

Wireless Tools

Joel Jaeggli

For

AIT Wireless Security Workshop

Tools

- NetStumbler
- Inssider
- Kismet
- Wi-Spy
- Embedded Tools in commercial APs
- AirSnort
- AirCrack (Ng)

Netstumbler (the granddaddy)

The screenshot displays the Network Stumbler application window. The title bar reads "Network Stumbler - [20080610184454]". The menu bar includes "File", "Edit", "View", "Device", "Window", and "Help". The toolbar contains various icons for file operations and network management. On the left, there is a sidebar with "Channels", "SSIDs", and "Filters" sections. The main area is a table listing detected APs.

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	SNR	Signal+	Noise-	SNR+	IP Addr	Subnet	Latitude	Longitude	First Seen
00156DA62669	wsws-2		6	11 Mbps	(Fake)	AP		19	-81	-100	19			N14°4.651'	E100°36.758'	18:45:02
00156DA626D9	wsws-1		6	11 Mbps	(Fake)	AP		19	-80	-100	20			N14°4.651'	E100°36.758'	18:45:02
00156DA66B06	wsws-3		6	11 Mbps	(Fake)	AP		19	-80	-100	20			N14°4.651'	E100°36.758'	18:45:02
00022D328189	Interlab AP-1A		1	11 Mbps	Proxim (...)	AP	WEP	27	-72	-100	28			N14°4.651'	E100°36.758'	18:45:02
00156DA66B14	wsws-5		11	11 Mbps	(Fake)	AP		29	-71	-100	29			N14°4.651'	E100°36.758'	18:45:02
00156DA655A1	wsws-4		6	11 Mbps	(Fake)	AP		30	-70	-100	30			N14°4.651'	E100°36.758'	18:45:02
000D0BFA837D	WS-workshop		1	54 Mbps		AP		47	-45	-100	55			N14°4.651'	E100°36.758'	18:45:02

The taskbar at the bottom shows the system tray with "7 APs active" and "GPS: N14°4.651' E100°36.758'". The system clock indicates the time is 18:45.

Netstumbler

- Windows APP
- Kicked off the notion of “war driving” the idea of driving around looking for open aps
- That's interesting but it's more useful as a survey tool.
- Not frequently updated anymore. As a result it's somewhat picky about the use of newer wireless cards and also it's a bit of a challenge to get it to run reliably on Windows Vista.

