WICRAWL | GTS 8

ARUBA™

The Mobile Edge Company

Luiz Eduardo Dos Santos
CISSP, CEH, CWNE, GCIH
Systems & Security Engineer, CALA

Agenda

- disclaimer
- what is wicrawl?
- why crawl?
- how does it work?
- screenshots
- resources
- acknoledgements

DISCLAIMER

- wicrawl is not related, by any means, to Aruba Networks
- wicrawl is a project from Midnight Research Labs http://midnightresearch.com
- Midnight Research Labs is a security research group, based out of the San Francisco Bay Area
- Luiz is a poor contributor to the project (and a horrible programmer)

ALL RIGHT THEN… BUT WHAT IS WICRAWL?

wicrawl is a free WiFi scanning/ auditing/ pen-testing tool developed by Midnight Research Labs based in two principles:

- passive scanning
- active crawling

from:

- a simple wardriving
- finding rogue APs
- finding "useful" WLANs
- pen-testing
- wicrawl's inspiration is key… facilitate finding "useful" wireless networks
- wicrawl's power is in the use of plug-ins

TOO MANY TOOLS OUT THERE… WHY-CRAWL?

- (again) ease of use
- kill the manual process of finding a useful wlan
- auto**magic**ally see “how deep the rabit hole goes”
- as MRL defines: “goal” oriented scanning
  (find what you’re actually looking for)
- run different cards simultaneously

WICRAWL BASICS

- PASSIVE WLAN SCANNING
- ASSOCIATION
- GET AN IP ADDRESS
- GET TO THE INTERNET
- MEASURES SPEED/ LATENCY
- RINSE AND REPEAT (OR GO FIND MORE STUFF)

