

Wireless Tools

Training materials for wireless trainers



The Abdus Salam
**International Centre
for Theoretical Physics**

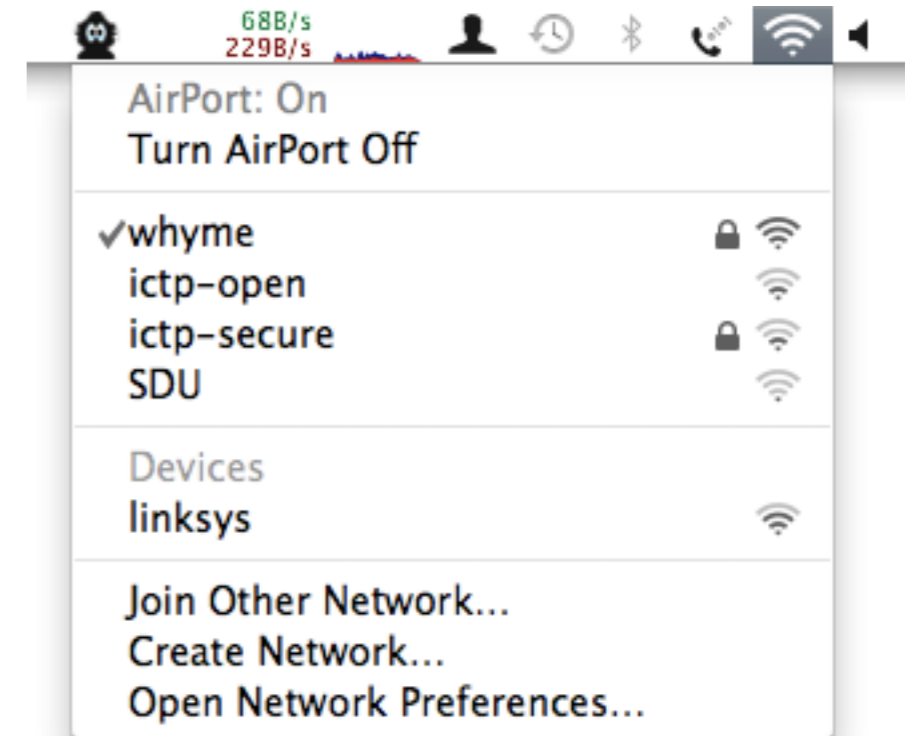
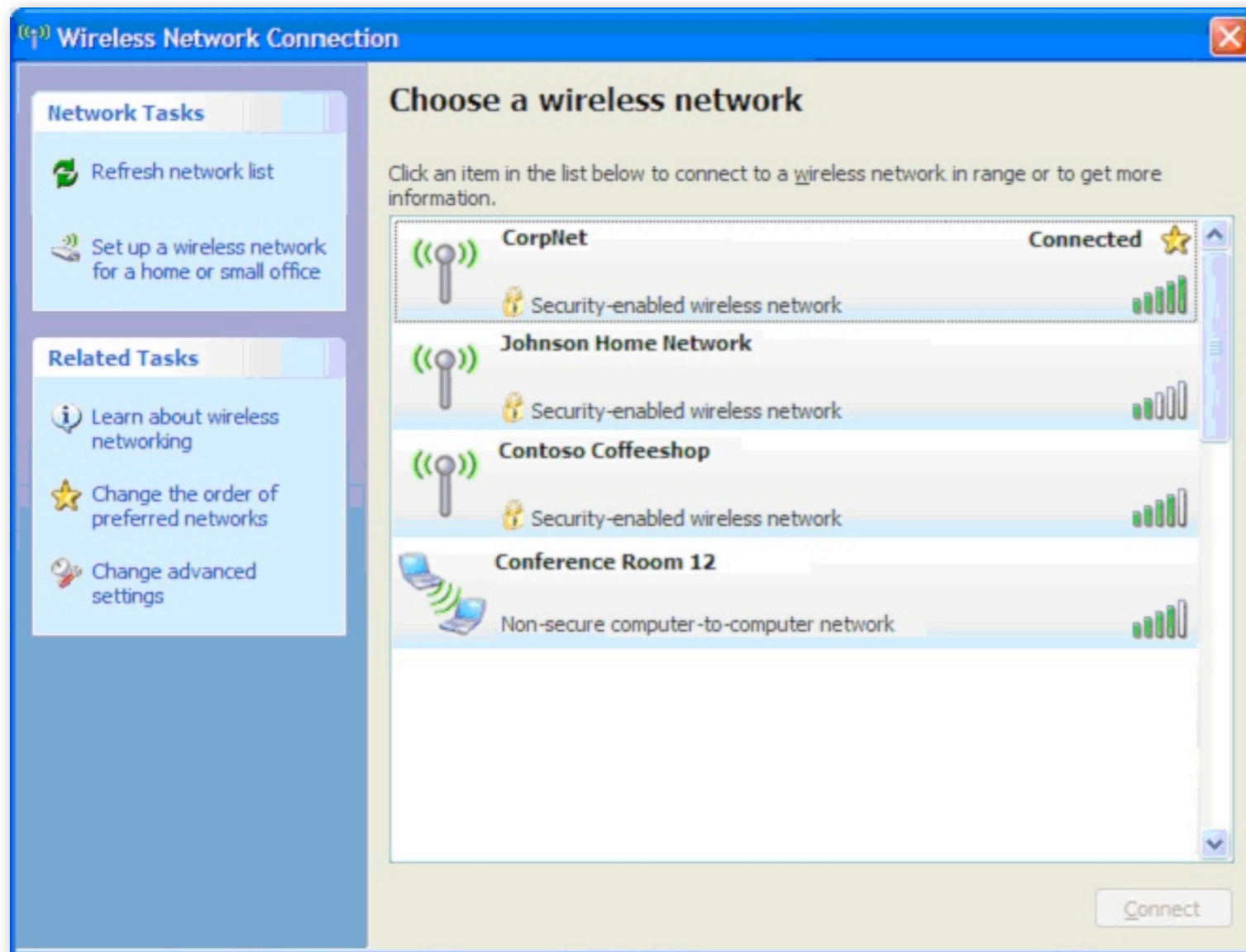
Goals