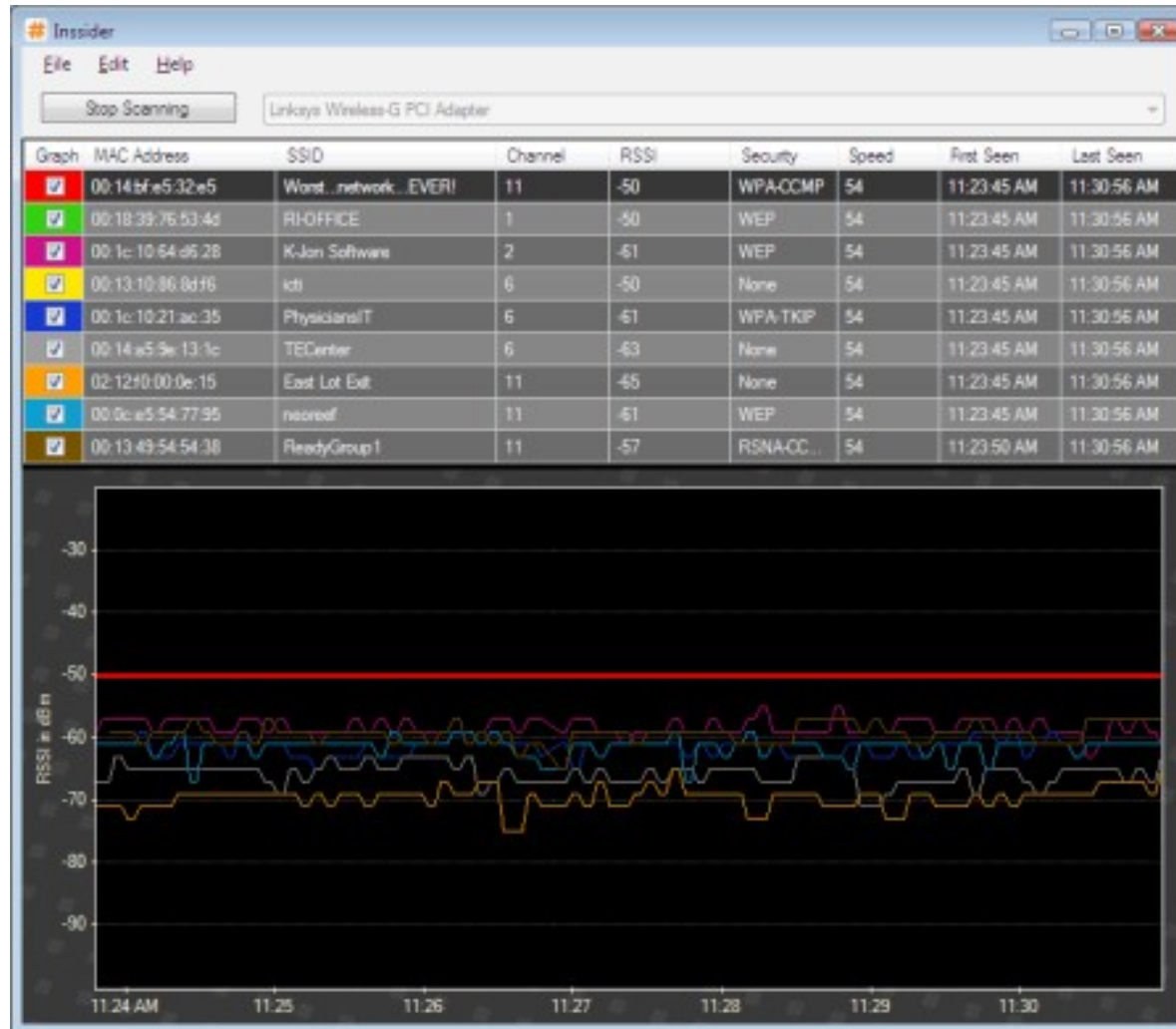
Netstumbler

- The addition of a GPS makes it useful RF surveys with 3rd party data reduction tools, which are unfortunately fairly rare and of indifferent quality.

Inssider

- Open source scanner developed at metageek
- Works well on Vista
- Supports a wide variety of chipsets
- No gps support yet
- Released march 2008

Inssider

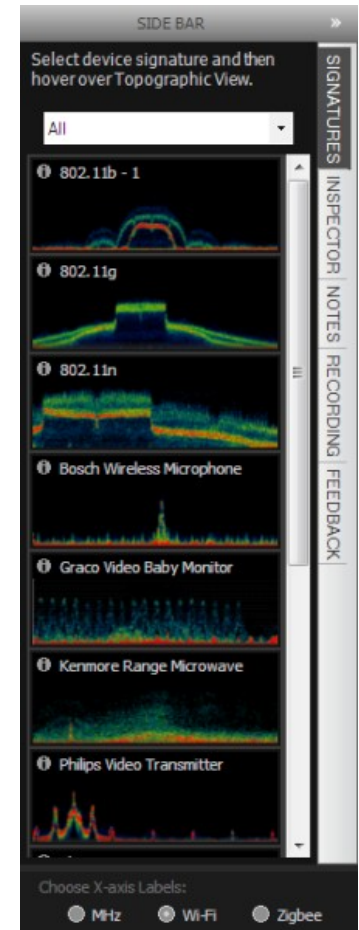
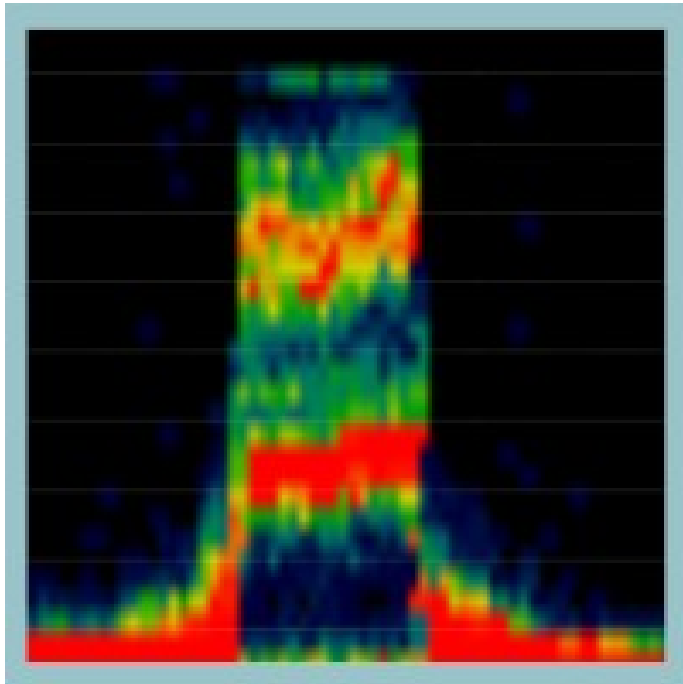


