Kismet & GPSdrive

Wireless network sniffing with Open Source Software

Antony Stone

Antony.Stone@Open.Source.IT

Wardriving

- The name “wardriving” is derived from “wardialling”, which means dialling arbitrary phone numbers to find out which ones are answered by modems (a historically popular method of accessing computers remotely)

- Wardriving means travelling around with radio equipment, listening out for wireless network signals, and recording information about the networks

Background

- Packet sniffing
  - Long-established practice on cabled networks
  - Listen passively to packets from/to other machines passing on the wire
  - Requires NIC in “promiscuous mode”
- Wireless packet sniffing
  - Signals are broadcast by radio
  - Passive receiver can hear all communications
  - Wireless NIC still needs promiscuous mode
    - Actually, RFmon mode

Background

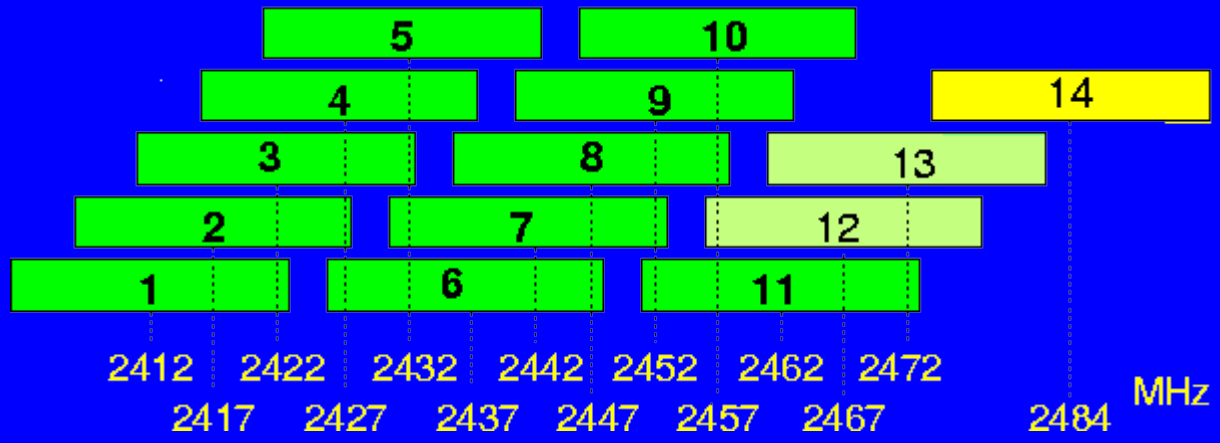
- Packet sniffing on cabled network - need physical connection
  - authorised user listening in on unauthorised traffic
- Packet sniffing on wireless network - can be (almost) anywhere
  - no requirement to be on the premises
  - may not be authorised user of network
  - passive sniffers impossible to detect

Why wireless packet sniffing?

- Access to interesting data
  - Targeted network eavesdropping
  - eg: content of emails
- Access to interesting information
  - Random network eavesdropping
  - eg: usernames / passwords
- Access to interesting networks
  - Bandwidth hijacking
  - eg: access to the Internet

802.11b networking

- 14 partially-overlapping channels ~2.45GHz



- Not all channels available in all countries
  - 11 in US, 13 in UK, 14 in Japan

802.11b networking

- Ad-hoc mode - between PCs (peer-to-peer)
- Infrastructure mode - Access Point is used like a hub on a cabled network
    - NB: a hub, not a switch - traffic is broadcast
- Each computer communicates with the AP
- Antenna on AP is very important
    - Signal power - strength of signals sent
    - Sensitivity - reception of weak signals

802.11b networking

- SSID
  - Service Set IDentifier
  - Name of the wireless network
- BSSID
  - Basic Service Set IDentifier
  - MAC address of Access Point
- Beacon frame broadcasts
  - “This is my BSSID!” every 0.1 seconds...