- ▶ to understand which are the software tools that may help you in:
 - ▶ monitor your WiFi network to identify problems
 - ▶ do a security auditing and prevent attacks
 - ▶ detect interferences

Types of wireless tools

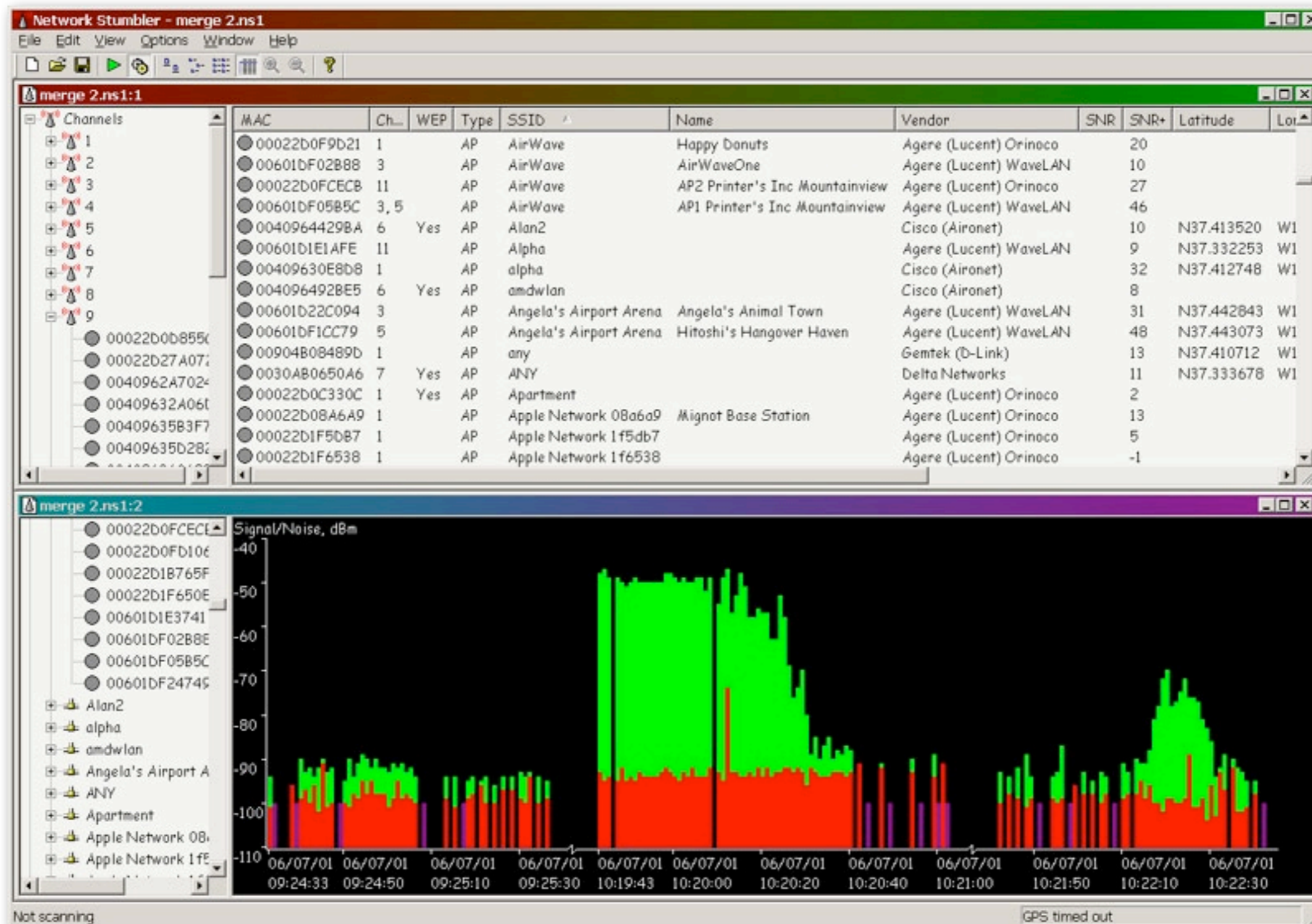
- ▶ **Network ESSID scanners**
- ▶ **Wireless protocol analyzers**
- ▶ **Encryption cracking tools**
- ▶ **Wireless device auditing and management**
- ▶ **“War driving” tools: network mapping**
- ▶ **Spectrum analysis**

Built-in wireless clients



NetStumbler

<http://www.stumbler.net>





<http://www.vistumbler.net/>

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

File Options Settings Export Extra

Stop Use GPS Active APs 1 / 507 Longitude E 0.0000000 Latitude N 0.0000000 Refresh loop (seconds): 1000 Actual loop time: 278 / 1000

Graph1 Graph2

#	Active	Mac Address	SSID	Signal	Manufacturer	Label	Auth
2	Active	00:1A:7D:75:E7:68	dd-wrt	72%	Linksys	My Wireless	Open
510	Dead	00:18:39:7D:10:50	linksys	0%	Unknown	Unknown	Open
509	Dead	00:14:BF:AC:E2:34	linksys	0%	Cisco-Linksys	Unknown	Open
504	Dead	00:13:00:05:10:15	Days+Inn	0%	Unknown	Unknown	Open
511	Dead	00:12:17:1C:93:DC	WORKGROUP	0%	Unknown	Unknown	Open
506	Dead	00:13:00:E4:21:12	Days+Inn	0%	Unknown	Unknown	Open
505	Dead	00:13:00:71:6B:FF	Days+Inn	0%	Unknown	Unknown	Open
508	Dead	00:00:0B:5D:78:FF		0%	Unknown	Unknown	Open
499	Dead	00:18:39:75:F4:7C	Meringold	0%	Unknown	Unknown	Open
502	Dead	1E:AB:CS:81:29:8E	hpsetup	0%	Unknown	Unknown	Open
501	Dead	00:18:F8:E4:25:D6	Ellen	0%	Cisco-Linksys	Unknown	Open

