

Wireless LAN Security

- Setup & Optimizing Wireless Client in Linux
- Hacking and Cracking Wireless LAN
- Setup Host Based AP (hostap) in Linux & freeBSD
- Securing & Managing Wireless LAN :
Implementing 802.1x EAP-TLS EAP-PEAP-
MSCHAPv2 , FreeRADIUS + dialupadmin +
MySQL with Windows XP SP1 & Linux Client
(DEMO 😊)
- Make Deep Security with WPA2

Wifi Protected Access = 802.1x + (TKIP or
CCMP)

Hacking and Cracking Wireless LAN

by

Josua M Sinambela

Email : josh at gadjahmada edu
jogja-wireless@yahoogroups.com

Hardware Requirement

- Card Wireless (USB/PCI/PCMCIA)

Recommended :

PCMCIA with Prism2 Firmware or Orinoco Compatible

USB with Prism Firmware or Orinoco Compatible

- PC/Notebook/Laptop with Linux/BSD OS

Recommended :

Notebook/Laptop with PCMCIA slot

- Optional Antenna for more gain

Tools/Software

- Kismet : War-driving with passive mode scanning and sniffing 802.11a/b/g, site survey tools
- Aircrack-ng : Sniffing and Cracking WEP
- Ethereal : Sniffing and Analyze dump packet
- Aircrack-ng : Wireless Scanning and monitoring
- Aircrack-ng : MITM Attack and DoS tools
- FakeAP : Fake AP tools
- WEPCrack : Cracking WEP

Kismet

- Needs driver which are capable of reporting packets in rfmon like :

ACX100, ADMTek, Atheros, Cisco, Prism2, Orinoco, WSP100, Drone, pcapfile, wrt54g

Not work : Intel Centrino, Broadcom, Airport Extreme, Atmel, Realtek, HermesII

- Source Code Download from :
www.kismetwireless.com
- For RPM-man :
<http://rpm.pbone.net> or Ask Uncle Google ☺
- How to Install Kismet from source ?
README !!! It requires many Libraries & Utilities.

Compiling and Installing

- `tar -zxvf kismet-2004-04-R1.tar.gz`
- `cd kismet-2004-04-R1`
- `./configure`
- `make (linux) or gmake (BSD)`
- `make install (linux) or gmake install (BSD)`
- `cd /usr/local/etc/`
- `vi kismet.conf`

kismet.conf

- `suiduser=josh`

Source Driver.. (in linux)

- `#source=orinoco,eth1,orinocosource`
- `#source=wlanng_avs,wlan0,newprism2source`
- `#source=hostap,wlan0,hostap`

Source Driver.. (prism2 in BSD)

- `#source=radiotap_fbsd_b,wi0,prismbsd`
- `pidfile=/home/josh`

How to Run kismet daemon

- Run kismet as superuser/root
- Run from shell/terminal console
- Run only in suiduser home directory (see kismet.conf) or in the directory that can be written by suiduser like /tmp
- cd /home/josh
- kismet

Session Edit View Bookmarks Settings Help

```

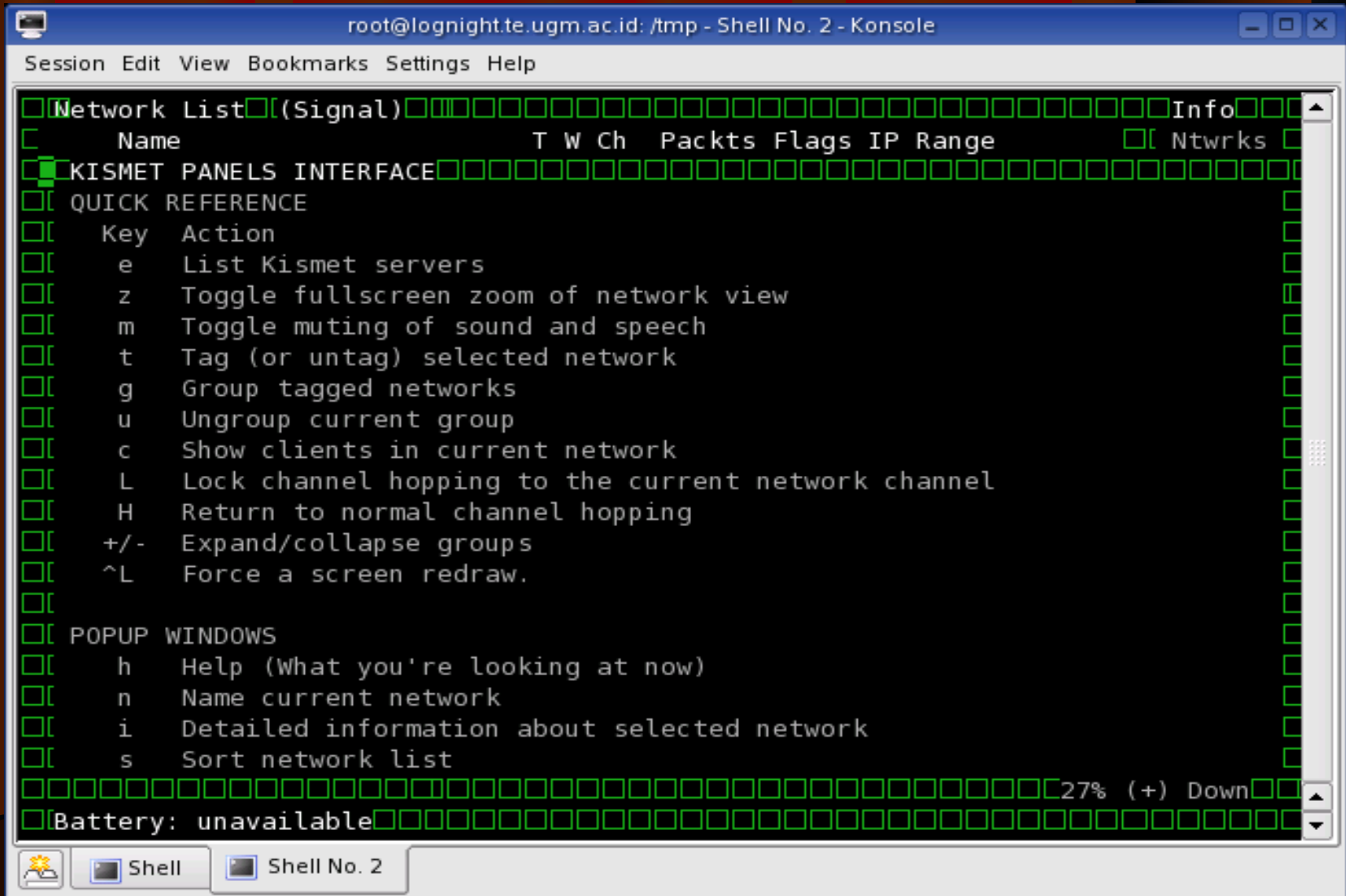
Network List (Signal) Info
Name          T W Ch  Packts  Flags  IP Range  Ntwrks
! complex     A Y 011   1937   T4     172.24.14.34  5
! 3Com        A N 006   5694   T3     172.24.14.0   Pckets
lantai_1_elektro  A N 002     1     0.0.0.0   14593
<no ssid>     A N ---    10   T4     172.16.160.108 Cryptd
. lantai_2    A N 007    72     0.0.0.0     0
Weak          0
Noise        159
Discrd       6868
Pkts/s       17
Elapsd
00:14:26
Status
Found new network "lantai_1_elektro" bssid 00:80:48:2B:6C:4B WEP N Ch 2 @ 11
Saving data files.
Requesting strings from the server
Sorting by signal strength
Battery: unavailable

