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
- Airsnort : Sniffing and Cracking WEP
- Ethereal : Sniffing and Analyze dump packet
- Airfart : Wireless Scanning and monitoring
- Airjack : 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

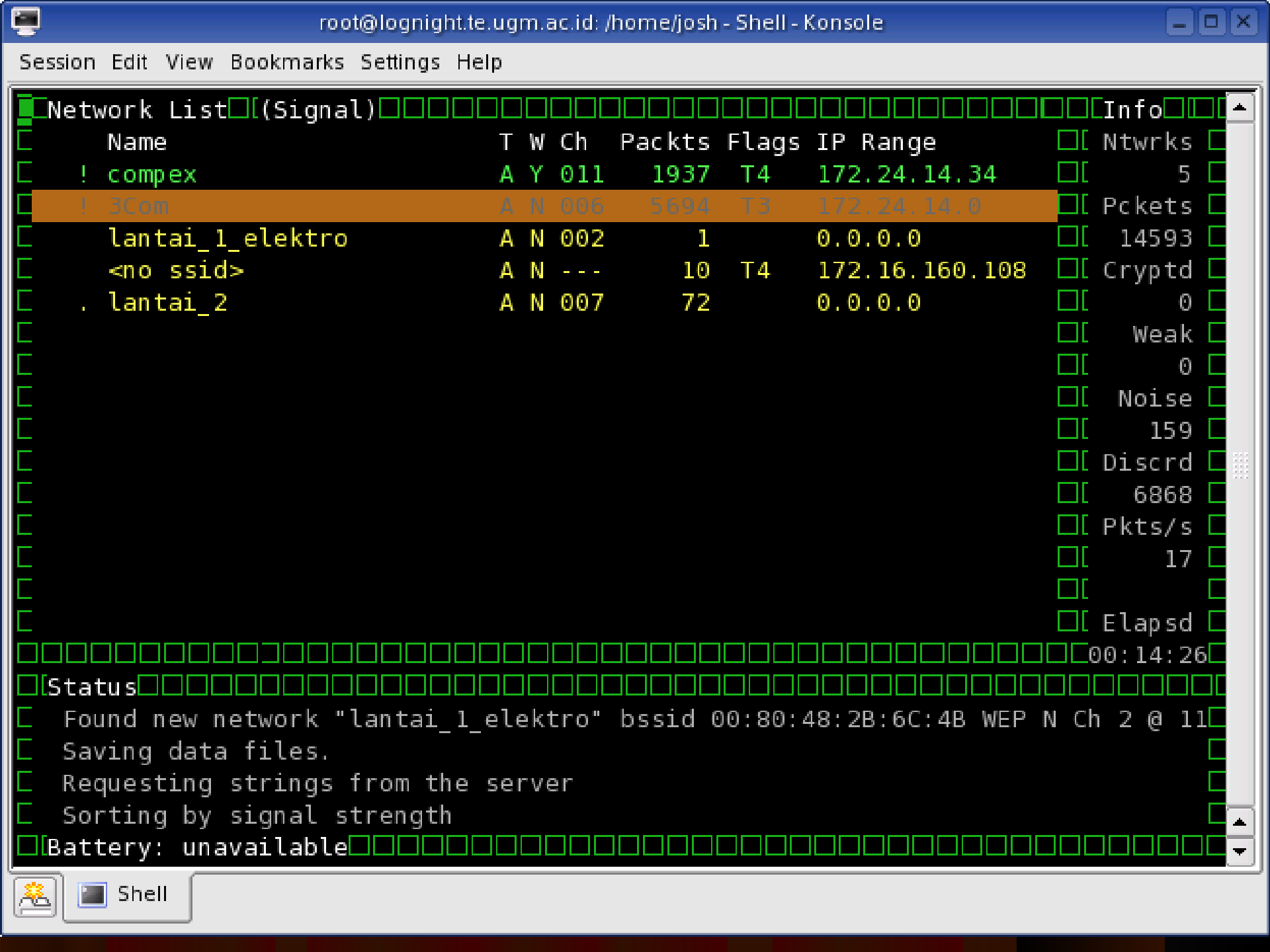
Source Driver.. (prism2 in BSD)

