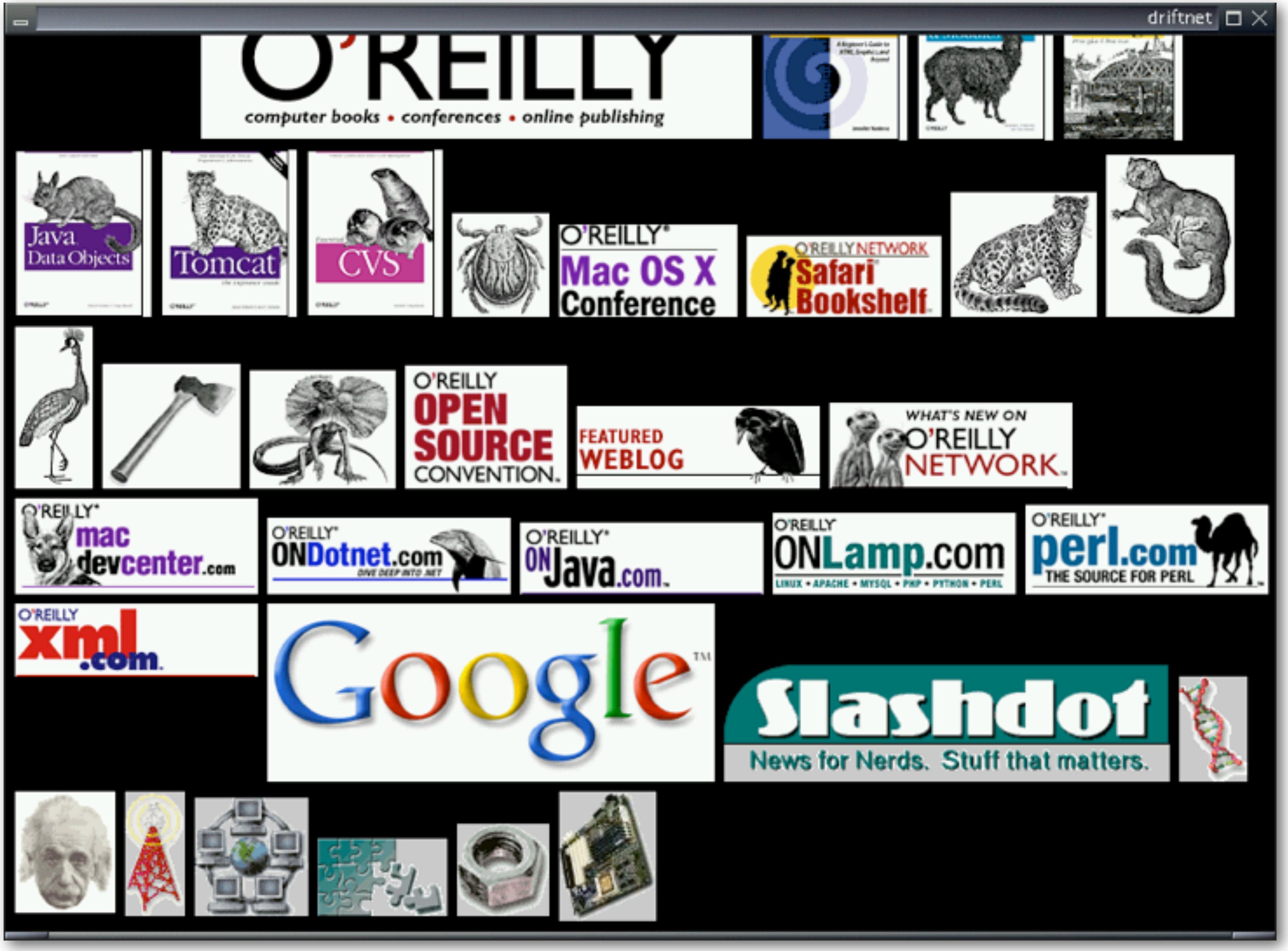
Etherpeg

http://www.etherpeg.org/

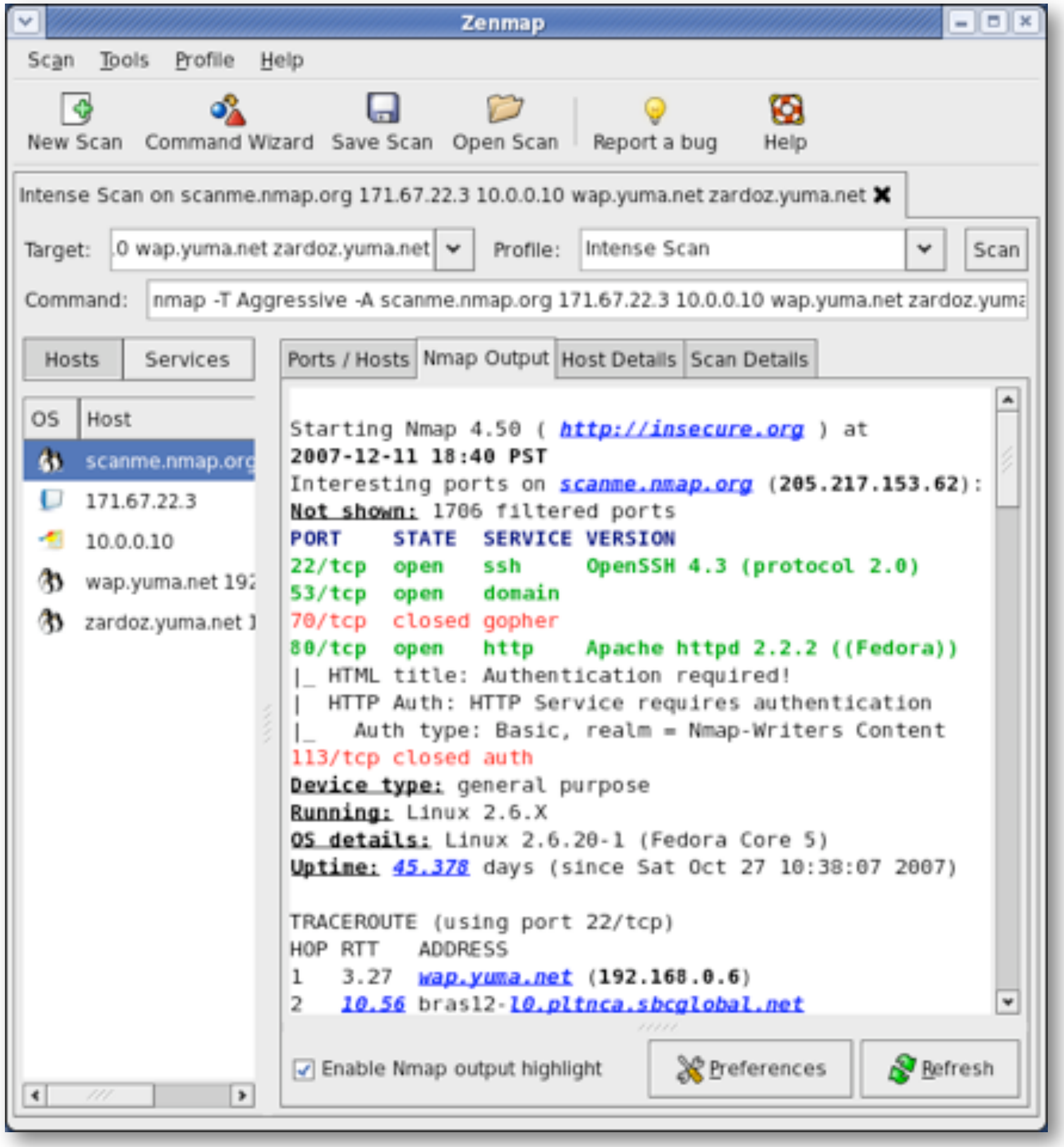


Driftnet

http://www.ex-parrot.com/~chris/driftnet/


driftnet
O'REILLY
computer books • conferences • online publishing
Java Data Objects
Tomcat
CVS
O'REILLY Mac OS X Conference
O'REILLY NETWORK Safari Bookshelf
O'REILLY OPEN SOURCE CONVENTION
FEATURED WEBLOG
WHAT'S NEW ON O'REILLY NETWORK
O'REILLY mac devcenter.com
O'REILLY ONDotnet.com DIVE DEEP INTO .NET
O'REILLY ONJava.com
O'REILLY ONLamp.com
LINUX • APACHE • MYSQL • PHP • PYTHON • PERL
O'REILLY perl.com THE SOURCE FOR PERL
O'REILLY xml.com
Google™
Slashdot
News for Nerds. Stuff that matters.