```



Shell

Press "h" for help



The screenshot shows a terminal window titled "root@lognight.te.ugm.ac.id: /tmp - Shell No. 2 - Konsole". The application interface is displayed in green text on a black background. At the top, there is a menu bar with "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". The main content area shows a network list with columns for Name, T, W, Ch, Packts, Flags, IP Range, and Ntwrks. The first entry is "KISMET PANELS INTERFACE". Below the list is a "QUICK REFERENCE" section with a table of key actions. The help menu is currently open, showing options for listing servers, toggling fullscreen, muting, tagging, grouping, and other actions. At the bottom, there is a status bar showing "27% (+) Down" and "Battery: unavailable".

```
root@lognight.te.ugm.ac.id: /tmp - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

Network List((Signal)Info
  Name          T W Ch  Packts Flags IP Range  Ntwrks
KISMET PANELS INTERFACE
QUICK REFERENCE
  Key  Action
  e    List Kismet servers
  z    Toggle fullscreen zoom of network view
  m    Toggle muting of sound and speech
  t    Tag (or untag) selected network
  g    Group tagged networks
  u    Ungroup current group
  c    Show clients in current network
  L    Lock channel hopping to the current network channel
  H    Return to normal channel hopping
  +/-  Expand/collapse groups
  ^L   Force a screen redraw.

POPOPUP WINDOWS
  h    Help (What you're looking at now)
  n    Name current network
  i    Detailed information about selected network
  s    Sort network list

27% (+) Down
Battery: unavailable
```

Kismet In Action

root@WLANTEST.te.elektro: /tmp

Network List (Signal)										Info
Name	T	Manuf	W	Ch	Pkts	Flags	IP Range	Size	Sgn	Ntwrks
<no ssid>	A	Lucent	N	---	26646		0.0.0.0	2M	0	142
! <no ssid>	A	Lucent	N	002	325615	A3	10.1.16.142.0	110M	57	Pkts
+ <Data Networks>	G	Unknown	N	011	286224	G	0.0.0.0	363M	0	936542
! <no ssid>	A	Proxim	N	003	156121	A4	10.155.110.18	3M	56	Cryptd
! <NATC...>	A	Lucent	N	005	284394	A3	10.2.1.8.2.0	81M	51	462864
! PC.../	A	Lucent	Y	002	361937		0.0.0.0	22M	0	Weak
! Any	A	Lucent	N	003	144830	A2	10.2.0.0	21M	49	1198
<no ssid>	A	Lucent	N	---	866545		0.0.0.0	64M	0	Noise
. ELEKTRO	A	Lucent	Y	011	230092	T	10.2.250.254	130M	47	147825
+ ! Probe Networks	G	Unknown	N	---	281		0.0.0.0	0B	47	Discrd
<no ssid>	A	Lucent	N	---	22535		0.0.0.0	1M	0	320793
<no ssid>	A	Lucent	N	---	45221		0.0.0.0	4M	0	Pkts/s
<index...>	A	Senao	N	009	54688	T3	172.16.59.0	4M	0	119
! n...AP2	A	Proxim	N	001	116725	T3	192.168.1.0.0	7M	0	
! <PC...>	A	Lucent	Y	002	42778		0.0.0.0	7M	44	
! LT...ASV.../	A	Unknown	N	002	28628	A4	202.133.83.23	290k	0	
! <BTS1...>	A	Lucent	N	003	90221	T4	10.2.113.55.8	8M	42	
<no ssid>	A	Proxim	N	---	3695	T4	192.168.1.6	394k	0	
! lantai_3	A	Lucent	N	008	1051	T3	172.20.1.0	88k	0	
! <no ssid>	A	Lucent	N	003	31568	A	0.0.0.0	3M	42	
+ ! <no ssid>	H	Unknown	N	013	253		0.0.0.0	1k	0	
<no ssid>	A	Cisco	N	011	17202	T3	10.5.76.0	27k	0	orinoc
! <no ssid>	A	Lucent	N	006	736	A4	0.0.0.0	63k	0	Ch: 9
! tik...	H	Unknown	N	013	3		0.0.0.0	76B	0	
<no ssid>	A	Lucent	N	---	9092		0.0.0.0	612k	0	Elapstd