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

File Options Settings Export Extra

Scan APs Use GPS Active APs 0 / 507 Longitude E 0.0000000 Latitude N 0.0000000 Refresh loop (seconds): 1000 Actual loop time: 278 / 1000

Graph1 Graph2

#	Active	Mac Address	SSID	Signal	Manufacturer	Label	Authentication	Channel	Encryption	Network Type	Latitude	Longitude	Manufacturer	Label
67	Active	00:05:52:0C:FC:00	HolidayExpress	18%			Open	6	None	Infrastructure	N 42.3140033	W 72.3252000	Cyberis	Unknown
66	Active	00:18:F8:E2:F3:1A	linksys	38%			Open	6	None	Infrastructure	N 42.3140033	W 72.3252000	Cisco-Linksys	Unknown
65	Active	00:12:08:85:48:7E	STYDORCROSS	18%			Open	6	WEP	Infrastructure	N 42.3142933	W 72.3260611	AboCom	Unknown
64	Dead	00:12:08:84:87:CA	Shelbridge Coffee HL	0%			Open	6	None	Infrastructure	N 42.3143000	W 72.3264413	AboCom	Unknown
63	Dead	00:00:0B:5D:78:FF		0%			Open	6	None	Infrastructure	N 42.3146387	W 72.3273200	AboCom	Unknown
62	Dead	00:14:8F:75:26:68	linksys_3E5_2504	0%			WPA-Personal	TXOP	TKIP	Infrastructure	N 42.3144700	W 72.3267787	Cisco-Linksys	Unknown

GPS Details

Quality: 1	Status: 4
GPSHW	GPSHW
Time: 6:16:10PM (GMT)	Time: 6:16:10PM (GMT)
Date: 11/11/08	Date: 11/11/08
Latitude: N 42.066387	Latitude: N 42.066387
Longitude: W 72.062752	Longitude: W 72.062752
Speed (MPH): 21.35	Horizontal Dilution: 1.2
Speed (MPH): 22.75 MPH	Altitude: 615.81345238
Speed (MPH): 34.36 MPH	Height of Gpsd: 34.38
Track Angle: 154.28	

GPS Compass

Kismet

<http://www.kismetwireless.net/>

Channels View

Signal
Noise

Networks Active

Networks
Active

Kismet Sort View Windows

Name	BSSID	T	C	Ch	Freq	Pkts	Size	Bcr%	Sig	Clnt	Manuf	Cty	Seen By
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
Autogroup Probe	00:13:E8:92:3F:CB	P	N	---	---	2	0B	---	0	1	IntelCorpo	---	wlan0
linksys	00:1A:70:D9:BC:13	A	N	6	2437	2	0B	10%	-86	1	Cisco-Link	---	wlan0
MPA41	00:1F:90:E6:E0:84	A	W	11	2462	3	0B	---	-86	1	ActiontecE	---	wlan0
6SI03	00:1F:90:FA:F4:CB	A	W	---	2412	3	0B	---	-83	1	ActiontecE	---	wlan0
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
TK421	00:18:01:FE:68:77	A	0	6	2437	4	0B	---	-79	1	ActiontecE	---	wlan0
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
7J4R0	00:1F:90:E6:04:F1	A	W	11	2462	7	0B	---	-80	1	ActiontecE	---	wlan0
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													
38cB	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)
45

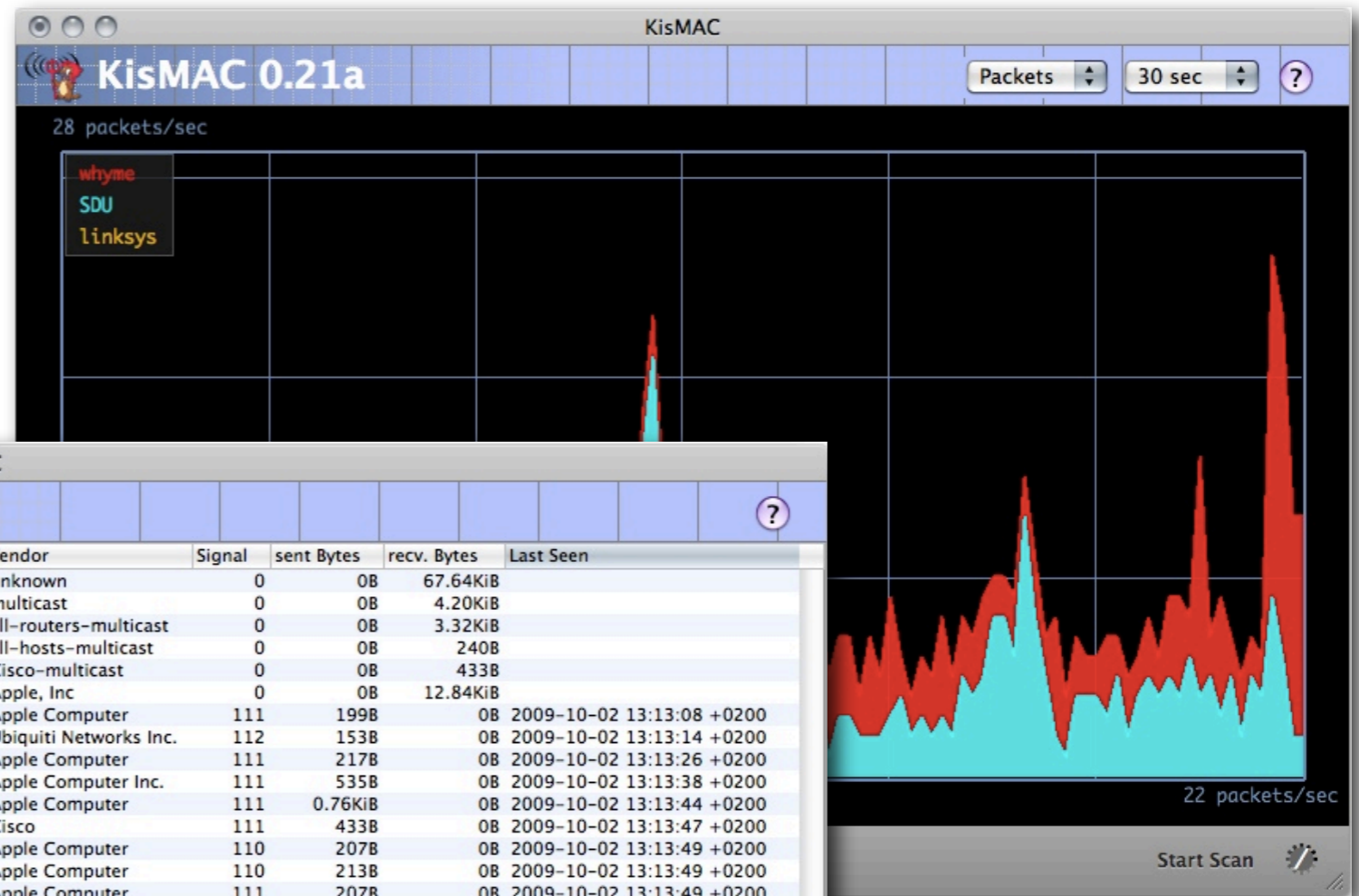
Packets
Data

```

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
INFO: Detected new managed network "linksys", BSSID 00:1A:70:D9:BC:13, encryption no, channel 6, 54.00 mbit
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
    
```