http://nmap.org/



Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net

Target: 0 wap.yuma.net zardoz.yuma.net

Profile: Intense Scan

Command: nmap -T Aggressive -A scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma

```
Starting Nmap 4.50 ( http://insecure.org ) at
2007-12-11 18:40 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
Not shown: 1706 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 4.3 (protocol 2.0)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Authentication required!
|  HTTP Auth: HTTP Service requires authentication
|_   Auth type: Basic, realm = Nmap-Writers Content
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 45.378 days (since Sat Oct 27 10:38:07 2007)

TRACEROUTE (using port 22/tcp)
HOP RTT   ADDRESS
1   3.27  wap.yuma.net (192.168.0.6)
2   10.56 bras12-10.pltnca.sbcglobal.net
```

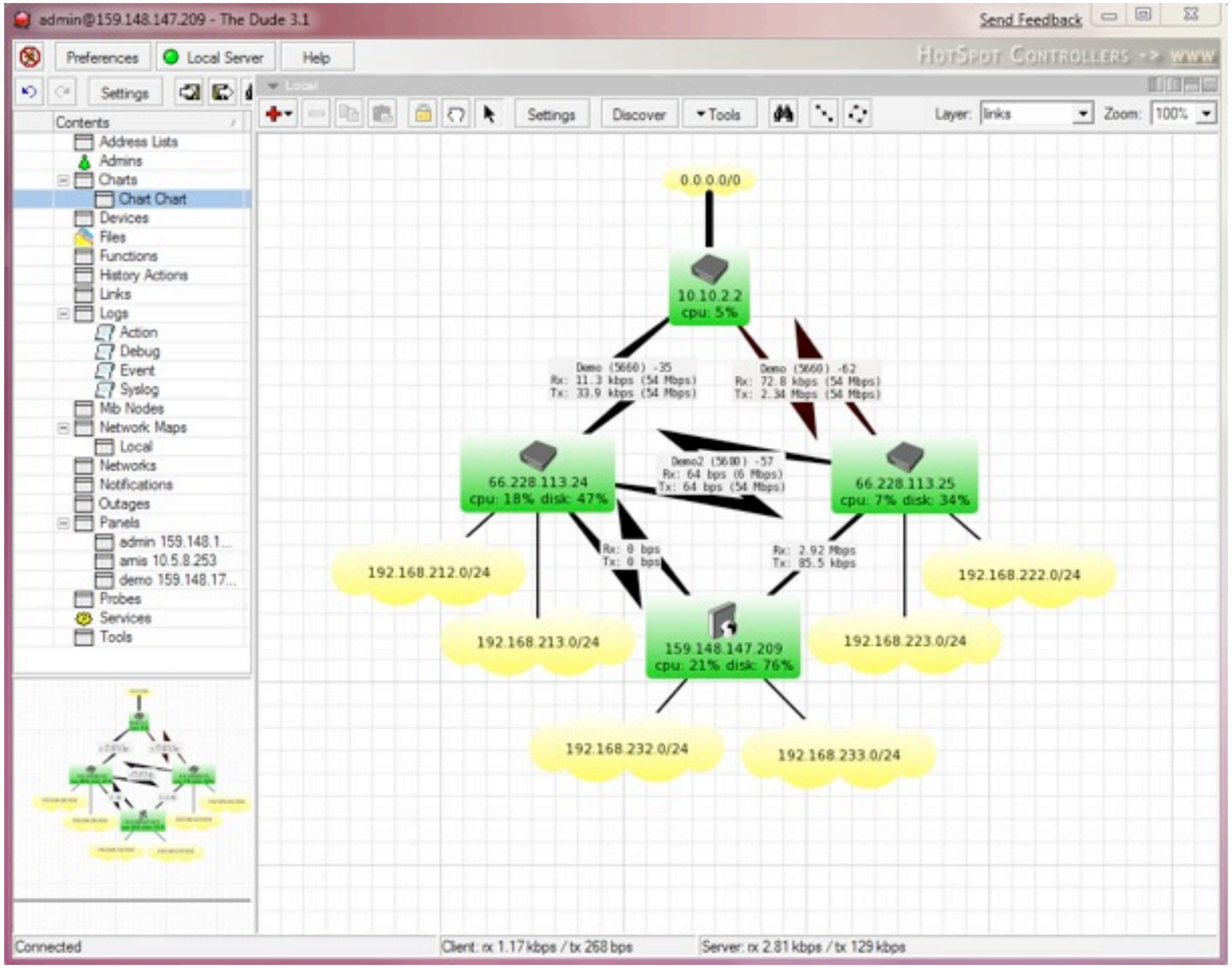
☑ Enable Nmap output highlight

- Network and port scanner
- Rogue AP detection
- Scans any number of ports on any number of hosts
- Sophisticated stealth scanning
- Idle, undetectable service “scanning”
- Available for all platforms