Wi-Spy

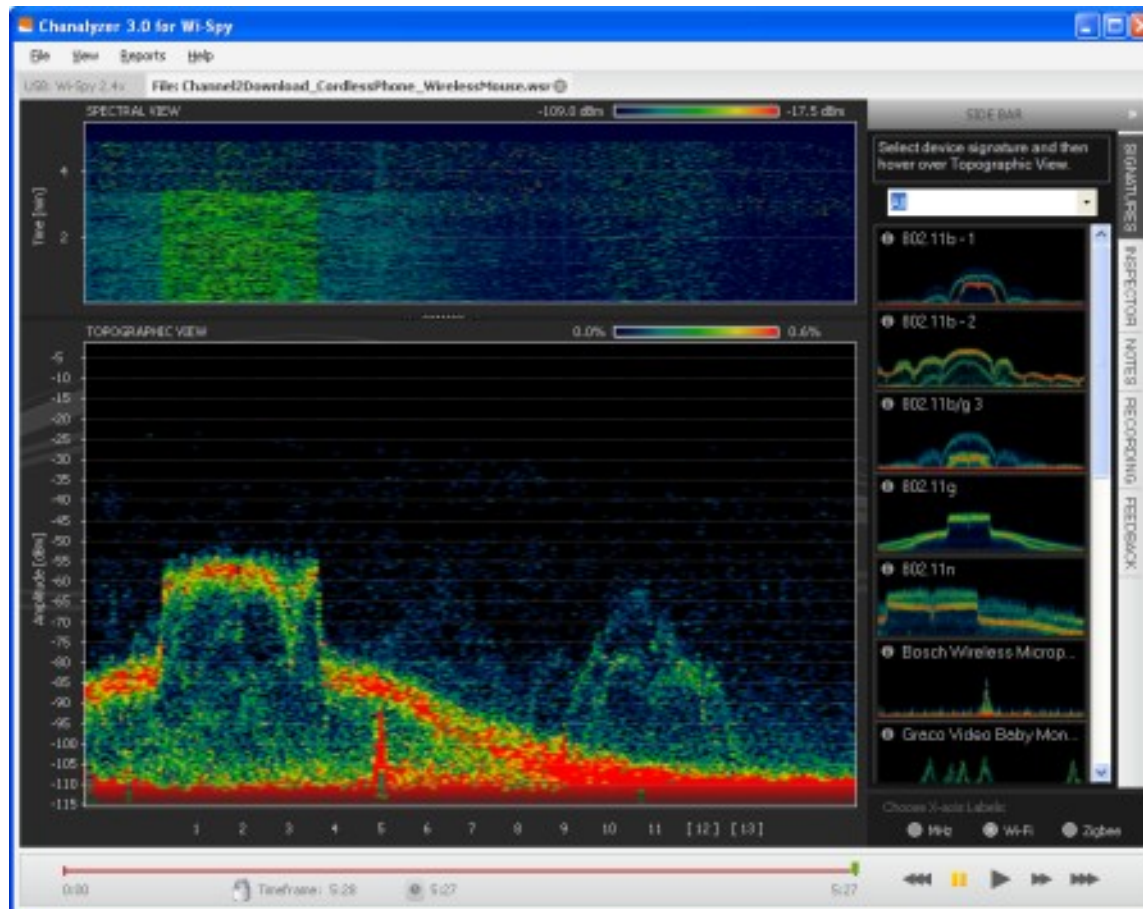


- Also from metageek
- When I first started shopping for wireless spectrum analyzers for the microwave band they were \$10,000
- Wi-Spy is \$399 or \$99 depending on version.