KisMAC

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



KisMAC 0.21a

Property	Setting
SSID	whyne
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

Comment:

Start Scan

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

File View Opt Spd GPS

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
- Hidden**
Strength: 20 Channel: 8 Open

No Service 3:19 PM

Settings **Wi-Fi Networks**

Wi-Fi ON

Settings

Settings

Networks

	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	12	
andyford 00:1b:2f:92:02:71	13	
WIREFREE 00:17:3f:ed:46:6c	6	

Networks Radar Logging

NOKIA

-Network List- (Autofit)

Name	T	W	Ch	Pkts	Flags
<no ssid>	A	Y	001	120	
<no ssid>	G	M	011	459	6
<no ssid>	A	Y	011	152	
<no ssid>	A	Y	011	155	
<no ssid>	A	Y	011	146	
<no ssid>	A	Y	011	155	
<no ssid>	A	Y	011	156	
<no ssid>	A	Y	011	135	
Schiphol-Group	A	M	011	302	T2
<no ssid>	A	O	011	129	
<no ssid>	A	O	011	215	T4
KPM	A	Y	001	114	
<no ssid>	A	Y	001	108	
KPM	A	Y	001	97	
<no ssid>	A	Y	001	89	
Schiphol-Group	A	O	001	1	
<no ssid>	A	O	011		

Status
Associated probe network "00:19:02:..." with "00:16:CA:..." via data.
Found new network "<no ssid>" bssid 00:16:CA:... 18.00 mbit

Font

```

ls
--Networks--(First Seen)-----Info-----
Name      T W Ch Pkts  ll
-----
Network Details-----
Name      : Nerva
SSID      : nerva
BSSID     : 00:04:5A:2E:3D:C1
Max Rate  : 11.0
First     : Tue Jan 1 00:16:55 20
Latest    : Tue Jan 1 00:30:05 20
Type      : Access Point (infrastr
Channel   : 6
WEP       : Yes
Beacon    : 100 (0.102400 sec)
Packets   : 358
Data      : 12
LLC       : 341
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

12:30 AM



Network List (Channel)

Name	T	W	Ch	Packets	Flags	IP Range
! SWN-BelmontEast	A	N	03	1370	T	0.0.0.0
tamtam	A	Y	05	74		0.0.0.0
! Wireless	A	N	06	1312	U3	192.168.0.0
! SpeedStream	A	N	11	850	T	0.0.0.0

Info

Ntwrks: 4
Packets: 3606
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

<capture> - Ethereal

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\nHost: muzik.rob.swn\r\nConnection: keep-alive\r\nReferer: http://muzik.rob.swn/cgi/playing?channel=Muzik\r\nUser-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en-us) AppleWebKit/74 (KHTML, like Gecko) Safari/74\r\nAccept: */*\r\nAccept-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\r\n

0000 00 40 63 c0 aa 4b 00 30 65 03 e7 8a 08 00 45 00 .@c..K.O e.....E.
0010 01 e5 5e 54 40 00 04 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..
0070 42 6f 6a 6a 65 63 74 69 6f 6a 2a 20 6b 65 65 70 Connecti on: keep

Filter: ip.addr == 10.15.6.33 [Reset] [Apply] File: <capture> Drops: 0

=
extremely
powerful
wireless
protocol
analyzer

The screenshot shows the Wireshark interface with a packet list table. The selected packet (No. 351) is an IEEE 802.11 Beacon frame. The details pane shows the structure of the beacon frame, including fixed parameters, capability information, and tagged parameters such as SSID (SWN-BelmontEast) and supported rates.

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
430	21.402110	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 [v] [Reset] [Apply] File: DumpLog 03-06-21 14:50.dump



```
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



<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.