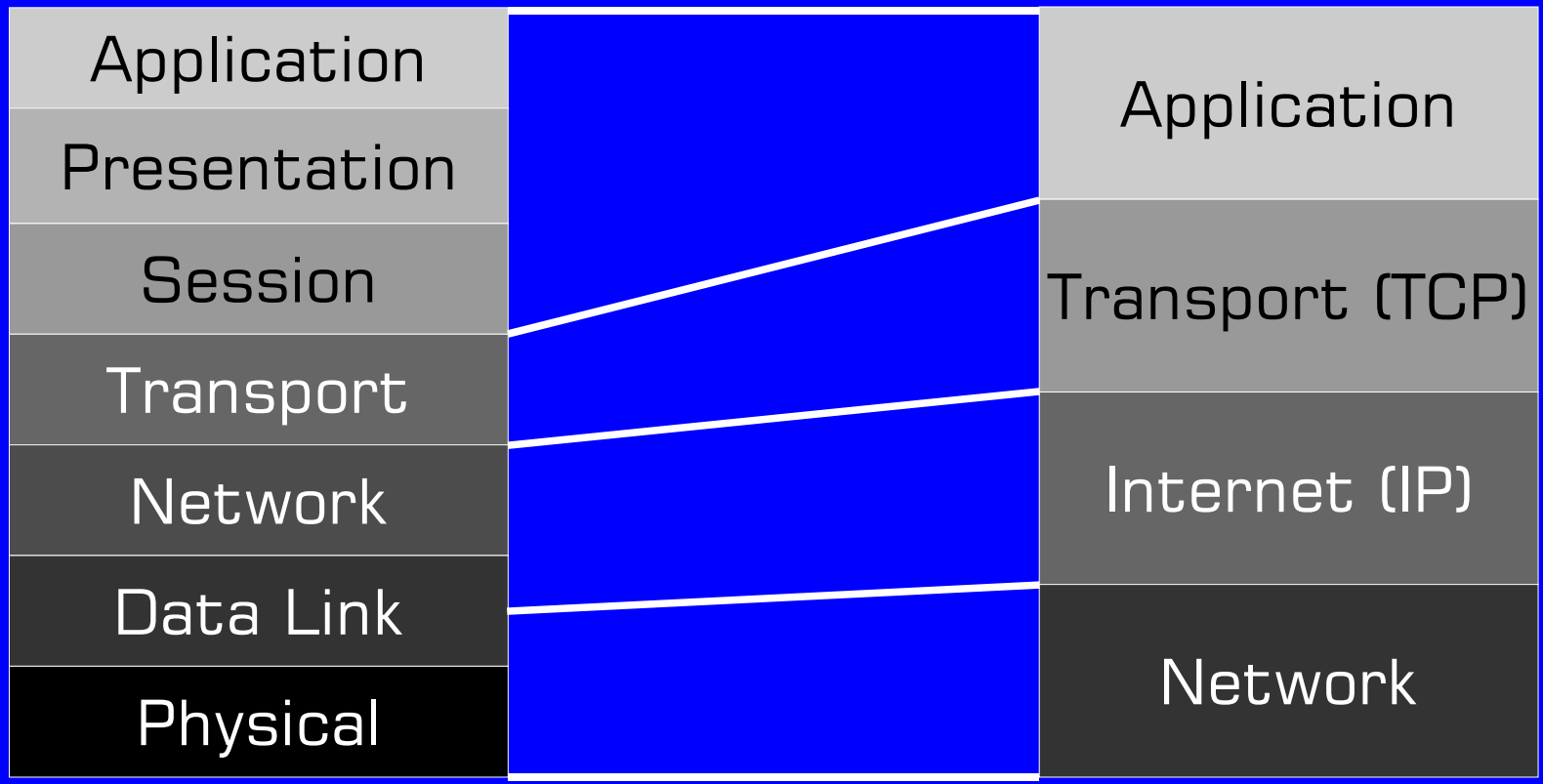
802.11b networking

- Passive network sniffing
  - 802.11 NIC in promiscuous mode with an antenna sensitive enough to pick up signals from:
    - Access Point
    - Communicating PCs
- Remote access to network (2-way)
  - Antenna needs to supply sufficient signal power to be picked up by Access Point (not PCs)
- Directional antennas are very helpful

Wireless network security

- WEP - Wired Equivalent Privacy
- Encrypt packet contents so that intercepting radio transmissions does not reveal data
- Data encryption based on RC4 algorithm
  - Same as used in SSL/TLS, Kerberos
  - Perfectly good stream cipher, if used correctly
- Cannot encrypt everything
- MAC addresses need to remain unencrypted