- #source=radiotap_fbsd_b,wi0,prismbsd

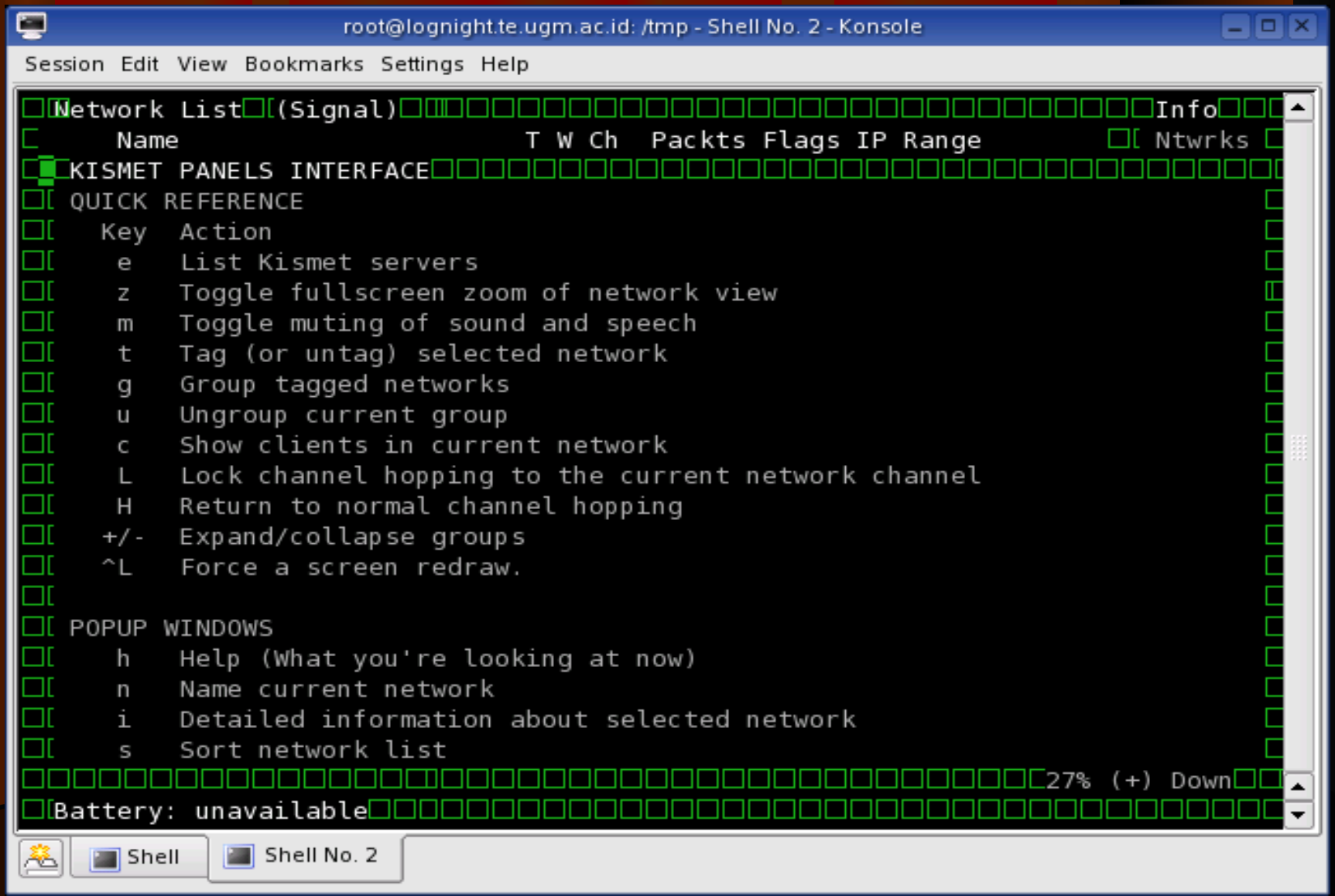
- piddir=/home/josh

How to Run kismet daemon

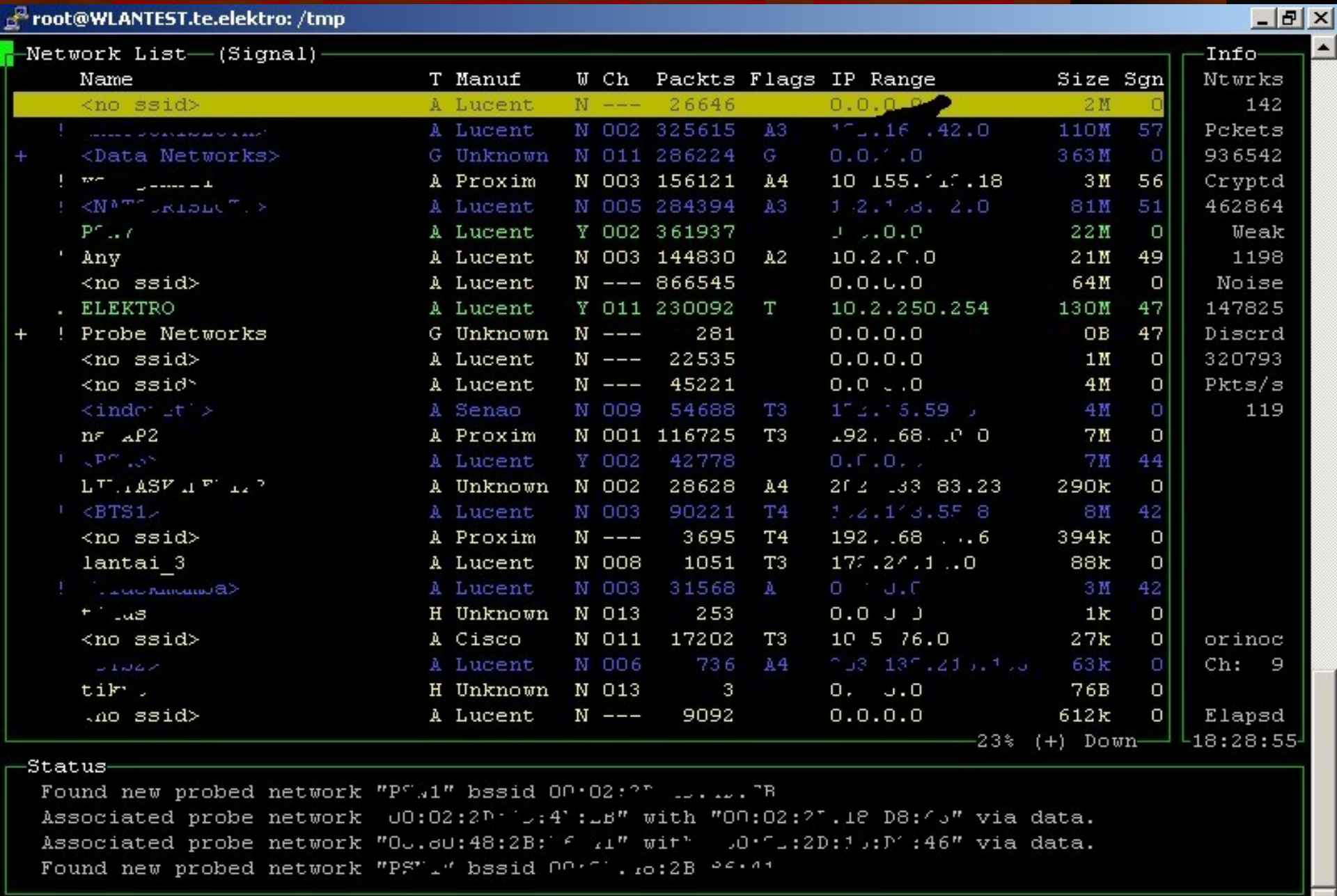
- Run kismet as superuser/root
- Run from shell/terminal console
- Run only in suiduser home directory (see kismet.conf) or in the directory that can be written by suiduser like /tmp
- cd /home/josh
- kismet


root@lognight.te.ugm.ac.id: /home/josh - Shell - Konsole
Session Edit View Bookmarks Settings Help
Network List (Signal)
Info
Name T W Ch Packts Flags IP Range
! compex A Y 011 1937 T4 172.24.14.34
! 3Com A N 006 5694 T3 172.24.14.0
lantai_1_elektro A N 002 1 0.0.0.0
<no ssid> A N --- 10 T4 172.16.160.108
. lantai_2 A N 007 72 0.0.0.0
Ntwrks
5
Pckets
14593
Cryptd
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