23% (+) Down 18:28:55

Status

```

Found new probed network "PC...1" bssid 00:02:20:10:10:78
Associated probe network "00:02:20:10:10:41:1B" with "00:02:20:10:10:18 D8:43" via data.
Associated probe network "00:00:48:2B:10:10:11" with "00:00:2D:10:10:46" via data.
Found new probed network "PS...1" bssid 00:00:10:2B:86:41
  
```

Kismet In Action

```

root@WLANTEST.te.elektro: /tmp
Network List (Signal) (-) Up Info
Name T Manuf W Ch Packts Flags IP Range Size Sgn Ntwrks
-----
[redacted] H Unknown N 001 20 0.0.0.0 228B 0 921
WLANTEST 38' A Unknown N 003 66250 A 0.0.0.0 5M 0 Pkts
<B> 2> A Lucent N 006 1358 A4 20.130.216.15 116k 0 180509
[redacted] H Unknown N 013 414 0.0.0.0 2k 0 Cryptd
In [redacted] H Unknown N 001 10 0.0.0.0 0B 0 880262
In [redacted] H Unknown N 001 34 0.0.0.0 836B 0 Weak
In [redacted] H Unknown N 001 8 0.0.0.0 76B 0 2302
In [redacted] H Unknown N 001 1 0.0.0.0 0B 0 Noise
In [redacted] H Unknown N 001 9 0.0.0.0 76B 0 277869
p [redacted] A Unknown N 013 7 0.0.0.0 0B 0 Discrd
[redacted] H Unknown N 006 7 0.0.0.0 76B 0 619432
In [redacted] H Unknown N 006 7 0.0.0.0 0B 0 Pkts/s
J [redacted] H Unknown N 001 35 0.0.0.0 304B 0 78
In [redacted] H Unknown N 001 10 0.0.0.0 152B 0
In [redacted] H Unknown N 001 8 0.0.0.0 152B 0
In [redacted] H Unknown N 006 1 0.0.0.0 0B 0
C.O. A D-Link N 008 433 T4 192.168.1.2 36k 0
ecc [redacted] A Linksys N 003 16 0.0.0.0 0B 0
<no ssid> H Unknown N --- 4 0.0.0.0 0B 0
[redacted] A Lucent Y 004 5629 0.0.0.0 390k 0
ph [redacted] A Orinoco N 008 38 0.0.0.0 374B 0
sat [redacted] A Lucent Y 004 141 0.0.0.0 5k 0 orinoc
[redacted] A Unknown N 006 6 A4 192.168.1.1 0B 0 Ch: 3
<no ssid> A Senao N 008 26 T4 200.16.139. 156B 0
in [redacted] A Senao N 005 46 T1 212.1.0.0 3k 0 Elapsed
97% (+) Down 41:00:02

Status
Found new probed network "FJM" bssid 00:02:2D:44:11:EB
Associated probe network "00:02:2D:44:11:EB" with "00:02:2D:44:11:EB" via data.
Associated probe network "00:8C:4D:2D:77:51" with "00:02:2D:44:11:EB" via data.
Found new network "T: done C" bssid 02:2D:CF:CC:10:65 WEP N Ch 1 @ 11.00 mbit
  
```


Kismet In Action

```
root@WLANTEST.te.elektro: /tmp
Network List (Signal)
Name          T Manuf      W Ch  Packts  Flags  IP Range          Size Sgn  Info
Ntwrks
+ Data Strings Dump
HTTP/1.1 302 Found
Pragma: no-cache
Cache-Control: no-cache
Expires: Wed, 11 Aug 2004 01:25:12 GMT
Set-Cookie: badsc=BOAU9kjUyB8VdN2bQo64ulsOHNTzAU2Wsaig3AkVqCGMKCiO_PAAwEEyiGiFO65-4-u4YuTrv
Location: http://ads.web.aol.com/content/BO/O/H7pTL2LufO_kw3xmlj8W1sns8a9RRNke8_SAqLzKBa609
P3P: CP="CUR TAI PSA UNI COM NAV STA NOI OUR"
Date: Wed, 11 Aug 2004 01:25:12 GMT
Content-Length: 0
HTTP/1.1 304 Not Modified
Date: Wed, 11 Aug 2004 01:33:10 GMT
Server: Apache/1.3.31 (Unix) PHP/4.3.6 mod_perl/1.27
Connection: Keep-Alive
Keep-Alive: timeout=15, max=99
ETag: "134002-216c-3f343a70"
:kiki!~.....kq-k@202.152.232.170 JOIN :#yogyakarta
HTTP/1.1 304 Not Modified
Date: Wed, 11 Aug 2004 01:33:11 GMT
Server: Apache/1.3.31 (Unix) PHP/4.3.6 mod_perl/1.27
Connection: Keep-Alive
Keep-Alive: timeout=15, max=98
ETag: "314047-34f-3f088dd0"
+OK X1 NT-POP3 Server mail.acsize.com (IMail 8.05 253751-4)
acsize.com
acsize.com
+OK send your password
+OK POP3 Server saying Good-Bye
^*HEARTBEAT
bravojmn
```

Kismet In Action

```
root@WLANTEST.te.elektro: /tmp
Network List (Signal)
Name          T Manuf      W Ch  Packts  Flags  IP Range      Size Sgn  Info
Ntwrks
-Data Strings Dump-                                     All
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
+ Referer: http://www.kedaulatan-rakyat.com/
+ Via: 1.1 proxy.sicmipa.ugm.ac.id:3128 (squid/2.5.STABLE5)
X-Forwarded-For: unknown
Cache-Control: max-age=259200
Connection: keep-alive
59nk^
%Q[do
70ZM&
=I9!I
WHOIS Ci_07
WHOIS Ci_07
HTTP/1.0 304 Not Modified
Date: Thu, 29 Jul 2004 00:08:18 GMT
Content-Type: image/jpeg
Last-Modified: Wed, 05 May 2004 07:06:52 GMT
Age: 1142080
X-Cache: HIT from cache.g...net.id
X-Cache-Lookup: HIT from cache...net :3128
Connection: keep-alive
:unFb0t!unffyy@h00045a7d93e7.ne.client2.attbi.com PART #teenparty :Adchecking...
,wVjuh
]1E\=
86&>F
q+9*rE5x
.*/KR:
hIN(id
+OK X1 NT-POP3 Server mail.decorize.com (IMail 8.05 254853-2)
Bali:1
```