The Dude

http://www.mikrotik.com/thedude.php

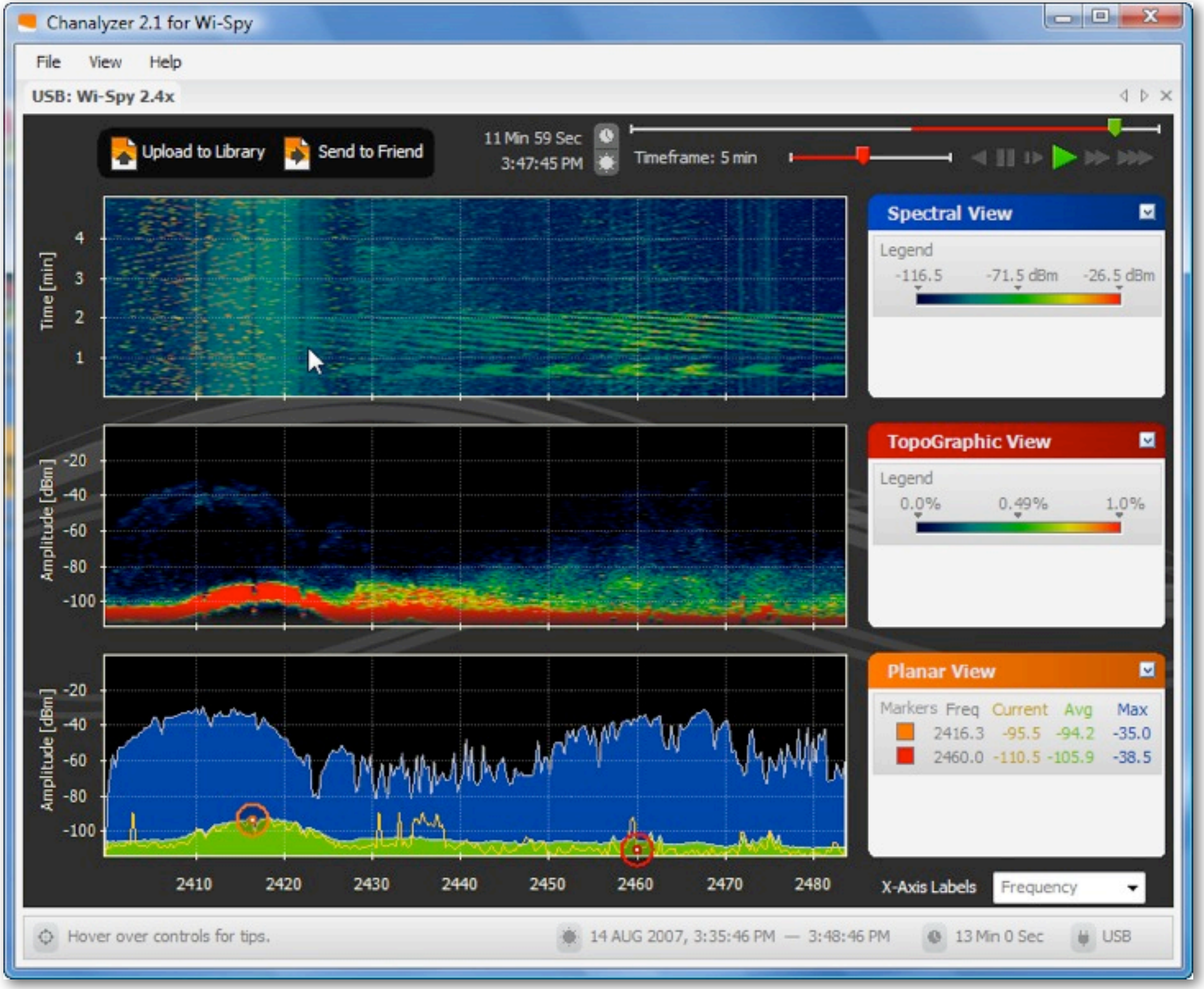
- The Dude network monitor is a network auditing and monitoring tool by MikroTik.
- The Dude automatically scans devices within specified subnets, draws a map of the networks monitors services and sends alerts when there are problems.
- Only available for Windows.