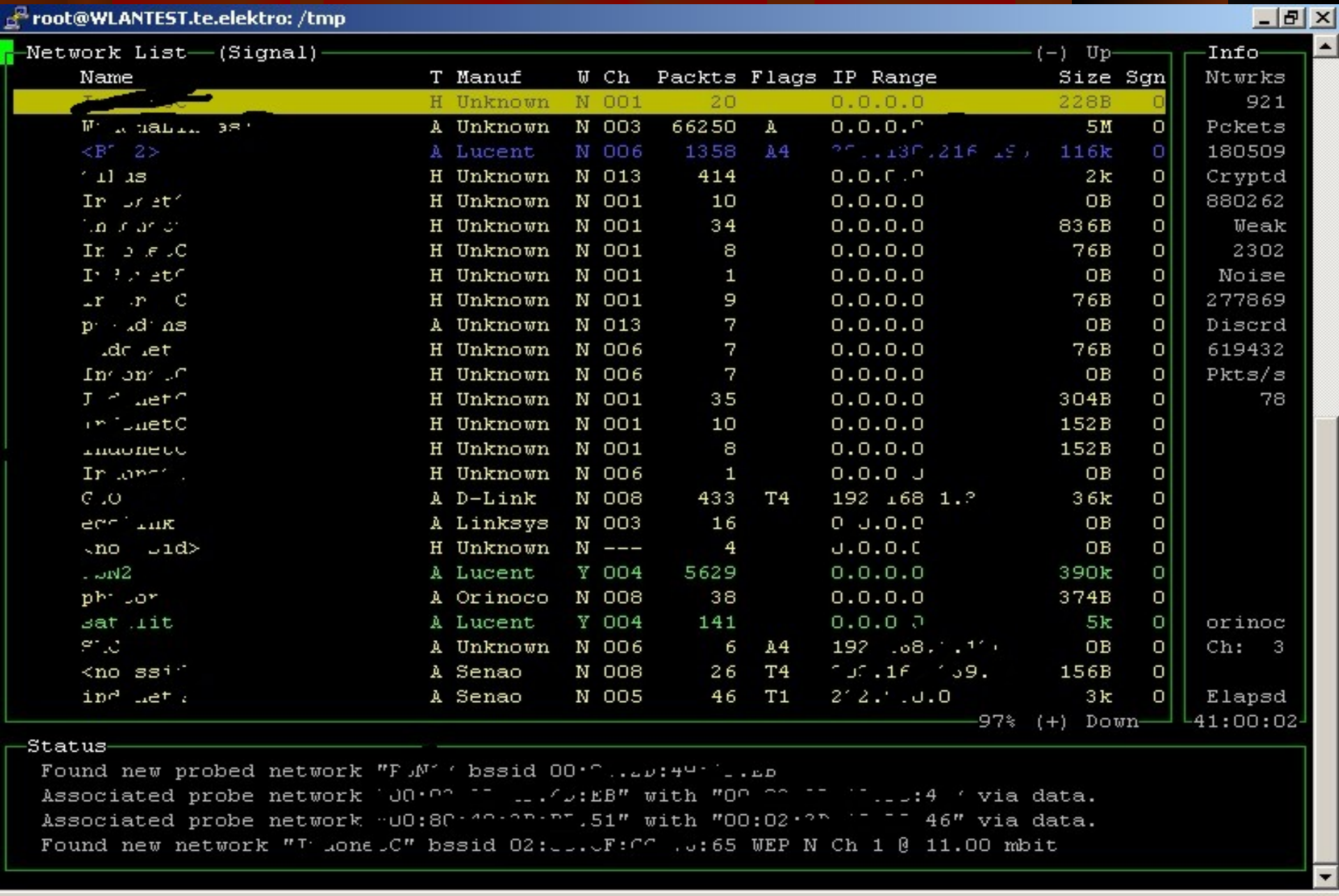
Press “h” for help



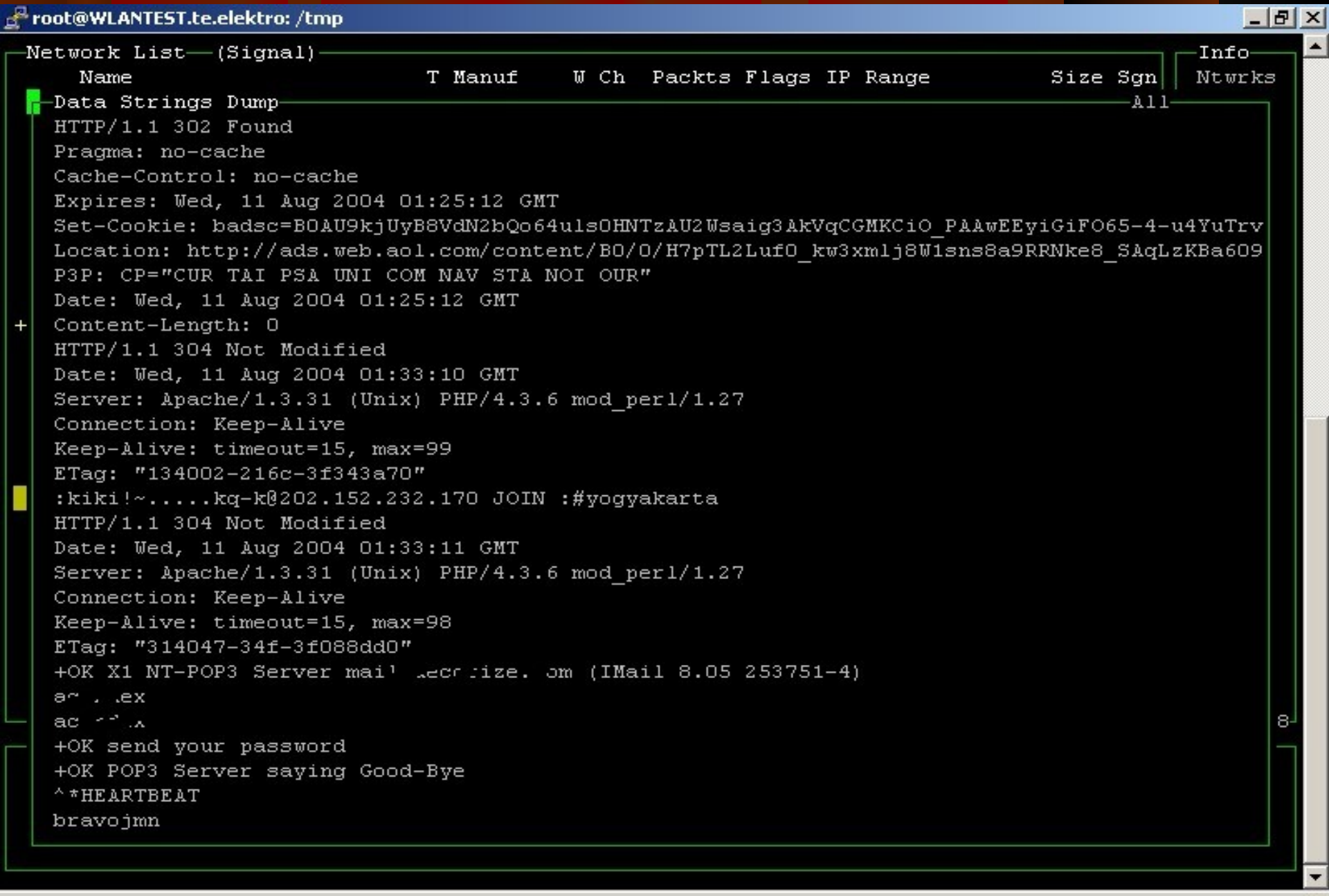
Kismet In Action