AirSnort

- Works only with Cards :
Cisco, Prism2, Orinoco
- Source Code Downloaded from :
<http://airsnort.shmoo.com>
For RPM-man :
<http://rpm.pbone.net> or Ask uncle Google ☺
- How to Install AirSnort from source ?
README !!! It requires many Libraries & Utilities.

Compiling and Installing

- `tar -zxvf airsnort-0.2.5.tar.gz`
- `cd airsnort-0.2.5`
- `./configure`
- `make`
- `make install`

How to Run Airsnort

- Airsnort works in XWindows mode
- Open Terminal program
- su to Superuser/root (only root can change wireless adapter mode)
- Run with type airsnort &

AirSnort Interface

The screenshot shows the AirSnort application window. The title bar reads "AirSnort". The menu bar includes "File", "Edit", "Settings", and "Help".

Configuration options:

- scan
- channel
- Network device: Refresh
- Driver type:
- 40 bit crack breadth:
- 128 bit crack breadth:

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	PW: Hex	PW: ASC
	00:80:48:2B:7A:1A	compex		Tue Oct 5 08:41:48 2004	00:00:00	13	32	0	0		

At the bottom of the window, there are three buttons: "Start", "Stop", and "Clear".

AirSnort In Action

The screenshot shows the AirSnort application window. The title bar reads "AirSnort". The menu bar includes "File", "Edit", "Settings", and "Help".

Control elements include:

- Radio buttons for "scan" (selected) and "channel".
- A "channel" dropdown menu showing "9".
- A "Network device" dropdown menu showing "wlan0" and a "Refresh" button.
- A "Driver type" dropdown menu showing "Host AP/Orinoco".
- Spinners for "40 bit crack breadth:" (set to 2) and "128 bit crack breadth:" (set to 1).

The main display is a table with the following columns: C, BSSID, Name, WEP, Last Seen, Last IV, Chan, Packets, Encrypted, Interesting, PW: Hex, and PW. The table lists several detected wireless networks, with one row highlighted in blue.

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	PW: Hex	PW
	00:02:2D:90:25:FC	lantai_3		Tue Aug 3 10:14:48 2004	00:00:00	8	6336	0	0		
	00:00:00:00:00:00		Y	Tue Aug 3 09:10:08 2004	00:00:00		64285	64284	0		
	00:04:75:62:2A:E0	3Com		Tue Aug 3 09:02:16 2004	00:00:00	6	1801	0	0		
	00:90:CC:0E:A5:61	lantai_2		Tue Aug 3 12:02:58 2004	00:00:00	7	2748	0	0		
	00:02:2D:1C:59:28		Y	Tue Aug 3 12:02:58 2004	78:64:0B		1480	1480	0		
	00:02:2D:1C:59:28		Y	Mon Aug 2 21:36:00 2004	2E:A3:29	2	5295	5287	0		
	00:02:2D:1C:59:28		Y	Tue Aug 3 09:10:06 2004	AA:AA:03	2	52318	29977	1		
	00:02:2D:1C:59:28		Y	Tue Aug 3 09:09:02 2004	C5:14:5F	2	12685	10475	0		
	00:80:C8:AC:EF:AB		Y	Tue Aug 3 12:02:59 2004	FE:8C:CF		8057	8057	0		
	00:80:C8:AC:CD:1C		Y	Tue Aug 3 12:02:59 2004	77:28:06		9607	9607	30		
	00:60:B3:1D:35:68			Tue Aug 3 09:10:04 2004	00:00:00	3	25679	0	0		
	00:02:2D:90:23:39	ELEKTRO	Y	Tue Aug 3 09:10:07 2004	C2:48:58	3	14701	1851	0		
	00:80:48:2B:82:88		Y	Tue Aug 3 12:02:54 2004	AA:AA:03		2136	2066	0		
	00:02:2D:90:23:39		Y	Tue Aug 3 09:10:07 2004	AA:AA:03	5	50929	27241	0		
	00:60:80:1D:35:68		Y	Tue Aug 3 09:10:05 2004	3E:0A:09	1	8204	4362	0		
	00:80:48:2B:82:88		Y	Tue Aug 3 09:10:06 2004	AA:AA:03	2	5589	880	0		
	00:60:1D:1D:35:68	egbra		Tue Aug 3 09:10:08 2004	00:00:00	10	14170	0	0		
	00:02:2D:18:D8:46		Y	Tue Aug 3 09:00:22 2004	28:D1:33		138	129	0		
	00:02:2D:90:23:39			Tue Aug 3 09:10:02 2004	00:00:00	3	7103	0	0		
	00:02:6F:30:84:CC			Tue Aug 3 09:05:45 2004	00:00:00		45	0	0		

At the bottom of the window, there are three buttons: "Start", "Stop", and "Clear".

Ethereal

- Get the source
<http://www.ethereal.com>
- Or install from Installation CD
I use Mandrake 10.0 Official. It is available
- Run Ethereal in XWindows

Ethereal in Action

The screenshot displays the Ethereal network protocol analyzer interface. The title bar reads "Kismet-Aug-03-2004-19.dump - Ethereal". The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The main display area is divided into two sections: a packet list and a packet details pane.