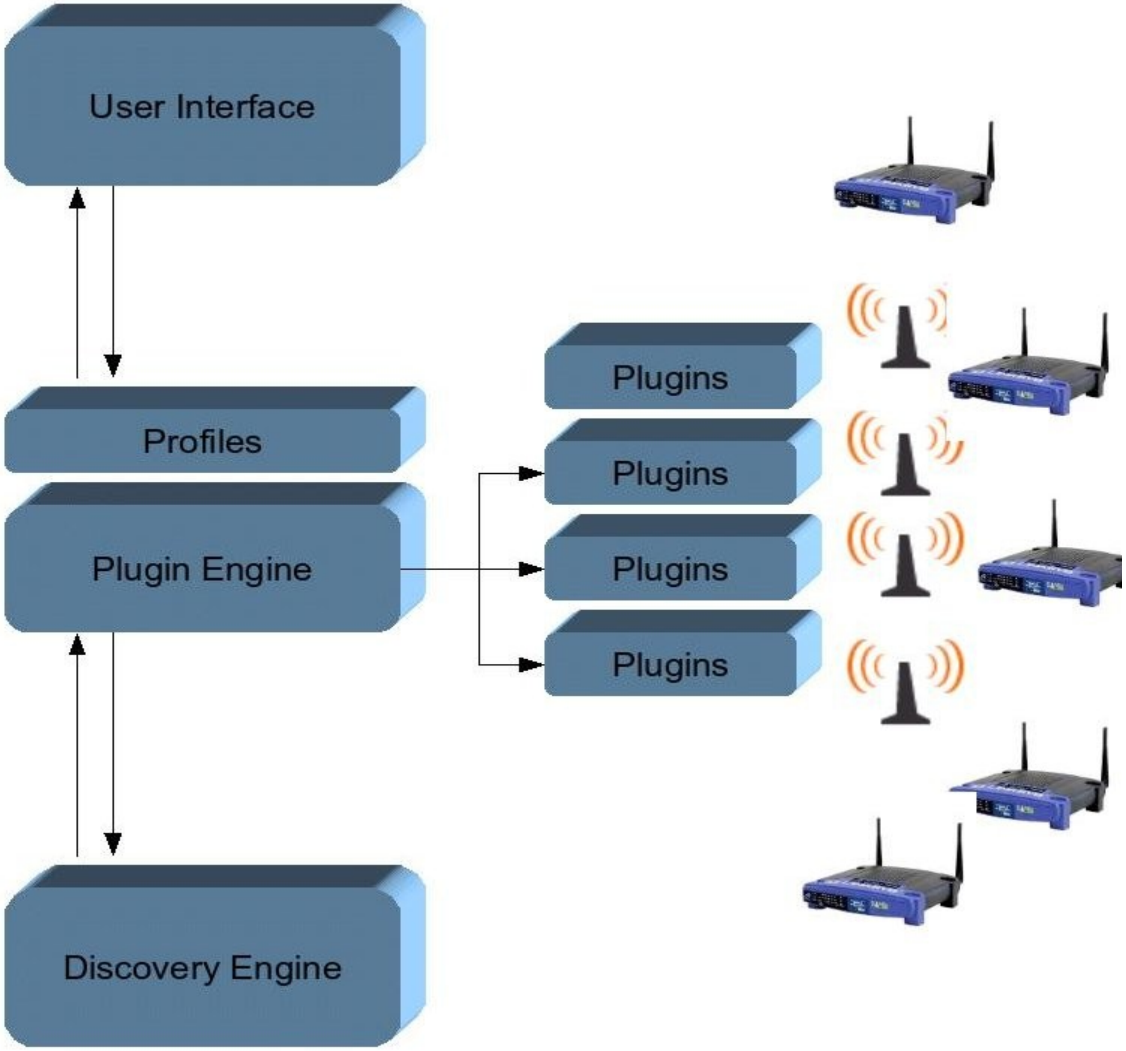
ADVANCED WICRAWL

- WEP/ WPA-PSK CRACKING
- NMAP/ NESSUS SCANNING
- WEP KEY BRUTE-FORCING
- MAC SPOOFING
- AND ANY SUGGESTIONS YOU MIGHT HAVE
- … IT’S ALL ABOUT THE PLUG-INS

logical pieces

- discovery Engine
- plug-in Engine
- plug-ins
- profiles
- ui(s)

GENERAL ARCHITECTURE



(SOME OF THE) WICRAWL COOLNESS

- DISTRIBUTED ON BACKTRACK'S LIVE CD DISTRO
- MULTIPLE CARD SUPPORT
- GUI/ PROFILE BASED
- BEING PORTED TO LINKSYS WRT54G

Profile Examples

- Pen-testing
  - ‘All’ card scheduling
  - Schedule all plugins
  - Short, medium and long run lengths
- Wardriving
  - ‘First’ card scheduling
  - Schedule only basic, short or even no plugins
  - Short run lengths only
- Holding Internet Access
  - ‘Signal’ card scheduling
  - Only basic plugins, plus hold internet plugin
  - Probably short run lengths only

Plug-ins

- There are two types of plug-ins:
- Scheduled
  - Handles the tools and are scheduled according to a profile
  - Synchronous
  - Examples: Association, mapping, anything associated with an access point
- Hooks
  - More timing sensitive
  - Synchronous or asynchronous
  - Examples: GPSd, antenna movement, TTS

Plug-in Template

- # The name of the plugin
- $name="Example PERL Plugin";

- # The binary file to run
- $bin="my_plugin.pl";

- # Version number of the plugin
- $version="0.1";

- # Card requires to be in monitor mode or not...
- #monitor=yes|no
- $monitor="no";

- # Length the plugin will take to run
- # examples dhcpd would be short, aircrack would be long
- #runlength=short|medium|long
- $runlength="short";