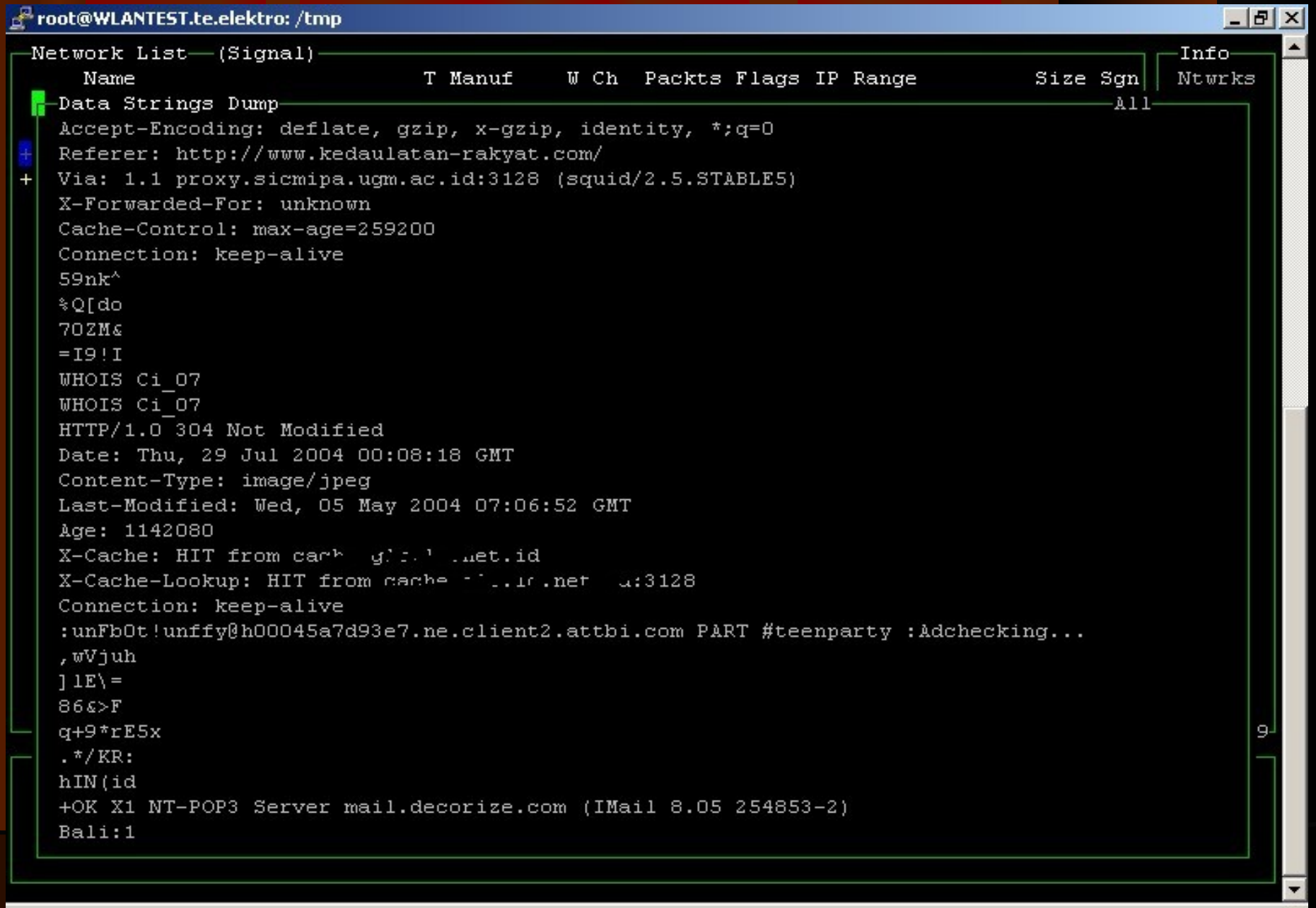
Kismet In Action



Kismet In Action



Kismet In Action



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.