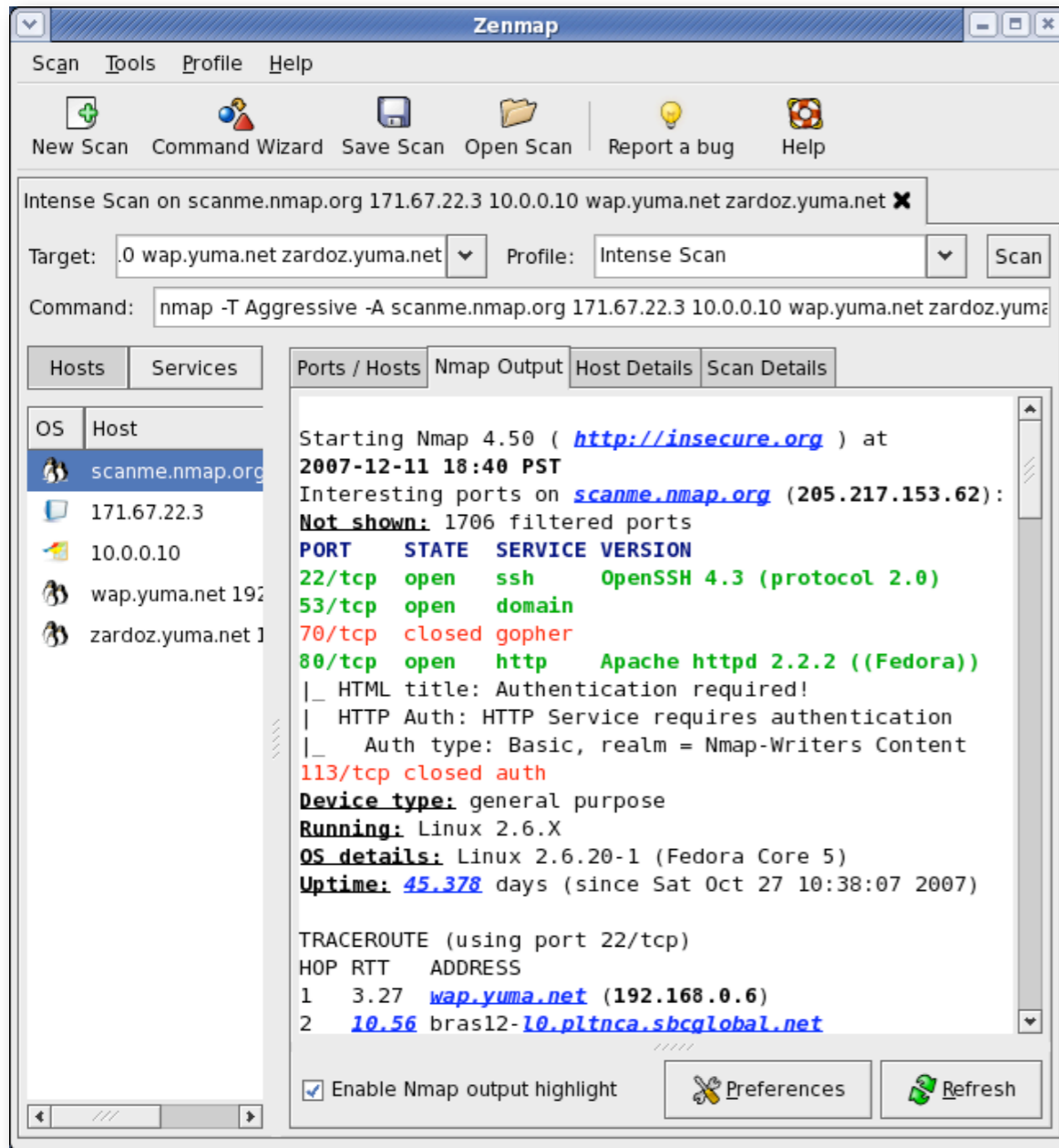
Driftnet

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





<http://nmap.org/>

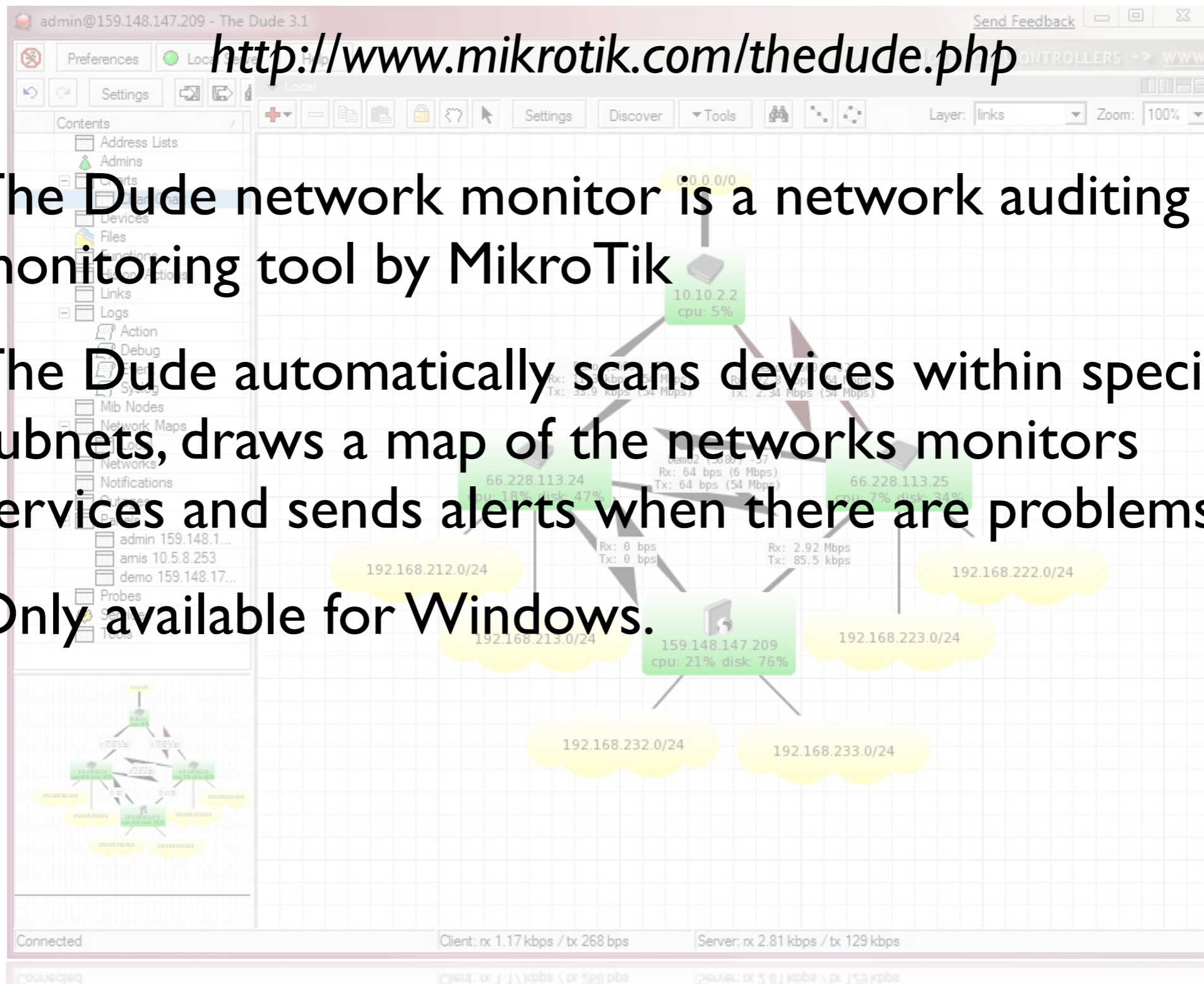


- ▶ Network and port scanner
- ▶ Rogue AP detection
- ▶ Scans any number of ports on any number of hosts
- ▶ Sophisticated stealth scanning
- ▶ Idle, undetectable service “scanning”
- ▶ Available for all platforms

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.