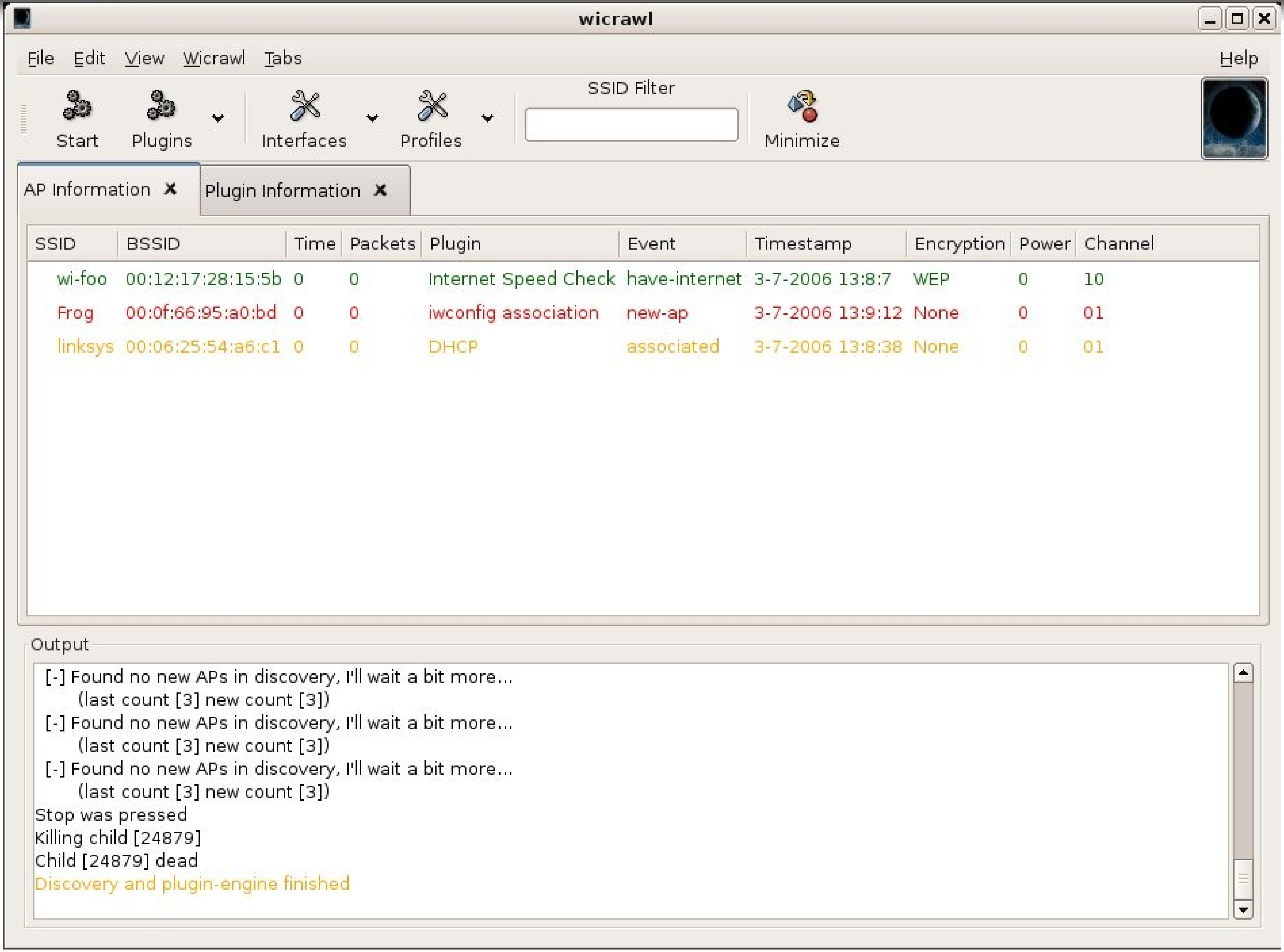
- # Whether this plugin is offline
- #offline=yes|no
- $offline="no";

- # plugin suggested "runlevel"
- # 0-99
- $runlevel=11;

- # event to register for
- $event="associated";

- # timeout value
- $timeout=30;