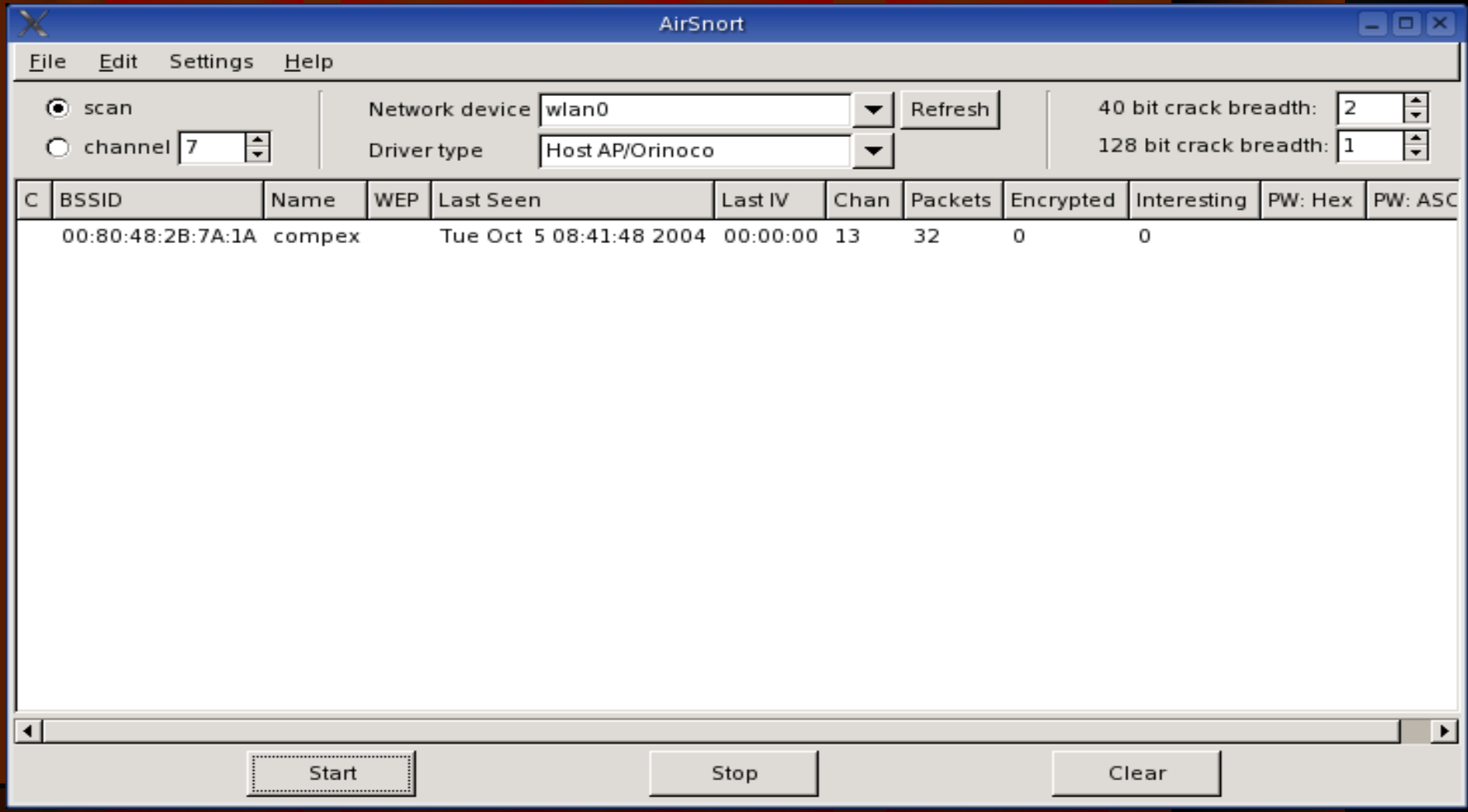
Compiling and Installing

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

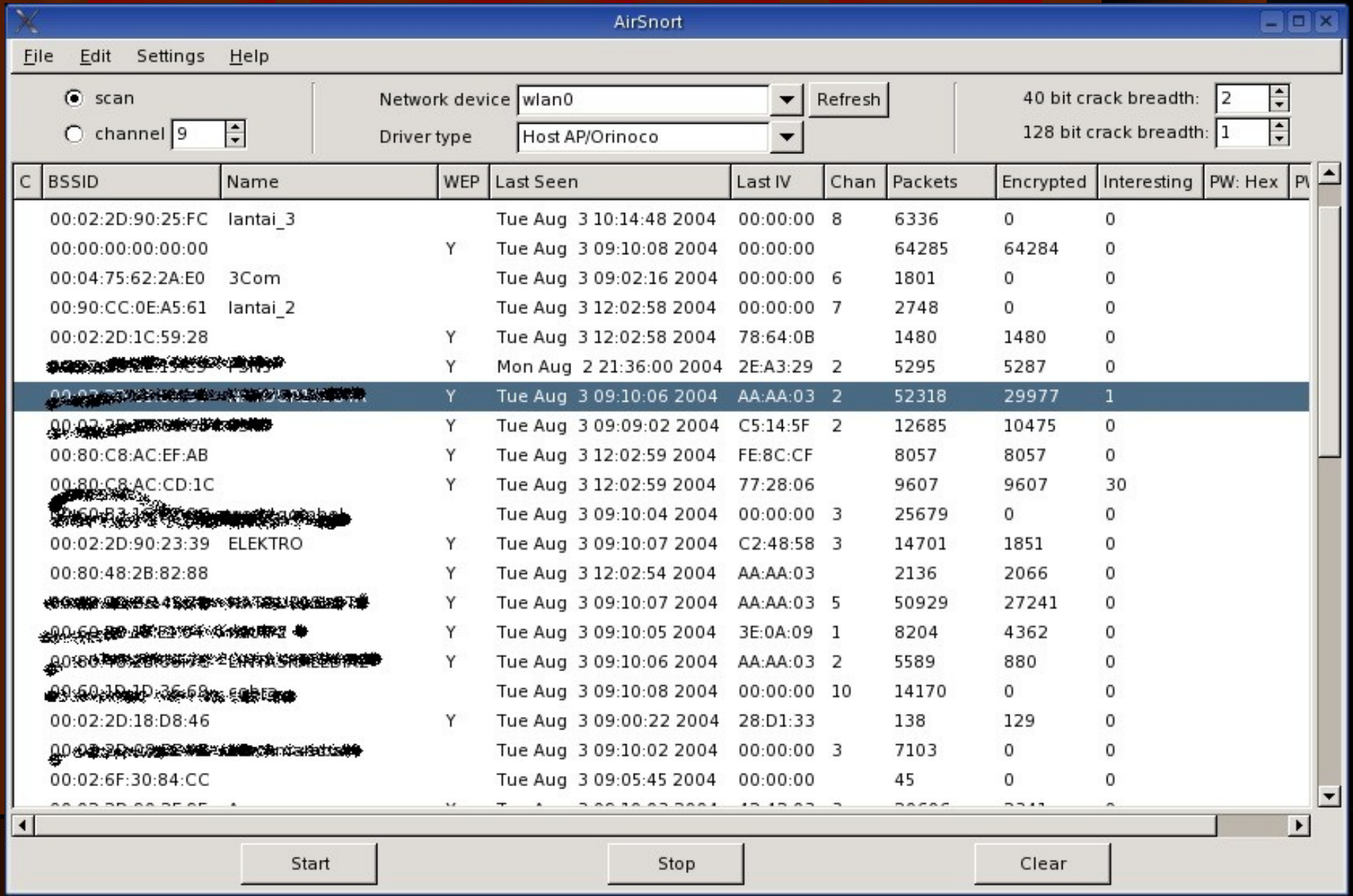
How to Run Airsnort

- 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



AirSnort In Action