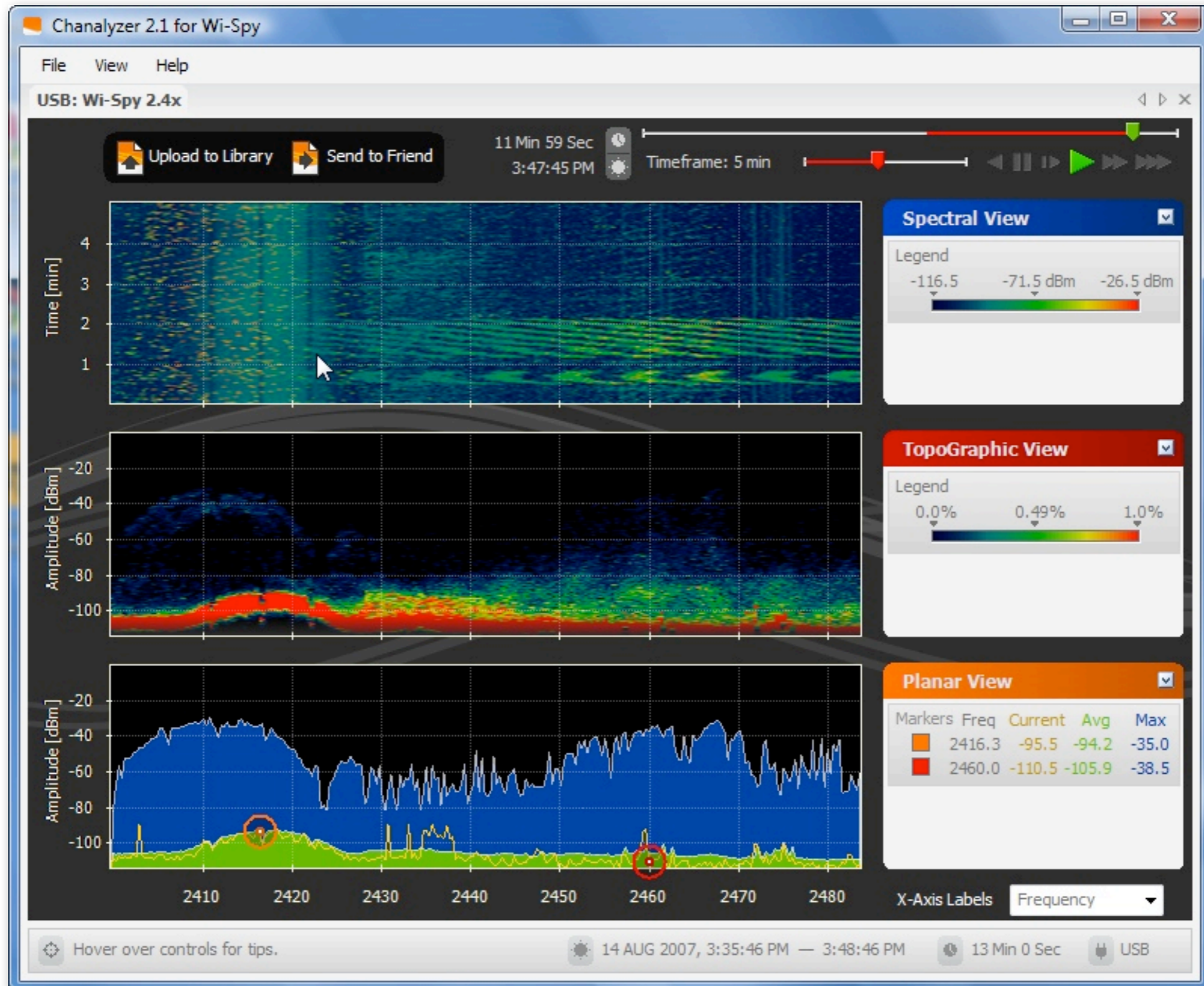


Wi-Spy spectrum analyzer

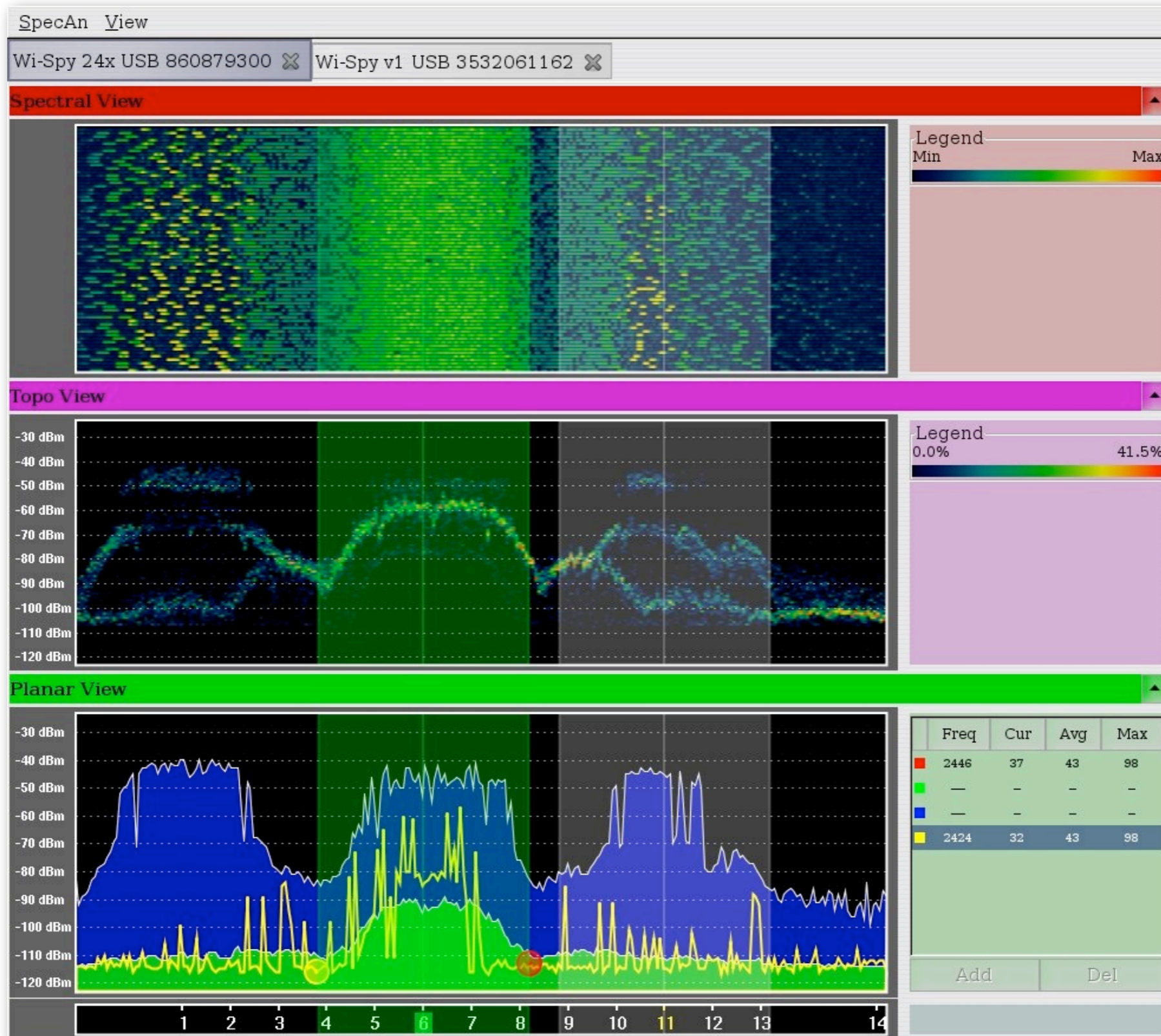