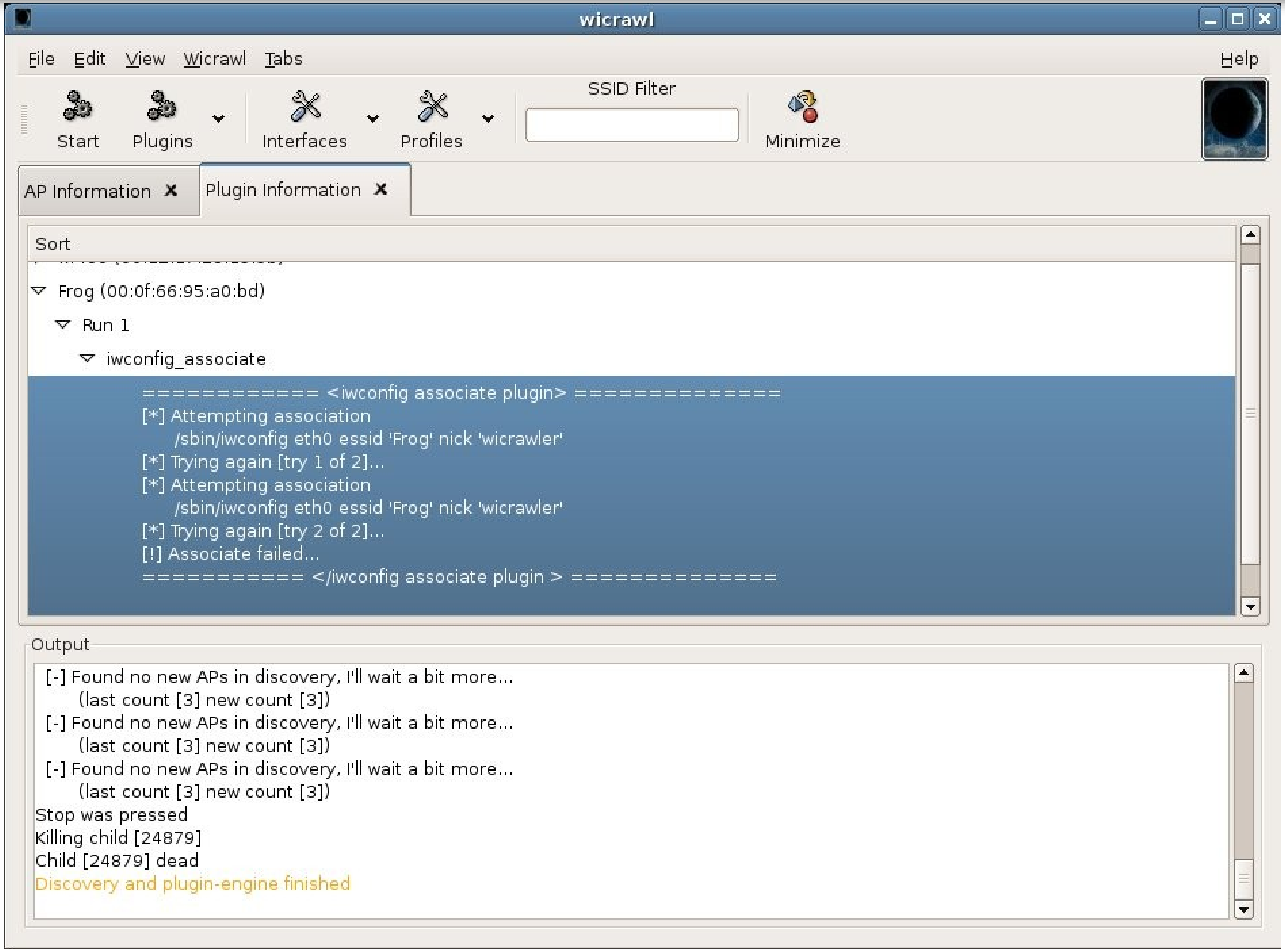
SCREENSHOTS



SSID	BSSID	Time	Packets	Plugin	Event	Timestamp	Encryption	Power	Channel
wi-foo	00:12:17:28:15:5b	0	0	Internet Speed Check	have-internet	3-7-2006 13:8:7	WEP	0	10
Frog	00:0f:66:95:a0:bd	0	0	iwconfig association	new-ap	3-7-2006 13:9:12	None	0	01
linksys	00:06:25:54:a6:c1	0	0	DHCP	associated	3-7-2006 13:8:38	None	0	01

```
 [-] Found no new APs in discovery, I'll wait a bit more...
     (last count [3] new count [3])
 [-] Found no new APs in discovery, I'll wait a bit more...
     (last count [3] new count [3])
 [-] Found no new APs in discovery, I'll wait a bit more...
     (last count [3] new count [3])
Stop was pressed
Killing child [24879]
Child [24879] dead
Discovery and plugin-engine finished
```