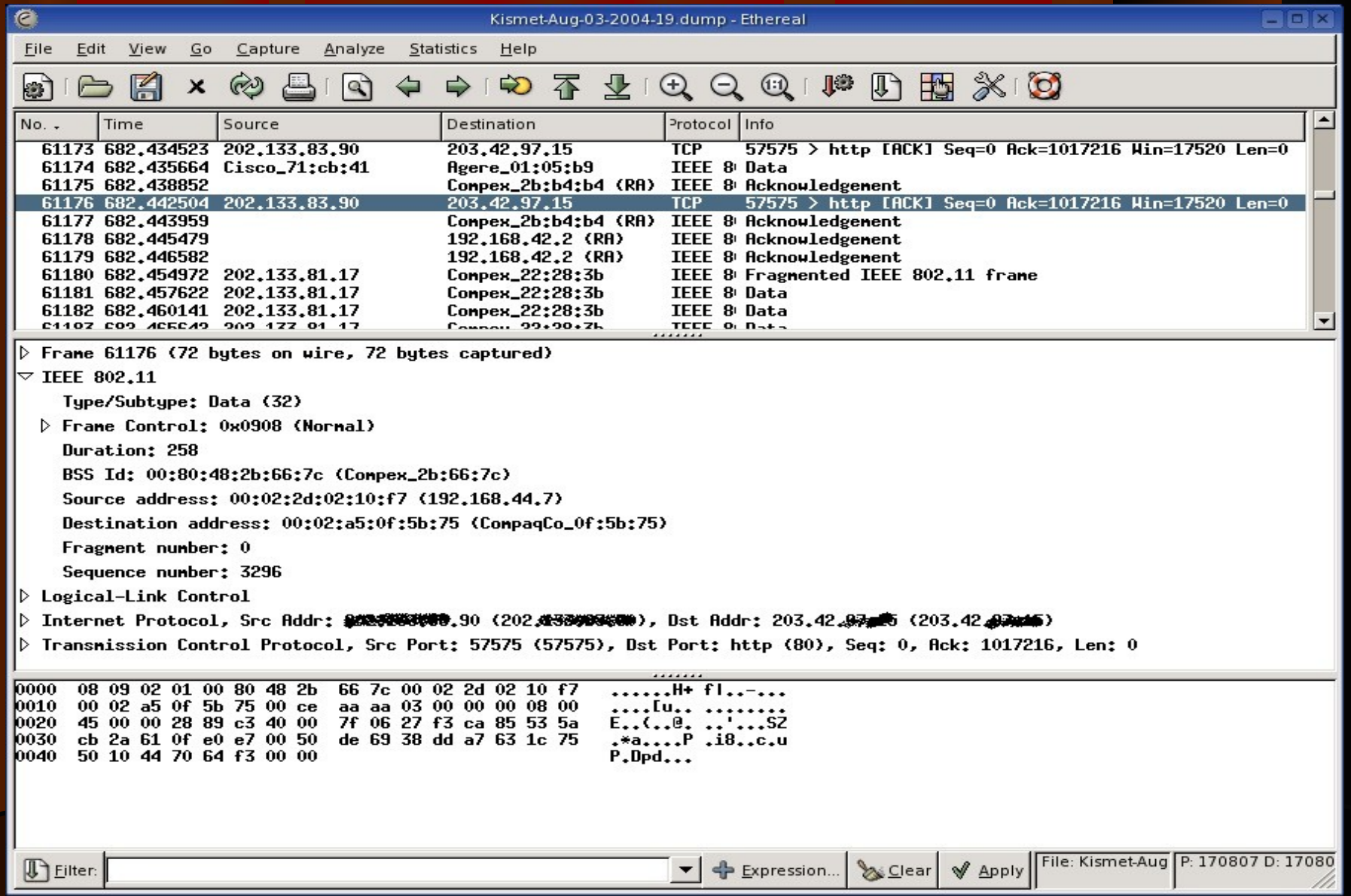
Ethereal

- 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

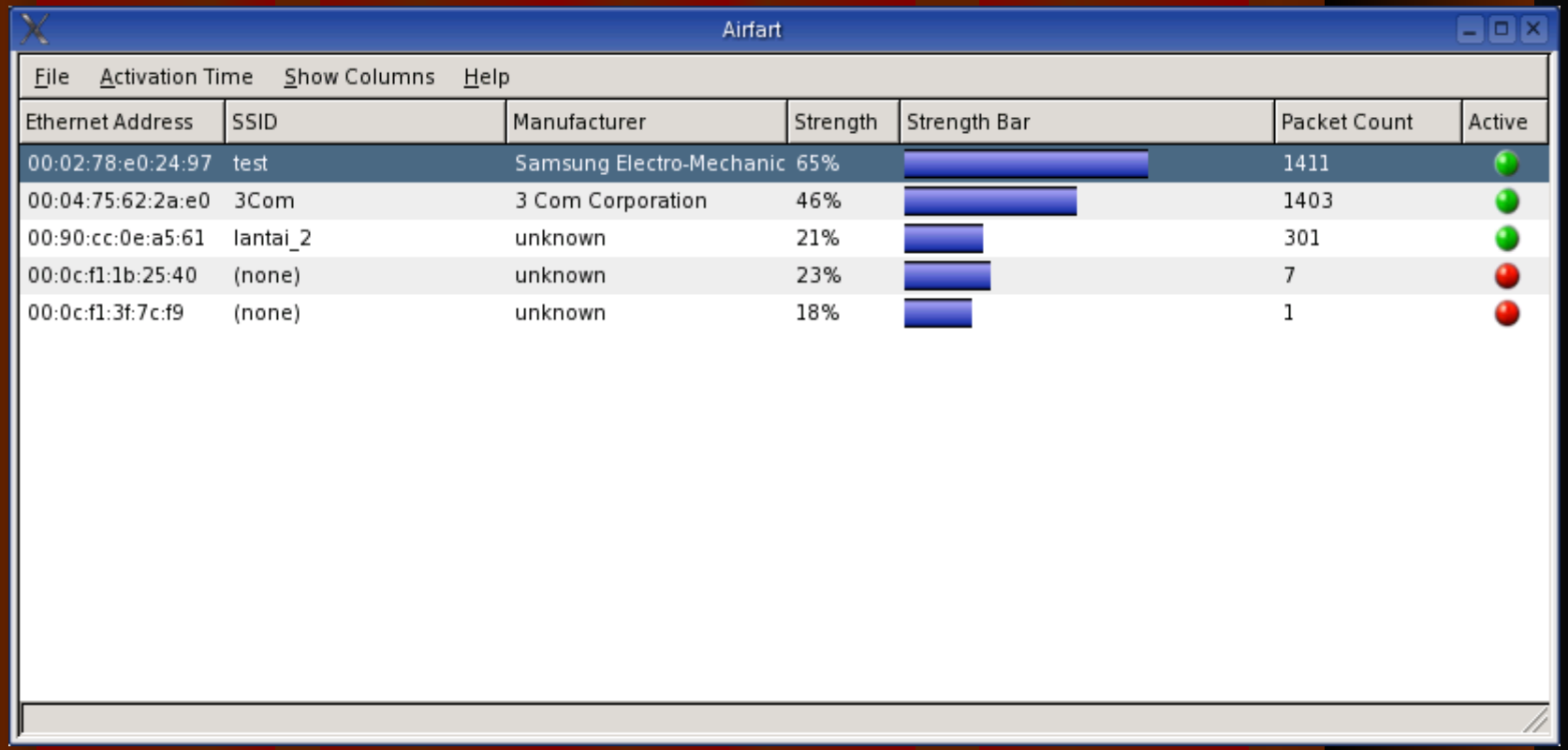


AirFart

- Used for Scanning and Wireless Monitoring
- Only supports prism2 cards with wlan-ng driver.
- Get source from :