<http://www.metageek.net/>



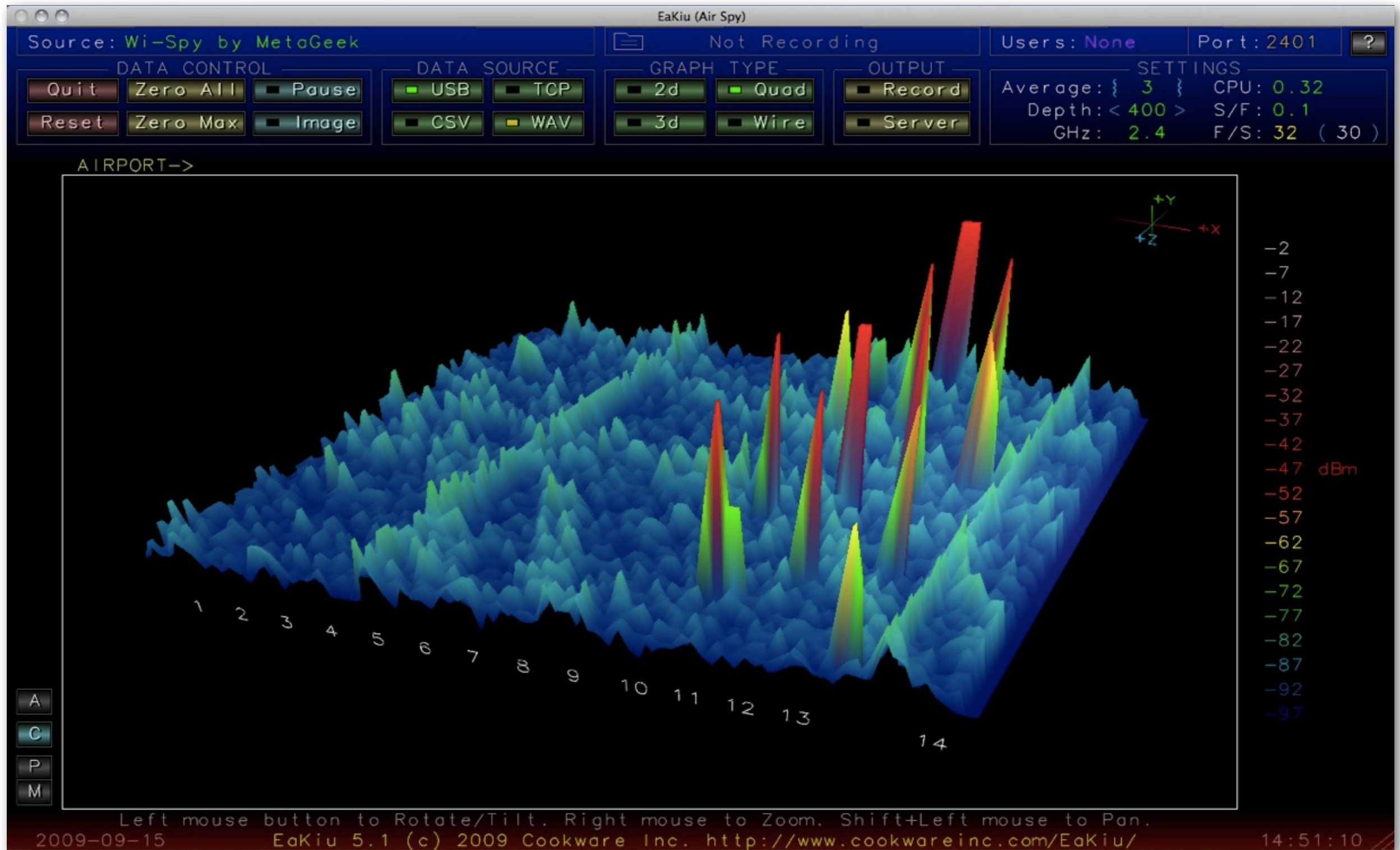
Chanalyzer



Spectools