No.	Time	Source	Destination	Protocol	Info
61173	682.434523	202.133.83.90	203.42.97.15	TCP	57575 > http [ACK] Seq=0 Ack=1017216 Win=17520 Len=0
61174	682.435664	Cisco_71:cb:41	Agere_01:05:b9	IEEE 802.11	Data
61175	682.438852		Compex_2b:b4:b4 (RA)	IEEE 802.11	Acknowledgement
61176	682.442504	202.133.83.90	203.42.97.15	TCP	57575 > http [ACK] Seq=0 Ack=1017216 Win=17520 Len=0
61177	682.443959		Compex_2b:b4:b4 (RA)	IEEE 802.11	Acknowledgement
61178	682.445479		192.168.42.2 (RA)	IEEE 802.11	Acknowledgement
61179	682.446582		192.168.42.2 (RA)	IEEE 802.11	Acknowledgement
61180	682.454972	202.133.81.17	Compex_22:28:3b	IEEE 802.11	Fragmented IEEE 802.11 frame
61181	682.457622	202.133.81.17	Compex_22:28:3b	IEEE 802.11	Data
61182	682.460141	202.133.81.17	Compex_22:28:3b	IEEE 802.11	Data
61183	682.462822	202.133.81.17	Compex_22:28:3b	IEEE 802.11	Data

Frame 61176 (72 bytes on wire, 72 bytes captured)

- IEEE 802.11
 - Type/Subtype: Data (32)
 - Frame Control: 0x0908 (Normal)
 - Duration: 258
 - BSS Id: 00:80:48:2b:66:7c (Compex_2b:66:7c)
 - Source address: 00:02:2d:02:10:f7 (192.168.44.7)
 - Destination address: 00:02:a5:0f:5b:75 (CompaqCo_0f:5b:75)
 - Fragment number: 0
 - Sequence number: 3296
- Logical-Link Control
- Internet Protocol, Src Addr: 202.133.83.90 (202.133.83.90), Dst Addr: 203.42.97.15 (203.42.97.15)
- Transmission Control Protocol, Src Port: 57575 (57575), Dst Port: http (80), Seq: 0, Ack: 1017216, Len: 0

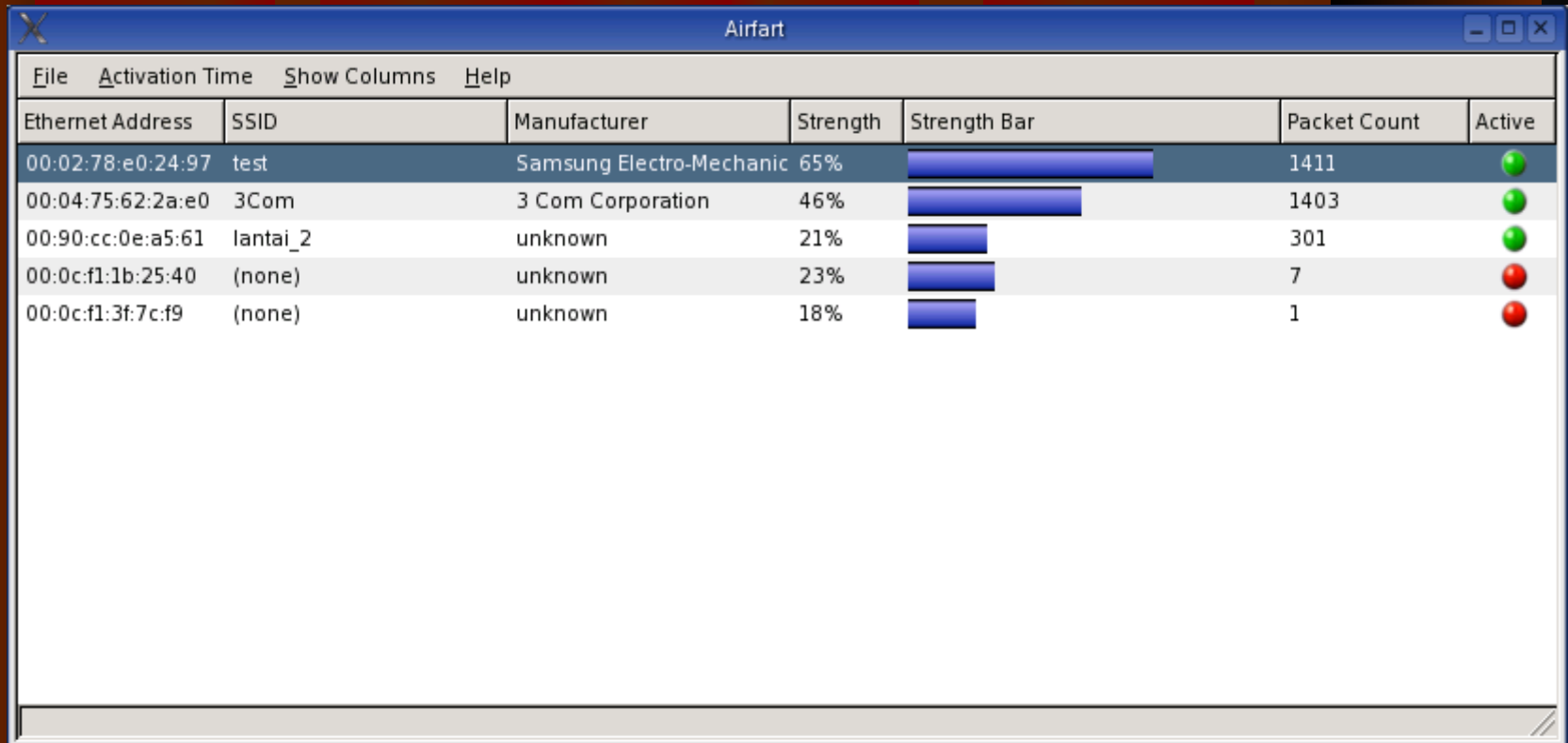
```
0000  08 09 02 01 00 80 48 2b 66 7c 00 02 2d 02 10 f7  ....H+ fl..-...
0010  00 02 a5 0f 5b 75 00 ce aa aa 03 00 00 08 00  ....lu.. ..
0020  45 00 00 28 89 c3 40 00 7f 06 27 f3 ca 85 53 5a  E..(..@. ...SZ
0030  cb 2a 61 0f e0 e7 00 50 de 69 38 dd a7 63 1c 75  .*a....P .i8..c.u
0040  50 10 44 70 64 f3 00 00                          P,Dpd...
```