  http://sourceforge.net/projects/airfart

AirFart Interfaces



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

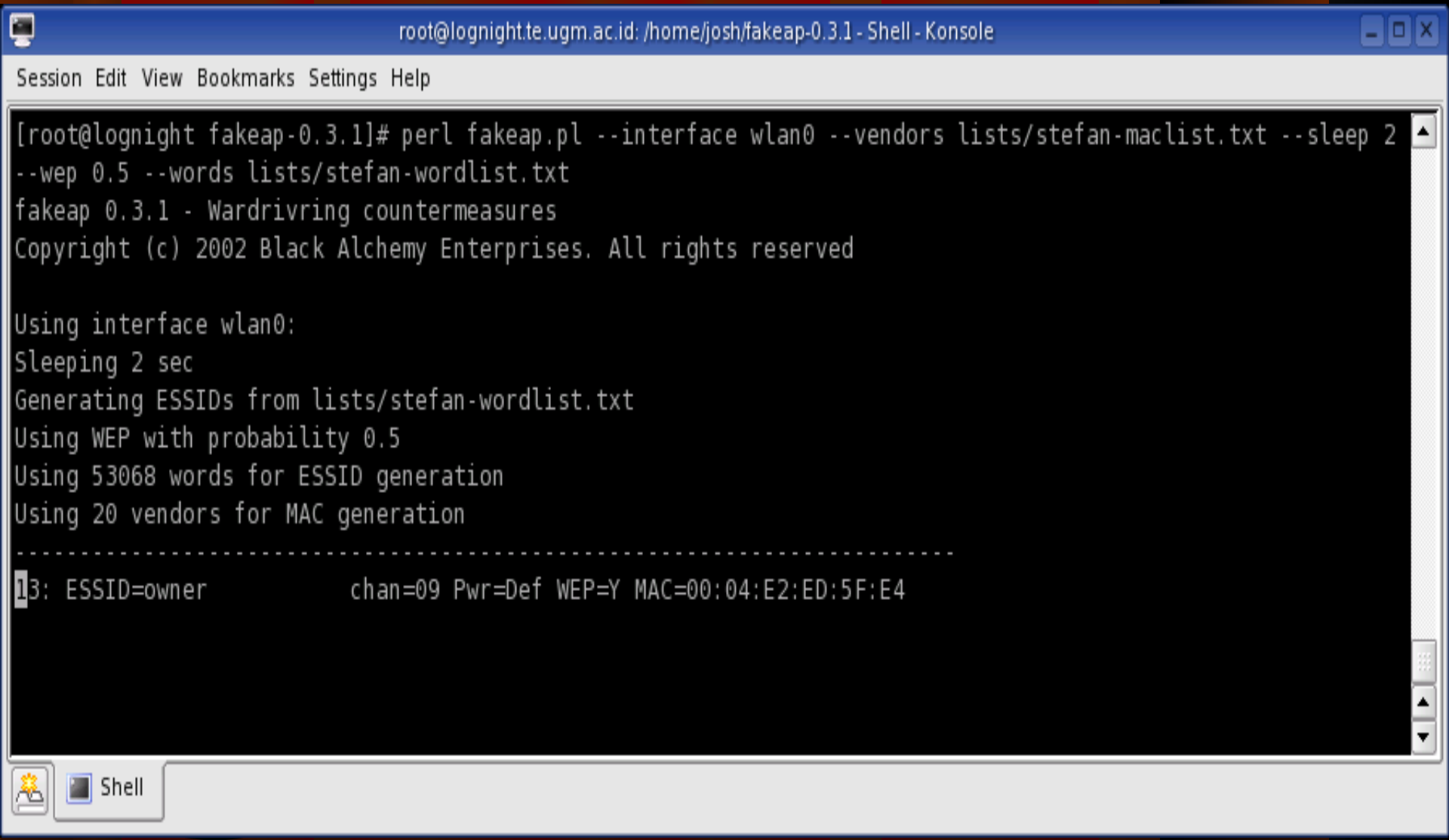
Edit fake.pl

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

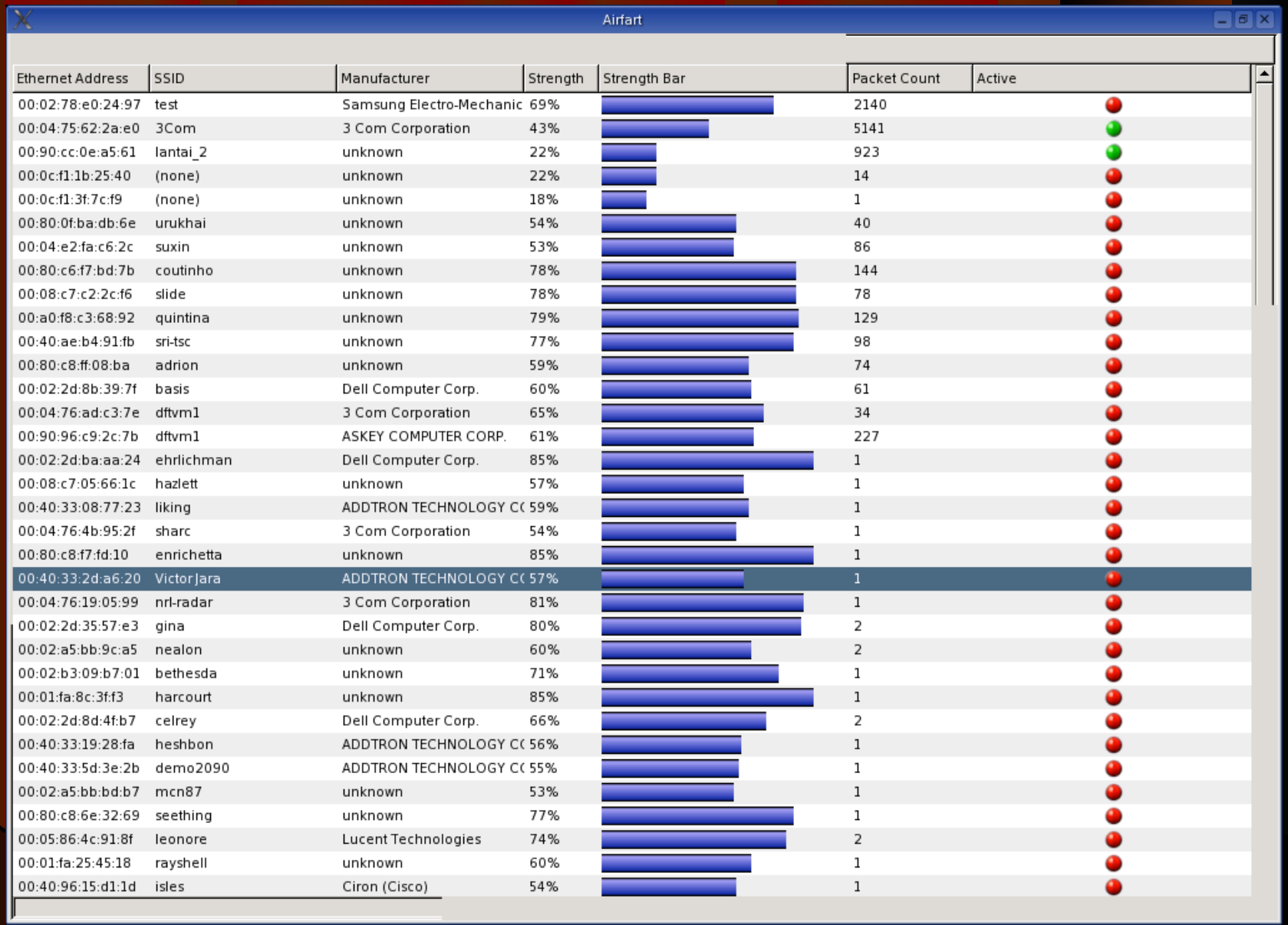
RUN fake.pl