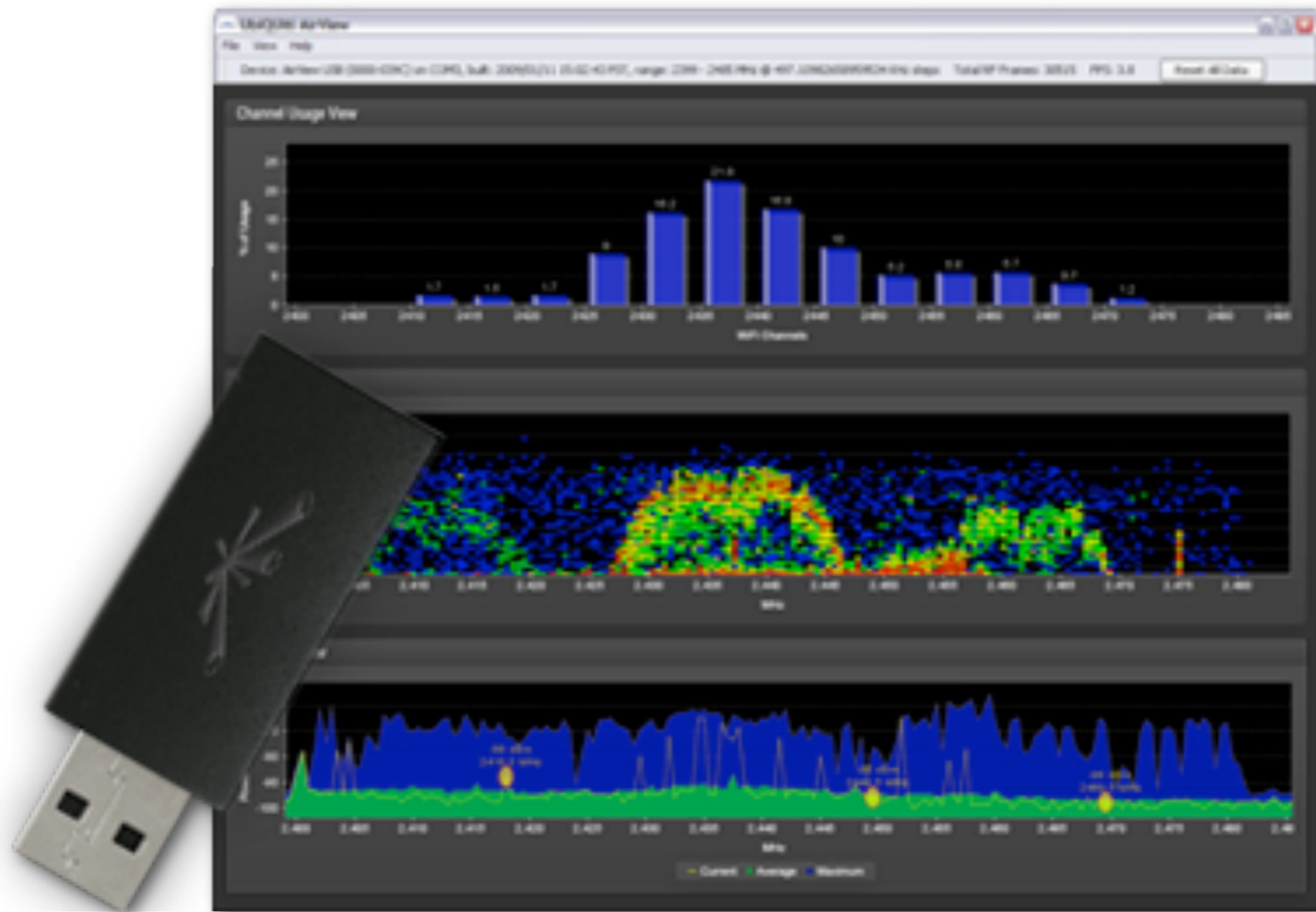


EaKiu



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>