OSI & TCP/IP networking models



OSI 7-layer model

TCP/IP 4-layer model

Packets and headers

- HTTP request

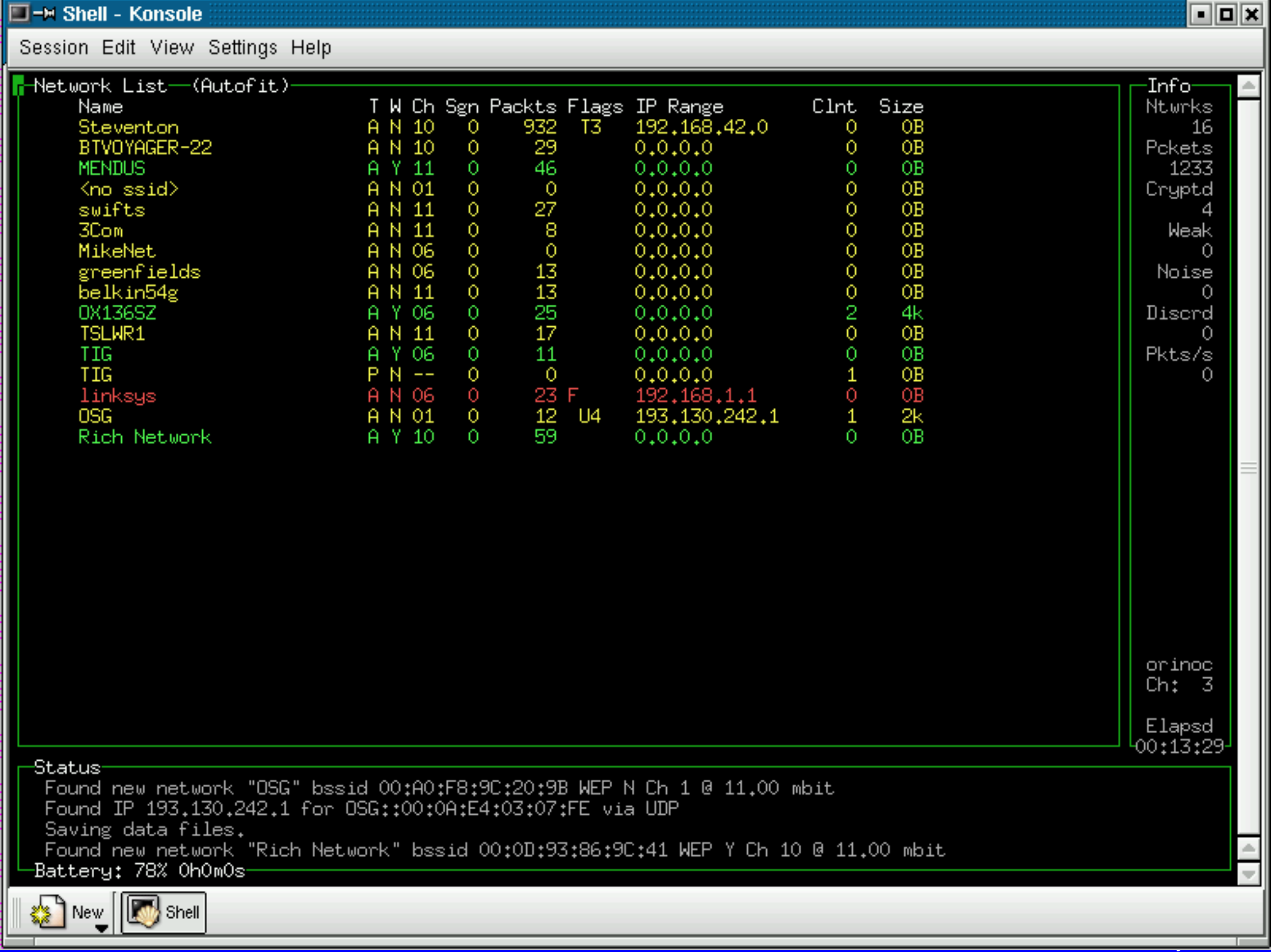
- TCP header

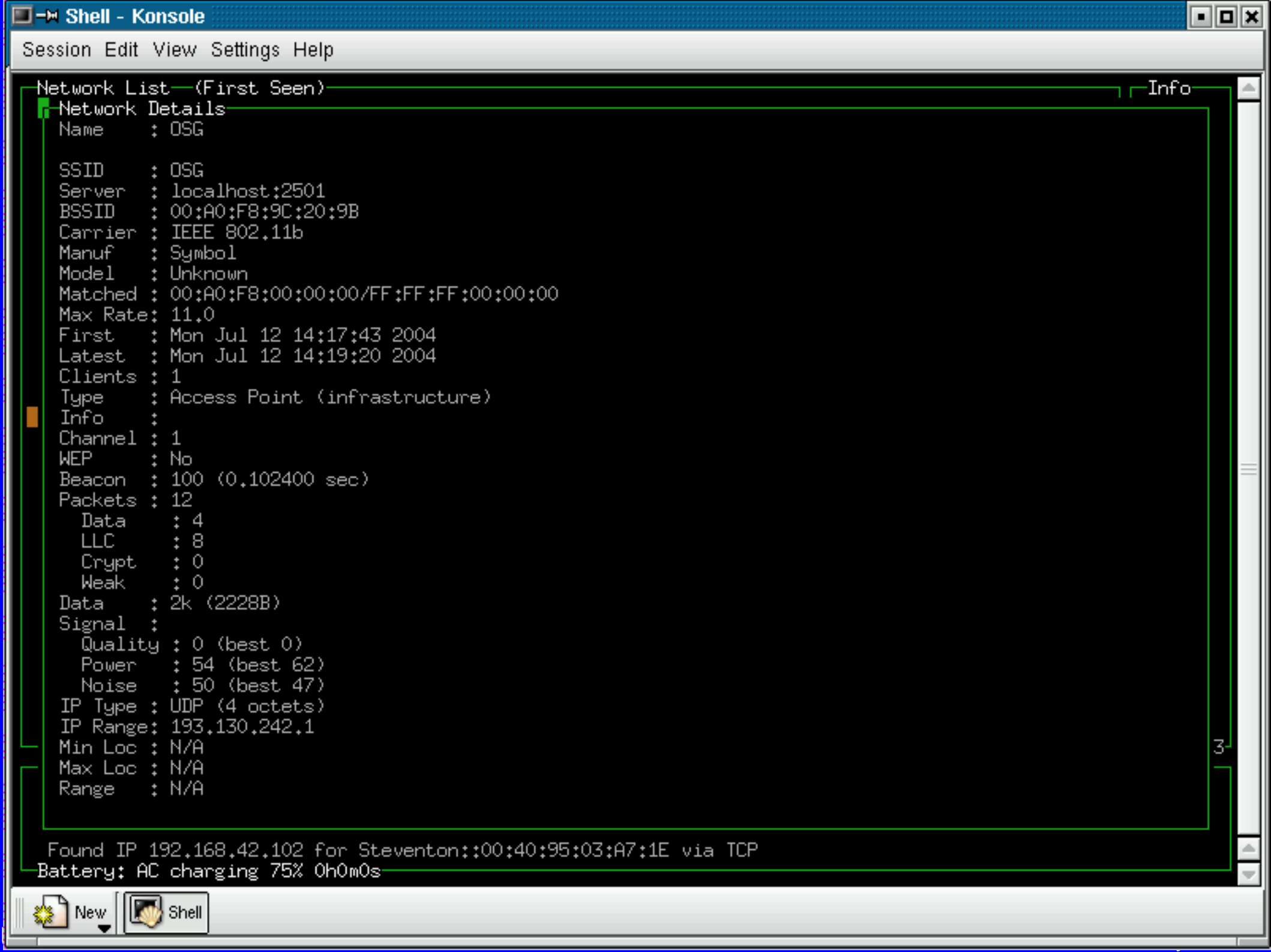
- IP header

- Ethernet or 802.11b header

Kismet packet sniffer

- What information will Kismet record?
  - Channel number
  - Network name (SSID)
  - Access point MAC address (BSSID)
    - Access point Manufacturer
  - SSID set to default?
  - WEP on or off?
  - Number of client systems connected
  - IP address range in use (a bit of a guess)
  - Content of packets (datastream)


Shell - Konsole
Session Edit View Settings Help
Network List (Autofit)
Name T W Ch Sgn Packts Flags IP Range Clnt Size
Steventon A N 10 0 932 T3 192.168.42.0 0 0B
BTVOYAGER-22 A N 10 0 29 0.0.0.0 0 0B