Wi-Spy



Wi-Spy



Wi-Spy

- Unfortunately no 5Ghz version
 - Sadly that piece of kit is still \$2500
- Spectrum analyzer is used in conjunction With a wireless survey tool and a other wireless survey tools

Kismet

- Kismet is:
 - an 802.11 layer2 wireless network detector
 - sniffer
 - and intrusion detection system
- Utilizes a client server model, which means
 - Distributed network probes
 - At tool you deploy into your network and leave ips services

Kismet

```
jaeggli@winged-monkey:/etc/kismet
```

Network List (Autofit)							Info
Name	T	W	Ch	Packts	Flags	IP Range	Ntwrks
. WS-workshop	A	N	001	33		0.0.0.0	1

Pckets
35

Cryptd
0

Weak
0

Noise
0

Discrd
0

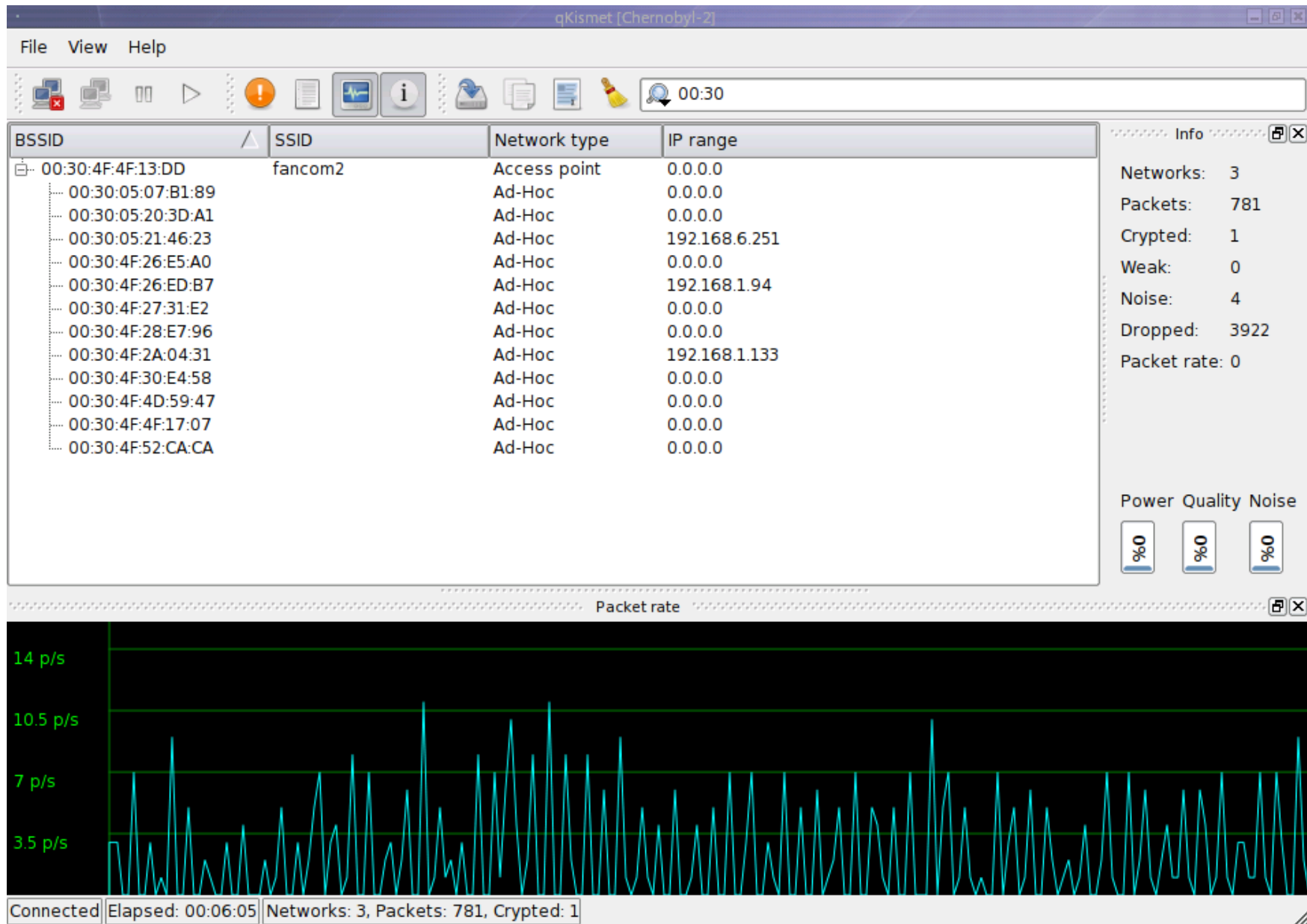
Pkts/s
2

Elapsd
00:00:22

Status
Connected to Kismet server version 2007.10.R1 build 20050815211952 on localh