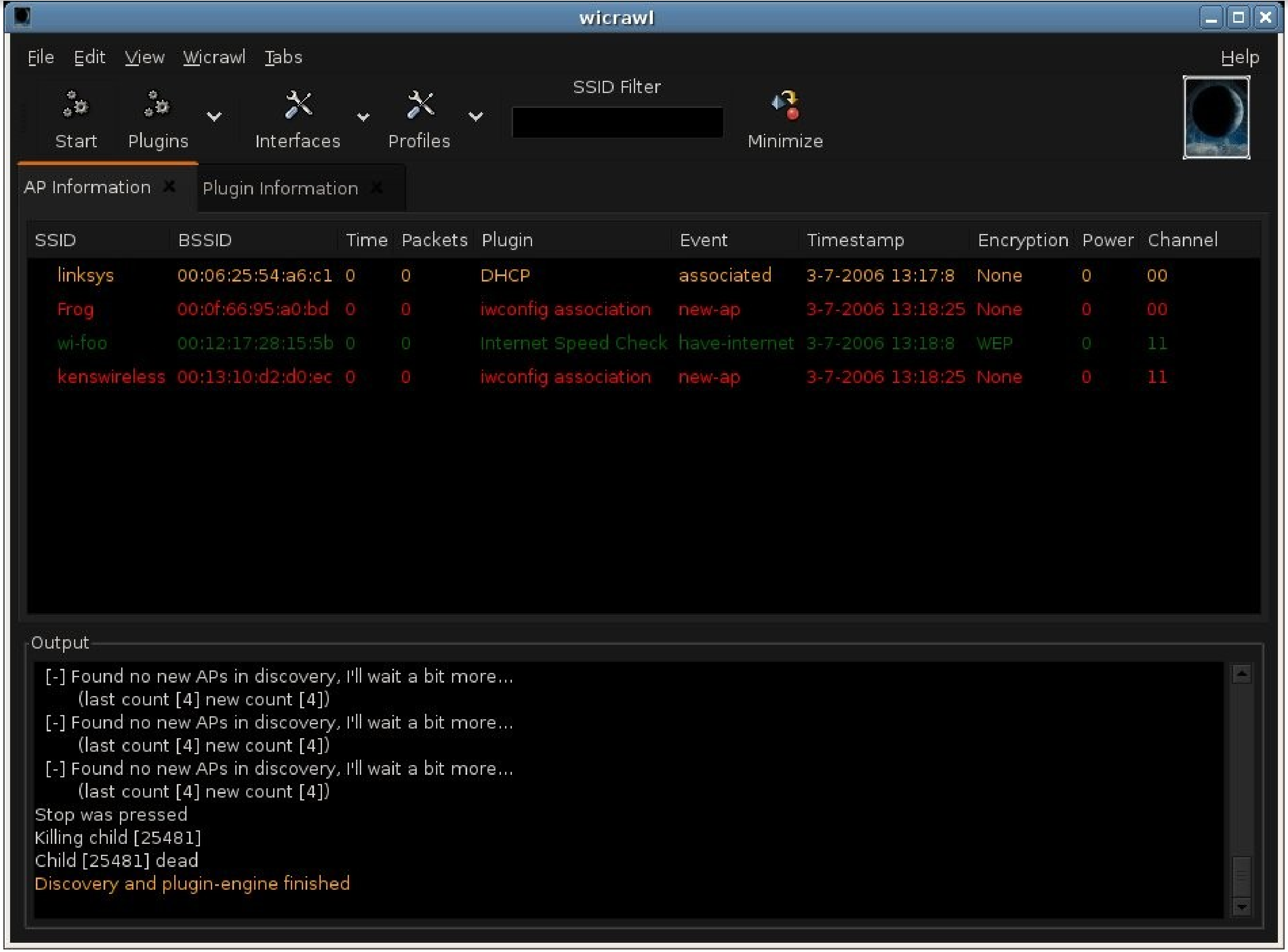
SCREENSHOTS



```
▽ Frog (00:0f:66:95:a0:bd)
  ▽ Run 1
    ▽ iwconfig_associate
        ============ <iwconfig associate plugin> ==============
        [*] Attempting association
              /sbin/iwconfig eth0 essid 'Frog' nick 'wicrawler'
        [*] Trying again [try 1 of 2]...
        [*] Attempting association
              /sbin/iwconfig eth0 essid 'Frog' nick 'wicrawler'
        [*] Trying again [try 2 of 2]...
        [!] Associate failed...
        =========== </iwconfig associate plugin > ==============
```

```
 [-] Found no new APs in discovery, I'll wait a bit more...
       (last count [3] new count [3])
 [-] Found no new APs in discovery, I'll wait a bit more...
       (last count [3] new count [3])
 [-] Found no new APs in discovery, I'll wait a bit more...
       (last count [3] new count [3])
Stop was pressed
Killing child [24879]
Child [24879] dead
Discovery and plugin-engine finished
```