Filter: + Expression... Clear Apply File: Kismet-Aug P: 170807 D: 17080











AirFart

- Used for Scanning and Wireless Monitoring
- Only supports prism2 cards with wlan-ng driver.
- Get source from :
<http://sourceforge.net/projects/airfart>

AirFart Interfaces



The screenshot shows a window titled "Airfart" with a menu bar containing "File", "Activation Time", "Show Columns", and "Help". Below the menu bar is a table with the following columns: "Ethernet Address", "SSID", "Manufacturer", "Strength", "Strength Bar", "Packet Count", and "Active". The table contains five rows of data, each with a corresponding strength bar and active status indicator.

Ethernet Address	SSID	Manufacturer	Strength	Strength Bar	Packet Count	Active
00:02:78:e0:24:97	test	Samsung Electro-Mechanic	65%		1411	
00:04:75:62:2a:e0	3Com	3 Com Corporation	46%		1403	
00:90:cc:0e:a5:61	lantai_2	unknown	21%		301	
00:0c:f1:1b:25:40	(none)	unknown	23%		7	
00:0c:f1:3f:7c:f9	(none)	unknown	18%		1	

FakeAP

- FakeAP generates 802.11b beacon with random ESSID, BSSID (MAC) and channel.
- Works only with PRISM2/2.5/3 Card with hostap driver (Master Mode)
- Needs hostap-utils for activate WEP
- Get from <http://www.blackalchemy.to/project/fakeap>,

Install FakeAP

- [root@lognight local]# tar -zxvf fakeap031.tar.gz
fakeap-0.3.1/
fakeap-0.3.1/fakeap.pl
fakeap-0.3.1/CREDITS
fakeap-0.3.1/COPYING
fakeap-0.3.1/README
fakeap-0.3.1/INSTALL
fakeap-0.3.1/lists/
fakeap-0.3.1/lists/stefan-maclist.txt
fakeap-0.3.1/lists/stefan-wordlist.txt
fakeap-0.3.1/lists/koaps-fo-wo
- [root@lognight local]# cd fakeap-0.3.1/
- [root@lognight fakeap-0.3.1]# vi fakeap.pl

Edit fake.pl

- my \$MAX_CHANNEL = 14;
- my \$IWCONFIG = "/sbin/iwconfig";
- my \$IFCONFIG = "/sbin/ifconfig";
- my \$CRYPTCONF = "/usr/src/hostap-utils-0.2.4/hostap_crypt_conf";

RUN fake.pl

```
[root@lognigh fakeap-0.3.1]# perl fakeap.pl
```

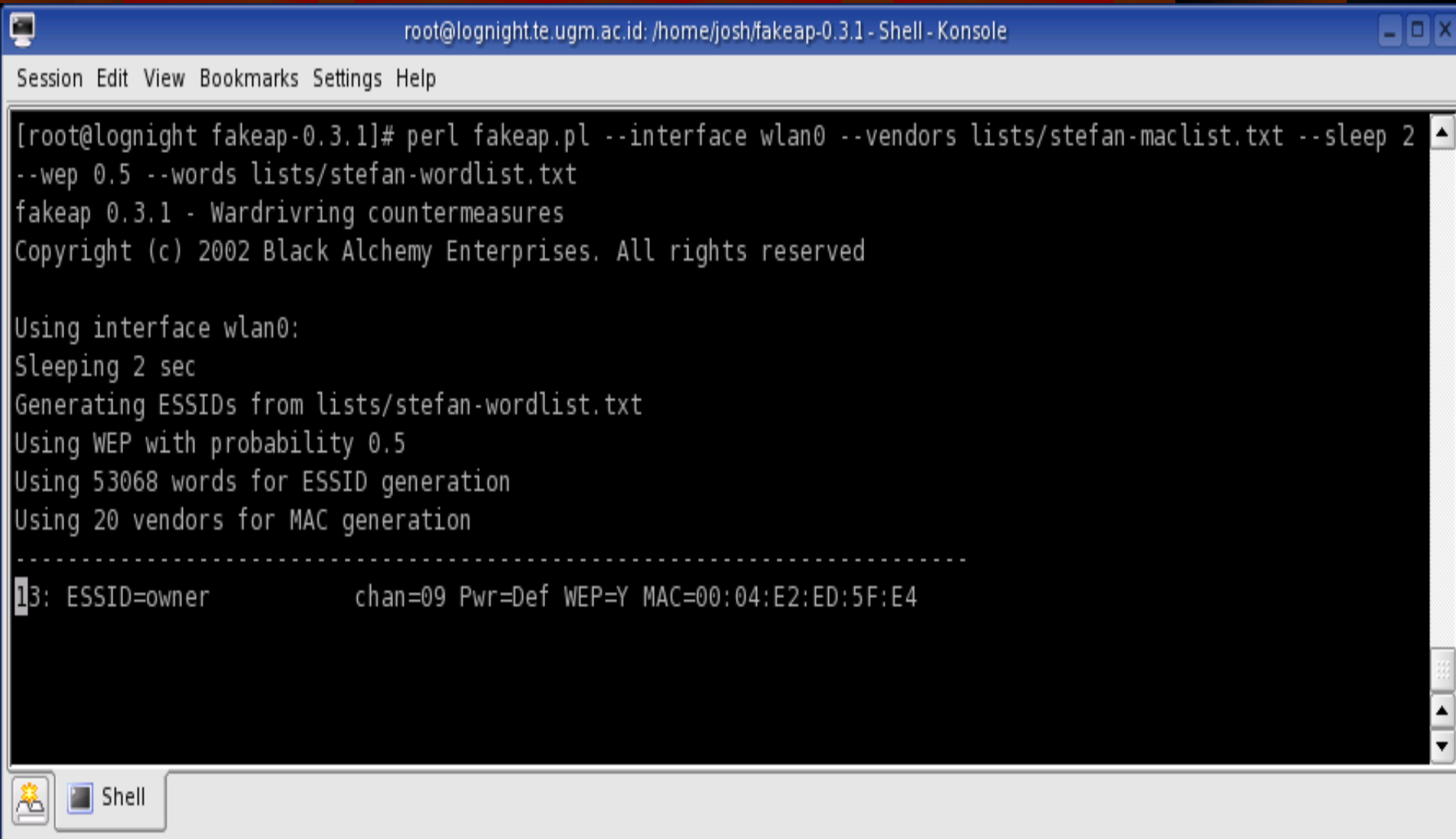
```
fakeap 0.3.1 - Wardriving countermeasures
```

```
Copyright (c) 2002 Black Alchemy Enterprises. All rights reserved
```

```
Usage: fakeap.pl --interface wlanX [--channel X] [--mac XX:XX...]
      [--essid NAME] [--words FILENAME] [--sleep N] [--vendors FILENAME]
      [--wep N] [--key KEY] [--power N]
```

```
--channel X    Use static channel X
--essid NAME   Use static ESSID NAME
--mac XX:XX... Use static MAC address XX:...
--words FILE   Use FILE to create ESSIDs
--sleep N      Sleep N Ssec between changes, default 0.25
--vendor FILE  Use FILE to define vendor MAC prefixes
--wep N        Use WEP with probability N where 0 < N <= 1
--key KEY      Use KEY as the WEP key. Passed raw to iwconfig
--power N      Vary Tx power between 1 and N. In milliwatts
```