Battery: AC 99%

Third-party frontend qkismet



Third-party frontend

The screenshot displays the qKismet [Chernobyl-2] application window. The main area shows a list of detected networks with columns for BSSID, SSID, Network type, and IP range. Below this, there are two panels for Alerts and Status messages, both showing a list of events with columns for Time, Header, BSSID, and Text. At the bottom, a status bar indicates the current state: Connected, Elapsed: 00:09:01, Networks: 6, Packets: 1792, Crypted: 4.

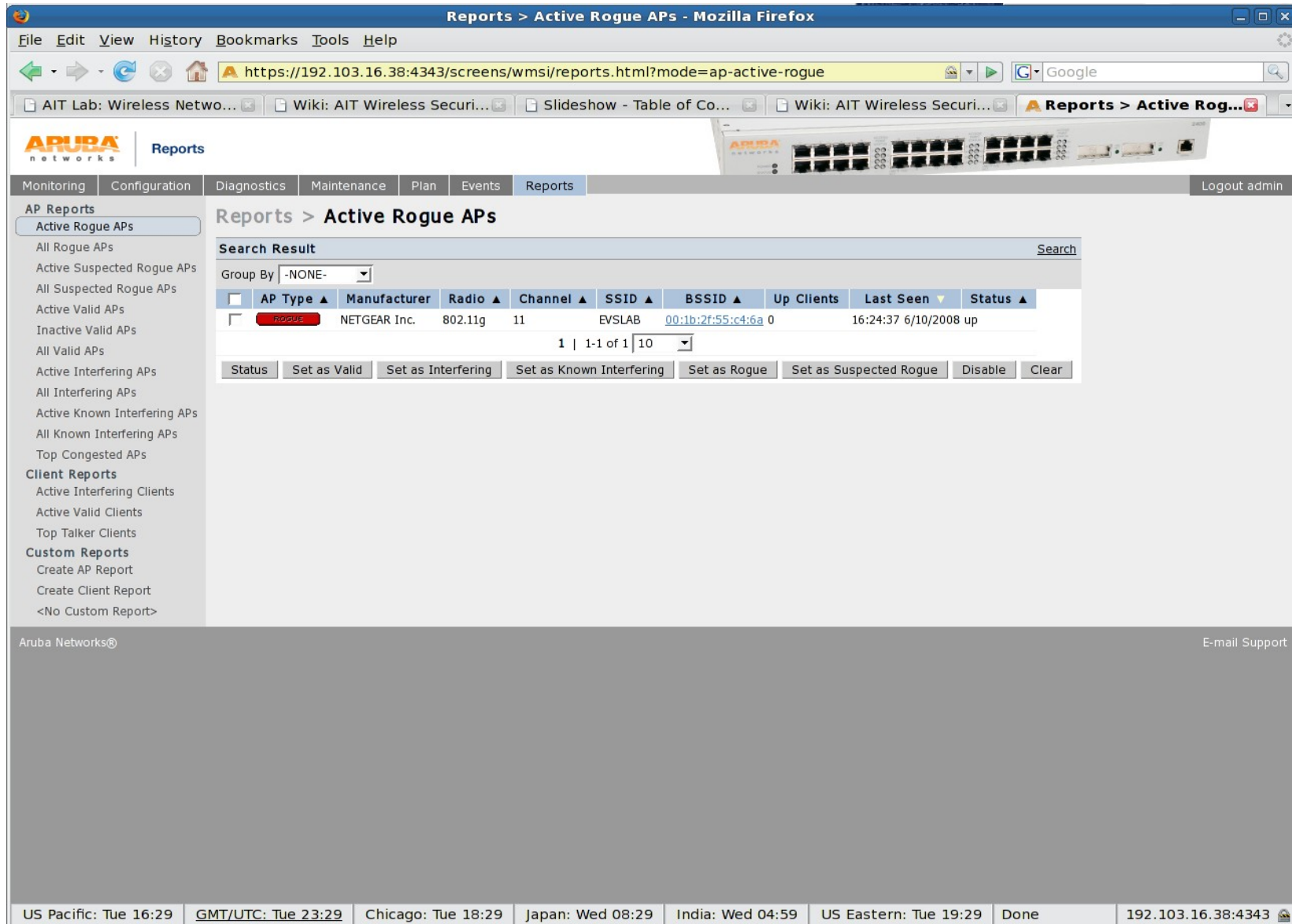
BSSID	SSID	Network type	IP range
00:02:2D:A5:40:87	PsiePole	Access point	10.10.6.254
00:02:6F:3C:6D:B7	linksys	Access point	193.109.91.156
00:16:41:C0:03:3E	neostrada_ef60	Access point	0.0.0.0
00:30:4F:34:1E:1C	fancom4	Access point	192.168.1.197
00:30:4F:4C:D9:72	fancom5	Access point	192.168.2.112
00:30:4F:4F:13:DD	fancom2	Access point	0.0.0.0
00:02:6F:3C:6D:C1		Ad-Hoc	192.168.6.243
00:02:6F:46:6E:25		Ad-Hoc	0.0.0.0
00:02:B3:0A:6B:00		Ad-Hoc	192.168.6.236
00:02:B3:2C:69:25		Ad-Hoc	0.0.0.0
00:02:B3:C1:6D:79		Ad-Hoc	0.0.0.0
00:04:0E:75:09:29		Ad-Hoc	192.168.2.112
00:08:A1:AF:DF:E0		Ad-Hoc	192.168.1.245
00:08:C7:9B:B4:97		Ad-Hoc	0.0.0.0
00:08:C7:9B:D7:23		Ad-Hoc	192.168.1.212
00:0A:50:11:2C:BF		Ad-Hoc	0.0.0.0
00:0E:2E:8F:03:CE		Ad-Hoc	0.0.0.0