Wi-Spy spectrum analyzer

http://www.metageek.net/

Chanalyzer



11 Min 59 Sec
3:47:45 PM

Timeframe: 5 min

Markers	Freq	Current	Avg	Max
🟧	2416.3	-95.5	-94.2	-35.0
🟥	2460.0	-110.5	-105.9	-38.5

X-Axis Labels Frequency

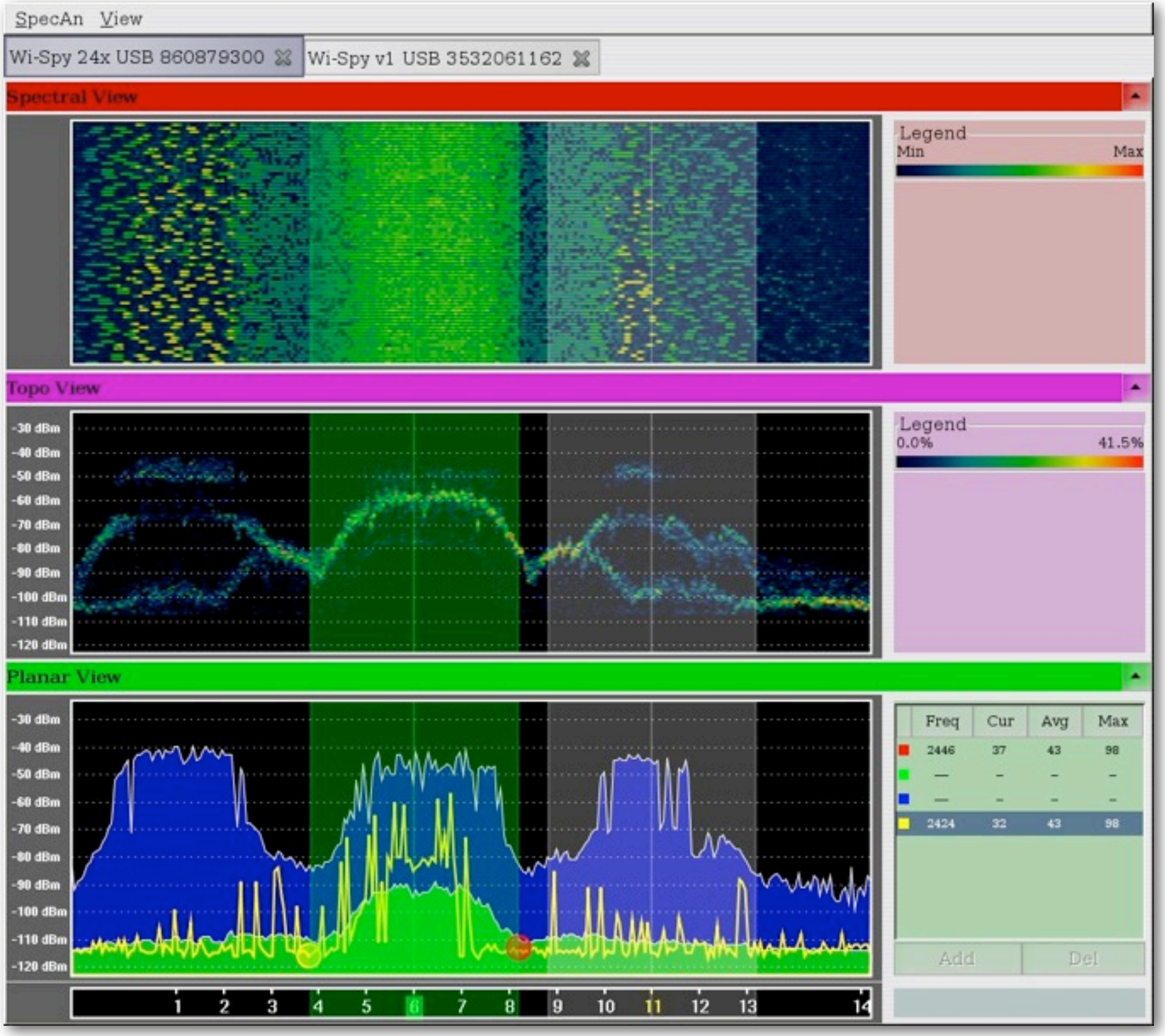
Hover over controls for tips.