FakeAP in Action



The image shows a terminal window titled "root@lognight.te.ugm.ac.id: /home/josh/fakeap-0.3.1 - Shell - Konsole". The terminal displays the execution of the "fakeap" command with various options. The output shows the program's version, copyright information, and configuration details. A sample output line is shown at the bottom, indicating the generated ESSID, channel, power, WEP status, and MAC address.

```
root@lognight.te.ugm.ac.id: /home/josh/fakeap-0.3.1 - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@lognight fakeap-0.3.1]# perl fakeap.pl --interface wlan0 --vendors lists/stefan-maclist.txt --sleep 2
--wep 0.5 --words lists/stefan-wordlist.txt
fakeap 0.3.1 - Wardriving countermeasures
Copyright (c) 2002 Black Alchemy Enterprises. All rights reserved

Using interface wlan0:
Sleeping 2 sec
Generating ESSIDs from lists/stefan-wordlist.txt
Using WEP with probability 0.5
Using 53068 words for ESSID generation
Using 20 vendors for MAC generation
-----
13: ESSID=owner          chan=09 Pwr=Def WEP=Y MAC=00:04:E2:ED:5F:E4
```

Impact of FakeAP for airfart

Ethernet Address	SSID	Manufacturer	Strength	Strength Bar	Packet Count	Active
00:02:78:e0:24:97	test	Samsung Electro-Mechanic	69%		2140	
00:04:75:62:2a:e0	3Com	3 Com Corporation	43%		5141	
00:90:cc:0e:a5:61	lantai_2	unknown	22%		923	
00:0c:f1:1b:25:40	(none)	unknown	22%		14	
00:0c:f1:3f:7c:f9	(none)	unknown	18%		1	
00:80:0f:ba:db:6e	urukhai	unknown	54%		40	
00:04:e2:fa:c6:2c	suxin	unknown	53%		86	
00:80:c6:f7:bd:7b	coutinho	unknown	78%		144	
00:08:c7:c2:2c:f6	slide	unknown	78%		78	
00:a0:f8:c3:68:92	quintina	unknown	79%		129	
00:40:ae:b4:91:fb	sri-tsc	unknown	77%		98	
00:80:c8:ff:08:ba	adrión	unknown	59%		74	
00:02:2d:8b:39:7f	basis	Dell Computer Corp.	60%		61	
00:04:76:ad:c3:7e	dftvm1	3 Com Corporation	65%		34	
00:90:96:c9:2c:7b	dftvm1	ASKEY COMPUTER CORP.	61%		227	
00:02:2d:ba:aa:24	ehrllichman	Dell Computer Corp.	85%		1	
00:08:c7:05:66:1c	hazlett	unknown	57%		1	
00:40:33:08:77:23	liking	ADDTRON TECHNOLOGY C	59%		1	
00:04:76:4b:95:2f	sharc	3 Com Corporation	54%		1	
00:80:c8:f7:fd:10	enrichetta	unknown	85%		1	
00:40:33:2d:a6:20	VictorJara	ADDTRON TECHNOLOGY C	57%		1	
00:04:76:19:05:99	nrl-radar	3 Com Corporation	81%		1	
00:02:2d:35:57:e3	gina	Dell Computer Corp.	80%		2	
00:02:a5:bb:9c:a5	nealon	unknown	60%		2	
00:02:b3:09:b7:01	bethesda	unknown	71%		1	
00:01:fa:8c:3f:f3	harcourt	unknown	85%		1	
00:02:2d:8d:4f:b7	celrey	Dell Computer Corp.	66%		2	
00:40:33:19:28:fa	heshbon	ADDTRON TECHNOLOGY C	56%		1	
00:40:33:5d:3e:2b	demo2090	ADDTRON TECHNOLOGY C	55%		1	
00:02:a5:bb:bd:b7	mcn87	unknown	53%		1	
00:80:c8:6e:32:69	seething	unknown	77%		1	
00:05:86:4c:91:8f	leonore	Lucent Technologies	74%		2	
00:01:fa:25:45:18	rayshell	unknown	60%		1	
00:40:96:15:d1:1d	isles	Ciron (Cisco)	54%		1	

Impact of FakeAP for Kismet

The screenshot shows a terminal window titled "root@lognight.te.ugm.ac.id: /tmp - Shell - Konsole". The main content is a network list with columns for Name, T W Ch, Packts, Flags, IP Range, Size, and Info. The 'verena' network is highlighted in green. Below the list, there is a status section with several lines of text. At the bottom, a battery status is shown as "Battery: unavailable".