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

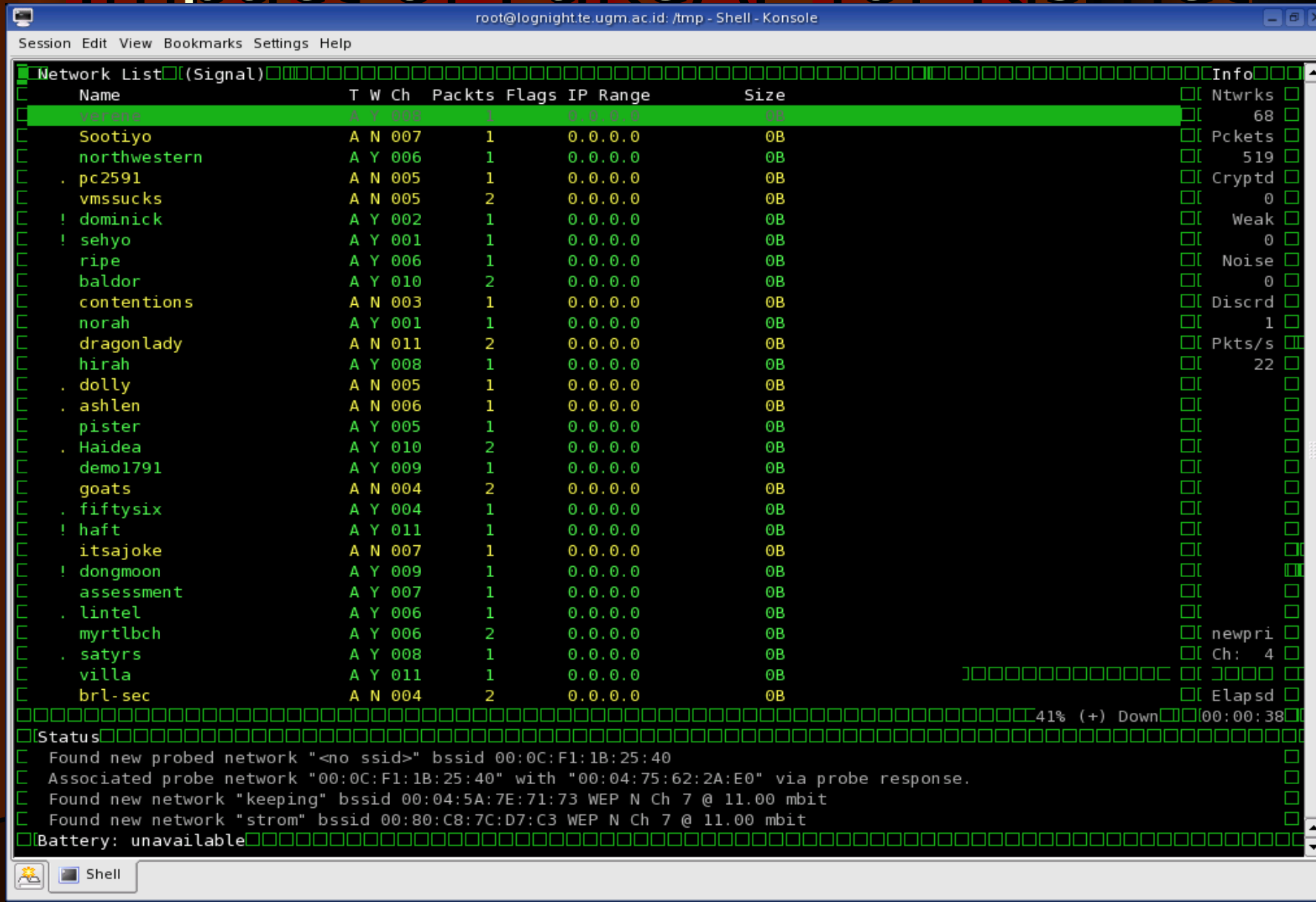
FakeAP in Action



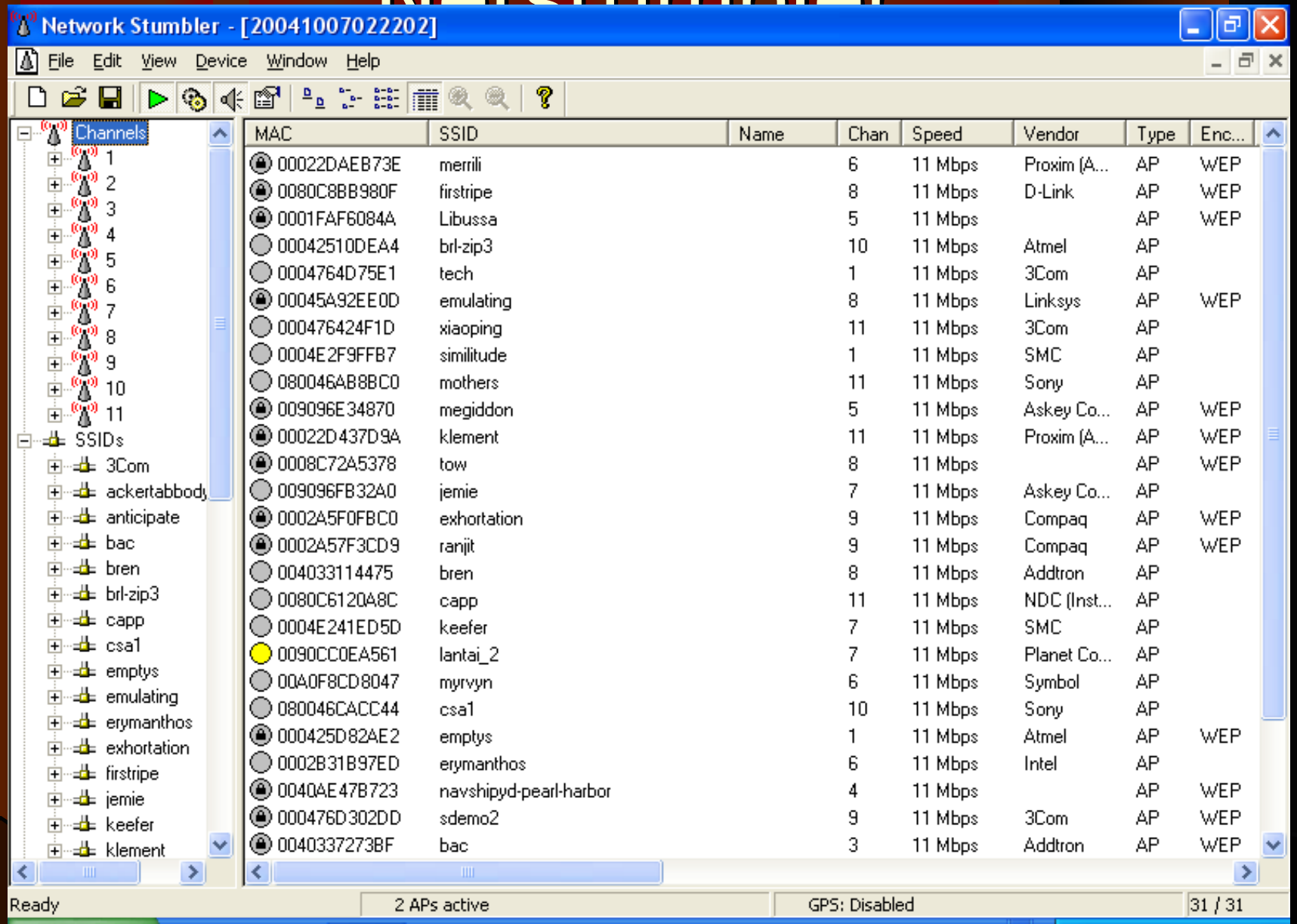
Impact of FakeAP for airfart



Impact of FakeAP for Kismet



Impact of FakeAP for Netstumbler



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