14 AUG 2007, 3:35:46 PM — 3:48:46 PM

13 Min 0 Sec

USB

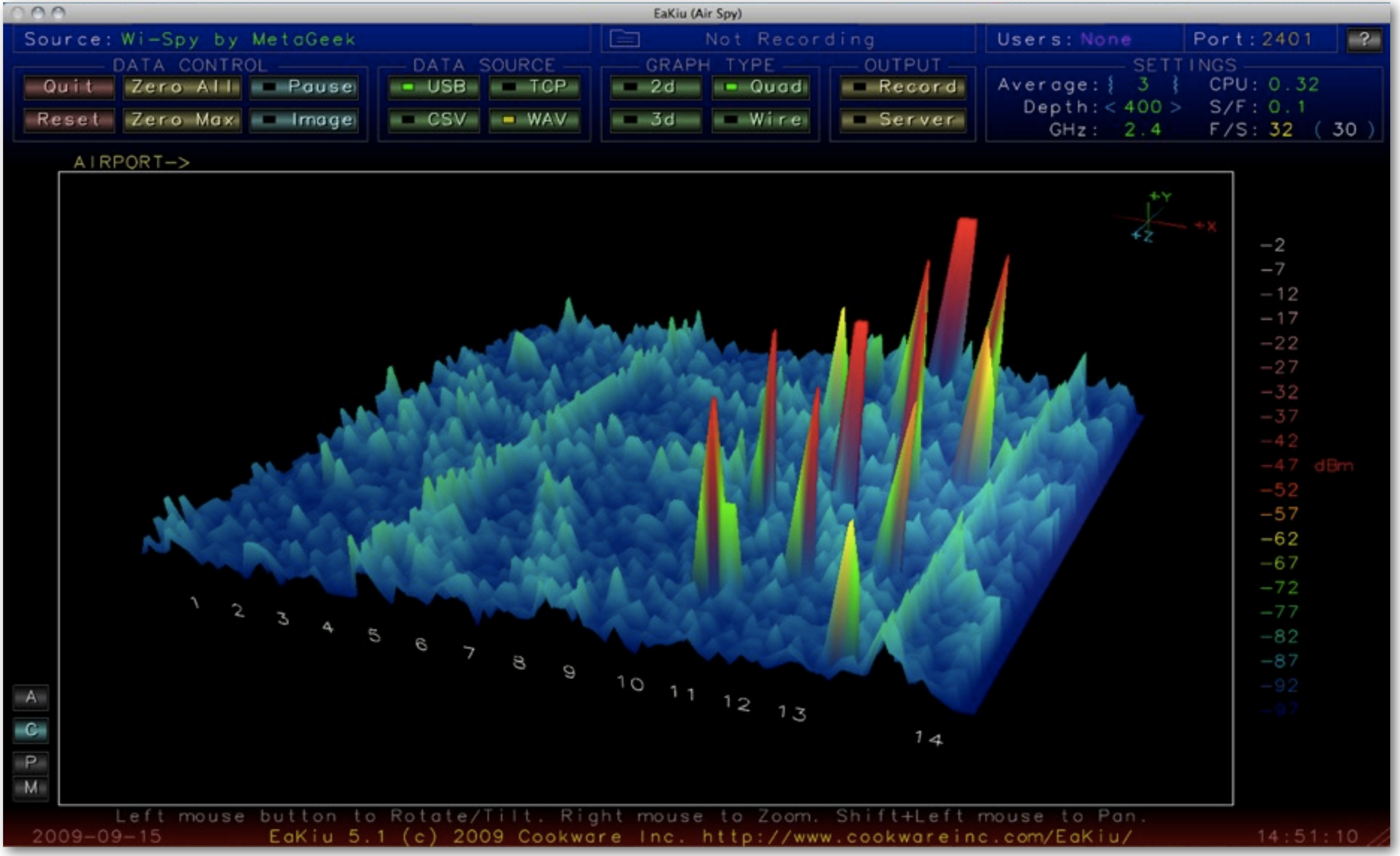
Spectools



	Freq	Cur	Avg	Max
🟥	2446	37	43	98
🟩	—	-	-	-
🟦	—	-	-	-
🟨	2424	32	43	98

EaKiu

http://www.metageek.net/



EaKiu (Air Spy)