Time	Header	BSSID	Text
pt. sie 24 17:18:57 2007	BSSTIMESTAMP	00:02:6F:3C:6D:B7	Out
pt. sie 24 17:18:35 2007	BSSTIMESTAMP	00:02:6F:3C:6D:B7	Out

Time	Header	BSSID	Text
pt. sie 24 17:19:50 2007	Found IP	192.168.6.245	for fancom2::00:02:B3:2...
pt. sie 24 17:19:46 2007	Found IP	192.168.2.112	for fancom2::00:04:0E:7...
pt. sie 24 17:19:46 2007	Found IP	192.168.2.31	for fancom2::00:11:95:4B...
pt. sie 24 17:19:30 2007	Found IP	192.168.6.251	for linksys::00:30:05:21...
pt. sie 24 17:19:17 2007	Found IP	192.168.6.246	for fancom2::00:D0:B7:...
pt. sie 24 17:19:15 2007	Found IP	83.23.81.33	for linksys::00:90:27:BB:4...
pt. sie 24 17:19:15 2007	Found IP	192.168.1.95	for fancom2::00:30:4F:26...
pt. sie 24 17:19:15 2007	Found IP	192.168.1.5	for fancom2::00:12:17:D3:...
pt. sie 24 17:19:06 2007	Found IP	192.168.6.238	for fancom2::00:02:B3:...

Connected | Elapsed: 00:09:01 | Networks: 6, Packets: 1792, Crypted: 4

Embedded In your APs (Aruba controller example)



The screenshot shows the Aruba controller web interface in Mozilla Firefox. The browser address bar displays the URL: `https://192.103.16.38:4343/screens/wmsi/reports.html?mode=ap-active-rogue`. The page title is "Reports > Active Rogue APs". The interface includes a navigation menu with "Monitoring", "Configuration", "Diagnostics", "Maintenance", "Plan", "Events", and "Reports". The "Reports" section is active, showing a sidebar with "AP Reports" and "Client Reports". The main content area displays a "Search Result" table for Active Rogue APs. The table has columns for AP Type, Manufacturer, Radio, Channel, SSID, BSSID, Up Clients, Last Seen, and Status. A single entry is shown: a ROGUE AP from NETGEAR Inc. on radio 802.11g, channel 11, with SSID EVSLAB and BSSID 00:1b:2f:55:c4:6a. The AP has 0 up clients and was last seen on 6/10/2008 at 16:24:37. Below the table are buttons for "Status", "Set as Valid", "Set as Interfering", "Set as Known Interfering", "Set as Rogue", "Set as Suspected Rogue", "Disable", and "Clear". The footer shows the time in various time zones: US Pacific: Tue 16:29, GMT/UTC: Tue 23:29, Chicago: Tue 18:29, Japan: Wed 08:29, India: Wed 04:59, US Eastern: Tue 19:29, Done, and the IP address 192.103.16.38:4343.