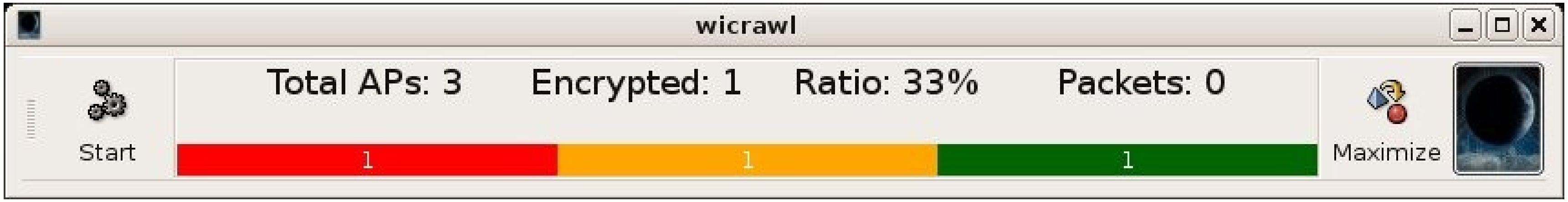
SCREENSHOTS



SSID	BSSID	Time	Packets	Plugin	Event	Timestamp	Encryption	Power	Channel
linksys	00:06:25:54:a6:c1	0	0	DHCP	associated	3-7-2006 13:17:8	None	0	00
Frog	00:0f:66:95:a0:bd	0	0	iwconfig association	new-ap	3-7-2006 13:18:25	None	0	00
wi-foo	00:12:17:28:15:5b	0	0	Internet Speed Check	have-internet	3-7-2006 13:18:8	WEP	0	11
kenswireless	00:13:10:d2:d0:ec	0	0	iwconfig association	new-ap	3-7-2006 13:18:25	None	0	11

```
 [-] Found no new APs in discovery, I'll wait a bit more...
     (last count [4] new count [4])
 [-] Found no new APs in discovery, I'll wait a bit more...
     (last count [4] new count [4])
 [-] Found no new APs in discovery, I'll wait a bit more...
     (last count [4] new count [4])
Stop was pressed
Killing child [25481]
Child [25481] dead
Discovery and plugin-engine finished
```

STATUS/ WARDRIVING BAR



wicrawl

Total APs: 3 Encrypted: 1 Ratio: 33% Packets: 0

Wrap-up

- More (and more) plug-ins to come
  - Better rogue-AP discovery
  - Captive portal brute-forcing/ defeating
  - …
- BSD/ Mac support
- Multiplexing APs

- Use it!
- Ideas are welcome too ;)

RESOURCES

- http://midnightresearch.com/projects/wicrawl
- http://midnightresearch.com
- http://www.remote-exploit.org/index.php/BackTrack

Acknoledgments / Major thanks to

- Aaron Peterson
  wicrawl's project manager/ developer

OBRIGADO

COMMENTS/ QUESTIONS/ FLAMES?

LUIZ (AT)

ARUBANETWORKS.COM