Source: Wi-Spy by MetaGeek

Not Recording

Users: None

Port: 2401

Average: { 3 }

CPU: 0.32

Depth: < 400 >

S/F: 0.1

GHz: 2.4

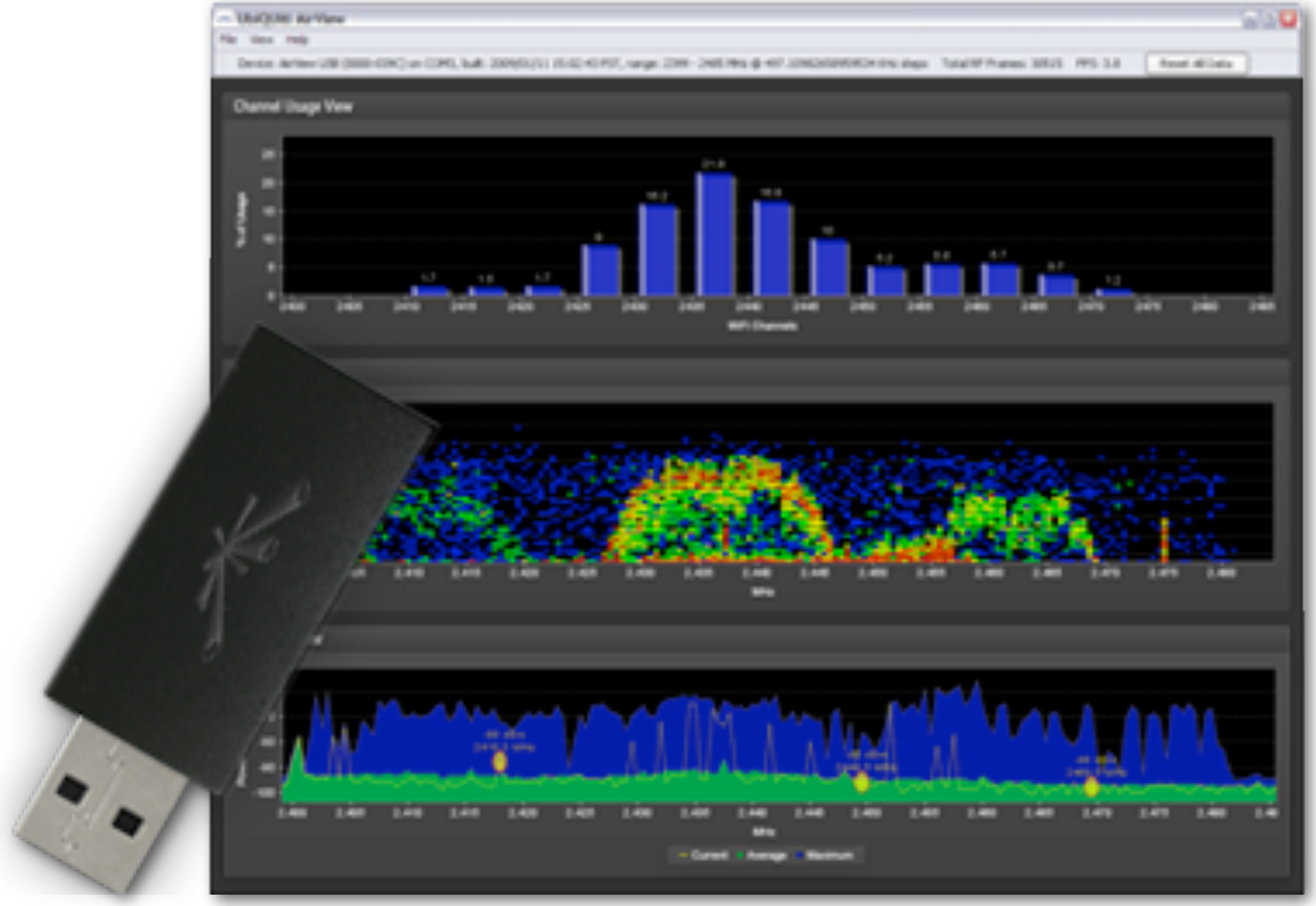
F/S: 32 (30)

Left mouse button to Rotate/Tilt. Right mouse to Zoom. Shift+Left mouse to Pan.