ARUBA networks Reports

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Logout admin

AP Reports

- Active Rogue APs
- All Rogue APs
- Active Suspected Rogue APs
- All Suspected Rogue APs
- Active Valid APs
- Inactive Valid APs
- All Valid APs
- Active Interfering APs
- All Interfering APs
- Active Known Interfering APs
- All Known Interfering APs
- Top Congested APs

Client Reports

- Active Interfering Clients
- Active Valid Clients
- Top Talker Clients

Custom Reports

- Create AP Report
- Create Client Report
- <No Custom Report>

Reports > Active Rogue APs

Search Result [Search](#)

Group By: -NONE-

<input type="checkbox"/>	AP Type ▲	Manufacturer	Radio ▲	Channel ▲	SSID ▲	BSSID ▲	Up Clients	Last Seen ▼	Status ▲
<input type="checkbox"/>	ROGUE	NETGEAR Inc.	802.11g	11	EVSLAB	00:1b:2f:55:c4:6a	0	16:24:37 6/10/2008	up

1 | 1-1 of 1 | 10

Status Set as Valid Set as Interfering Set as Known Interfering Set as Rogue Set as Suspected Rogue Disable Clear

Aruba Networks® E-mail Support

US Pacific: Tue 16:29 GMT/UTC: Tue 23:29 Chicago: Tue 18:29 Japan: Wed 08:29 India: Wed 04:59 US Eastern: Tue 19:29 Done 192.103.16.38:4343

Aruba controller continued

Reports > Active Interfering APs - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://localhost:4343/screens/wmsi/reports.html?mode=ap-active-interfering&start=0&page-size

ARUBA networks Reports

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Logout admin

AP Reports

- Active Rogue APs
- All Rogue APs
- Active Suspected Rogue APs
- All Suspected Rogue APs
- Active Valid APs
- Inactive Valid APs
- All Valid APs
- Active Interfering APs**
- All Interfering APs
- Active Known Interfering APs
- All Known Interfering APs
- Top Congested APs

Client Reports

- Active Interfering Clients
- Active Valid Clients
- Top Talker Clients

Custom Reports

- Create AP Report
- Create Client Report
- <No Custom Report>

Reports > Active Interfering APs

Search Result [Search](#)

Group By: -NONE-

<input type="checkbox"/>	AP Type ▲	Manufacturer	Radio ▲	Channel ▲	SSID ▲	BSSID ▲	Up Clients	Last Seen ▼	Status ▲
<input type="checkbox"/>	INTERFERING	Cisco-Linksys LLC	802.11g	6	sygate	00:14:bf:7b:dd:a8	0	21:22:28 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Aruba Networks	802.11g	1		00:0b:86:bb:0b:80	0	21:22:16 6/10/2008	up
<input type="checkbox"/>	INTERFERING	EPIGRAM, INC.	802.11g	1	danville	00:90:4c:7e:00:6e	0	21:22:10 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Tropos Networks, Inc.	802.11g	7	GoogleWiFiSecure	00:0d:97:04:99:d9	3	21:22:10 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Tropos Networks, Inc.	802.11g	7	GoogleWiFi	00:0d:97:07:41:00	0	21:22:08 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Cisco	802.11g	11	cisco4400	00:11:5c:97:61:d0	0	21:22:00 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Cisco-Linksys, LLC	802.11g	6	linksys	00:1d:7e:e8:50:4d	0	21:21:52 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Cisco Systems	802.11a	161	WIVO	00:14:1b:bb:34:81	0	21:21:37 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Go Networks	802.11g	1	ARC-NEL	00:14:06:10:0a:f0	2	21:21:28 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Buffalo Inc.	802.11g	1	buff3	00:16:01:7f:e2:3f	0	21:21:28 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Tropos Networks, Inc.	802.11g	11	GoogleWiFi	00:0d:97:04:88:b7	2	21:21:26 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Apple Computer Inc.	802.11g	1	speedline	00:14:51:77:93:55	0	21:21:24 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Cisco Systems	802.11g	1	StartYourVPN	00:17:0e:09:23:50	0	21:21:11 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Cisco Systems	802.11g	11	StartYourVPN	00:17:0e:09:25:10	0	21:21:09 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Cisco-Linksys, LLC	802.11g	6	GOONG2	00:1d:7e:c4:36:05	0	21:20:56 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Aruba Networks	802.11g	1	TelosWirelessxSec	00:0b:86:ba:f7:e0	0	21:20:56 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Tropos Networks, Inc.	802.11g	11	GoogleWiFi	00:0d:97:04:85:d7	0	21:20:44 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Tropos Networks, Inc.	802.11g	11	GoogleWiFi	00:0d:97:04:99:c4	0	21:20:44 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Unregistered	802.11g	11	MetroFi-Beta-Open	06:19:5e:b4:e6:9c	0	21:20:30 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Cisco-Linksys LLC	802.11g	1	GreatBigRobot	00:18:39:7e:3e:12	0	21:20:09 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Go Networks	802.11g	1	ARC-NEL	00:14:06:11:05:00	1	21:19:58 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Aruba Networks	802.11g	1		00:0b:86:bb:c5:f0	0	21:19:31 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Agere Systems	802.11b	6	NBI DSL	00:02:2d:0d:8d:bb	0	21:19:24 6/10/2008	up
<input type="checkbox"/>	INTERFERING	Cisco Systems	802.11g	0	danville	00:10:30:f5:b4:00	0	21:19:17 6/10/2008	up