Name	T W Ch	Packts	Flags	IP Range	Size	Info
verena	A Y 008	1		0.0.0.0	0B	Ntwrks 68 Pckets 519 Cryptd 0 Weak 0 Noise 0 Discrd 0 Pkts/s 22
Sootiyo	A N 007	1		0.0.0.0	0B	
northwestern	A Y 006	1		0.0.0.0	0B	
pc2591	A N 005	1		0.0.0.0	0B	
vmssucks	A N 005	2		0.0.0.0	0B	
! dominick	A Y 002	1		0.0.0.0	0B	
! sehyo	A Y 001	1		0.0.0.0	0B	
ripe	A Y 006	1		0.0.0.0	0B	
baldor	A Y 010	2		0.0.0.0	0B	
contentions	A N 003	1		0.0.0.0	0B	
norah	A Y 001	1		0.0.0.0	0B	
dragonlady	A N 011	2		0.0.0.0	0B	
hirah	A Y 008	1		0.0.0.0	0B	
dolly	A N 005	1		0.0.0.0	0B	
ashlen	A N 006	1		0.0.0.0	0B	
pister	A Y 005	1		0.0.0.0	0B	
Haidea	A Y 010	2		0.0.0.0	0B	
demo1791	A Y 009	1		0.0.0.0	0B	
goats	A N 004	2		0.0.0.0	0B	
fiftysix	A Y 004	1		0.0.0.0	0B	
! haft	A Y 011	1		0.0.0.0	0B	
itsajoke	A N 007	1		0.0.0.0	0B	
! dongmoon	A Y 009	1		0.0.0.0	0B	
assessment	A Y 007	1		0.0.0.0	0B	
lintel	A Y 006	1		0.0.0.0	0B	
myrtlbch	A Y 006	2		0.0.0.0	0B	
satyrs	A Y 008	1		0.0.0.0	0B	
villa	A Y 011	1		0.0.0.0	0B	
brl-sec	A N 004	2		0.0.0.0	0B	

41% (+) Down 00:00:38

Status

- Found new probed network "<no ssid>" bssid 00:0C:F1:1B:25:40
- Associated probe network "00:0C:F1:1B:25:40" with "00:04:75:62:2A:E0" via probe response.
- Found new network "keeping" bssid 00:04:5A:7E:71:73 WEP N Ch 7 @ 11.00 mbit
- Found new network "strom" bssid 00:80:C8:7C:D7:C3 WEP N Ch 7 @ 11.00 mbit

Battery: unavailable

Impact of FakeAP for Netstumbler

Network Stumbler - [20041007022202]

File Edit View Device Window Help

Channels

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...
00022DAEB73E	merrili		6	11 Mbps	Proxim (A...	AP	WEP
0080C8BB980F	firstripe		8	11 Mbps	D-Link	AP	WEP
0001FAF6084A	Libussa		5	11 Mbps		AP	WEP
00042510DEA4	brl-zip3		10	11 Mbps	Atmel	AP	
0004764D75E1	tech		1	11 Mbps	3Com	AP	
00045A92EE0D	emulating		8	11 Mbps	Linksys	AP	WEP
000476424F1D	xiaoping		11	11 Mbps	3Com	AP	
0004E2F9FFB7	similitude		1	11 Mbps	SMC	AP	
080046AB8BC0	mothers		11	11 Mbps	Sony	AP	
009096E34870	megiddon		5	11 Mbps	Askey Co...	AP	WEP
00022D437D9A	klement		11	11 Mbps	Proxim (A...	AP	WEP
0008C72A5378	tow		8	11 Mbps		AP	WEP
009096FB32A0	jemie		7	11 Mbps	Askey Co...	AP	
0002A5F0FBC0	exhortation		9	11 Mbps	Compaq	AP	WEP
0002A57F3CD9	ranjit		9	11 Mbps	Compaq	AP	WEP
004033114475	bren		8	11 Mbps	Addtron	AP	
0080C6120A8C	capp		11	11 Mbps	NDC (Inst...	AP	
0004E241ED5D	keefar		7	11 Mbps	SMC	AP	
0090CC0EA561	lantai_2		7	11 Mbps	Planet Co...	AP	
00A0F8CD8047	myrvyn		6	11 Mbps	Symbol	AP	
080046CACC44	csa1		10	11 Mbps	Sony	AP	
000425D82AE2	emptys		1	11 Mbps	Atmel	AP	WEP
0002B31B97ED	erymanthos		6	11 Mbps	Intel	AP	
0040AE47B723	navshipyd-pearl-harbor		4	11 Mbps		AP	WEP
000476D302DD	sdemo2		9	11 Mbps	3Com	AP	WEP
0040337273BF	bac		3	11 Mbps	Addtron	AP	WEP

SSIDs

- 3Com
- ackertabbody
- anticipate
- bac
- bren
- brl-zip3
- capp
- csa1
- emptys
- emulating
- erymanthos
- exhortation
- firstripe
- jemie
- keefar
- klement

Ready 2 APs active GPS: Disabled 31 / 31

AirJack

- Used for jamming (DoS) and Man In The Middle Attack (MITM)
- Works in prism2 and Lucent cards
- Only works for Linux kernel 2.4 ☹️

Hacking and Cracking Wireless LAN

by

Josua M Sinambela

Email : josh@ugm.ac.id

Network Administrator JTE

UGM