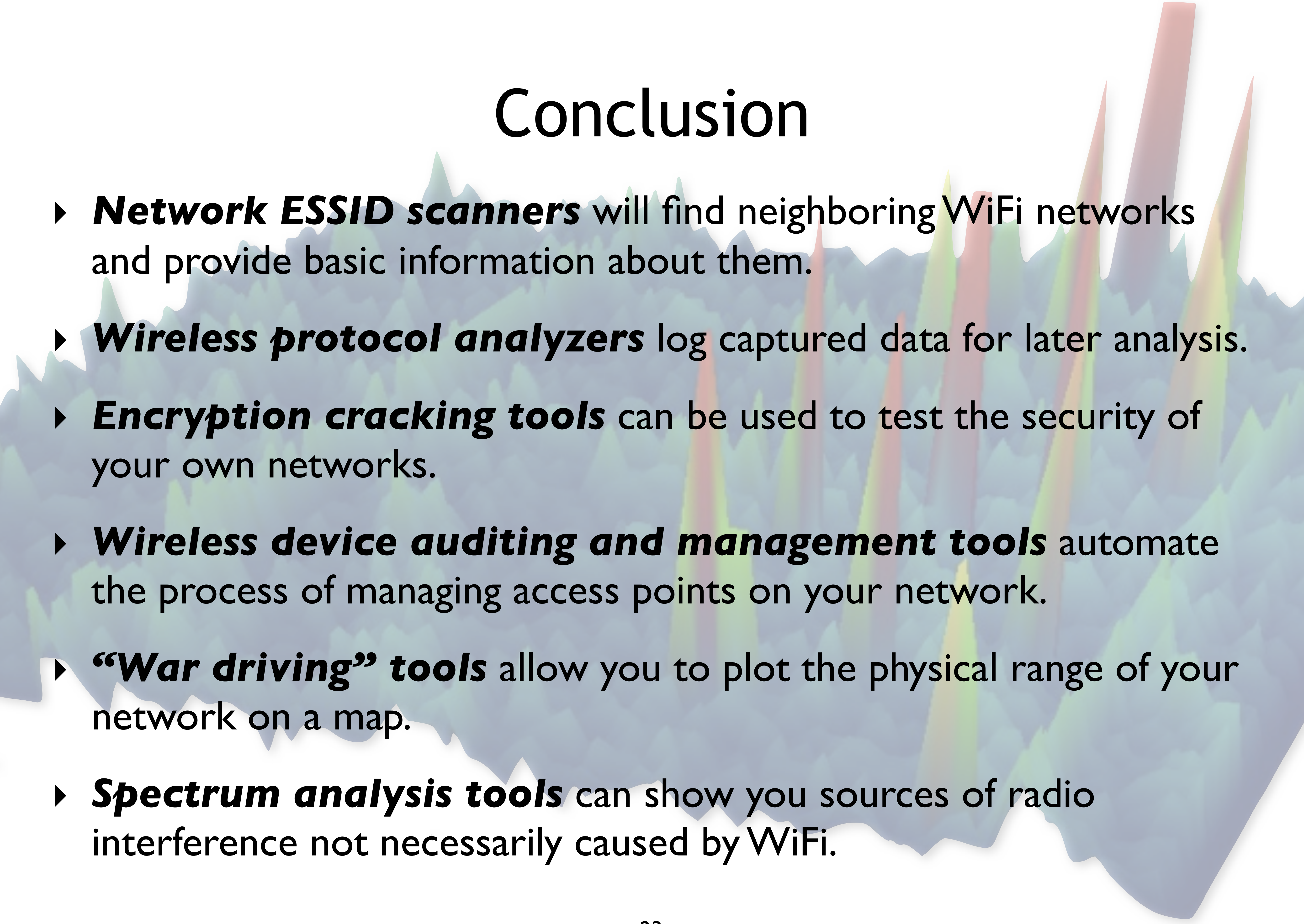
2009-09-15 EaKiu 5.1 (c) 2009 Cookware Inc. http://www.cookwareinc.com/EaKiu/ 14:51:10

Ubiquiti AirView

http://www.ubnt.com/



Conclusion



- ***Network ESSID scanners*** will find neighboring WiFi networks and provide basic information about them.
- ***Wireless protocol analyzers*** log captured data for later analysis.
- ***Encryption cracking tools*** can be used to test the security of your own networks.
- ***Wireless device auditing and management tools*** automate the process of managing access points on your network.
- ***"War driving" tools*** allow you to plot the physical range of your network on a map.
- ***Spectrum analysis tools*** can show you sources of radio interference not necessarily caused by WiFi.

Thank you for your attention

For more details about the topics presented in this lecture, please see the book ***Wireless Networking in the Developing World***, available as free download in many languages at:

http://wndw.net/

WIRELESS NETWORKING
IN THE DEVELOPING WORLD
SECOND EDITION
A practical guide to planning and building low-cost telecommunications infrastructure
wndw.net