Find: joel Next Previous Highlight all Match case Reached end of page, continued from top

US Pacific: Tue 21:23 GMT/UTC: Wed 04:23 Chicago: Tue 23:23 Japan: Wed 13:23 India: Wed 09:53 US Eastern: Wed 00:23 Done localhost:4343

Aruba client monitoring

Monitoring - Mozilla Firefox

File Edit View History Bookmarks Tools Help

https://localhost:4343/screens/switch/switch_mon.html?mode=clients&class=all&mac=

aircrack

FreeR... Kismet Chana... Power... NanoS... AirSno... Main [... htt...ml Power... (Untitl... Kismet A Mo... NetSt...

ARUBA networks | Monitoring

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Logout admin

Controller > Clients

Search Results [Search](#)

Clients All IPv4 IPv6

User Name	MAC address	Client IP	User Role	Authentication Method	ESSID	AP Name	Phy Type	Age	Roaming Status
	00:15:6d:a6:6b:14	192.103.16.13	pre-employee		ES Voice B	N/A	802.11g	54 days 10 hrs 34 mins	Associated

1 | 1-1 of 1 | 10

Status Profile Client Activity Packet Capture Locate Debug Disconnect Blacklist Ping

Aruba Networks® E-mail Support

Find: joel Next Previous Highlight all Match case Reached end of page, continued from top

US Pacific: Tue 21:31 GMT/UTC: Wed 04:31 Chicago: Tue 23:31 Japan: Wed 13:31 India: Wed 10:01 US Eastern: Wed 00:31 Done localhost:4343

Aruba packet capture

The screenshot shows a Mozilla Firefox browser window displaying the Aruba Packet Capture interface. The browser's address bar shows the URL: `https://localhost:4343/screens/wmsi/monitor.am.html?mode=am-pcaps&am-ip=192.168.100.226&`. The page title is "Enterprise Client 192.103.16.13 > Packet Capture (192.168.100.226)".

The interface includes a navigation menu on the left with categories like Network, Controller, WLAN, and Debug. The main content area shows a "Search Result" section with a table header:

ID	Type	Radio	Channel	Packets	Status	Target	Filter
None found.							

Below the search result, there are control buttons: Refresh, Stop, Delete, Pause, Resume, and New. A "New Raw Packet Capture" button and a "Launch WildPackets" link are also visible.

At the bottom of the interface, there are configuration options for the capture: `Interactive` (checked), `Target IP:` (empty), `Port:` `5555`, `Channel:` `1`, and `802.11a`.

The footer of the page includes "Aruba Networks®" and "E-mail Support". The browser's status bar at the bottom shows the time in various time zones: US Pacific: Tue 21:33, GMT/UTC: Wed 04:33, Chicago: Tue 23:33, Japan: Wed 13:33, India: Wed 10:03, US Eastern: Wed 00:33, and a search bar with "Find: joel".

Airsnort and Aircrack (Ng)

- Airsnort is a passive sniffer that will recover wep keys
- The updated version of Aircrack will also do wpa-psk keys