MENDUS A Y 11 0 46 0.0.0.0 0 0B
<no ssid> A N 01 0 0 0.0.0.0 0 0B
swifts A N 11 0 27 0.0.0.0 0 0B
3Com A N 11 0 8 0.0.0.0 0 0B
MikeNet A N 06 0 0 0.0.0.0 0 0B
greenfields A N 06 0 13 0.0.0.0 0 0B
belkin54g A N 11 0 13 0.0.0.0 0 0B
OX136SZ A Y 06 0 25 0.0.0.0 2 4k
TSLWR1 A N 11 0 17 0.0.0.0 0 0B
TIG A Y 06 0 11 0.0.0.0 0 0B
TIG P N -- 0 0 0.0.0.0 1 0B
linksys A N 06 0 23 F 192.168.1.1 0 0B
OSG A N 01 0 12 U4 193.130.242.1 1 2k
Rich Network A Y 10 0 59 0.0.0.0 0 0B
Info
Ntwrks 16
Pckets 1233
Cryptd 4
Weak 0
Noise 0
Discrd 0
Pkts/s 0
orinoc
Ch: 3
Elapsd
00:13:29
Status
Found new network "OSG" bssid 00:A0:F8:9C:20:9B WEP N Ch 1 @ 11.00 mbit
Found IP 193.130.242.1 for OSG::00:0A:E4:03:07:FE via UDP
Saving data files.
Found new network "Rich Network" bssid 00:0D:93:86:9C:41 WEP Y Ch 10 @ 11.00 mbit
Battery: 78% 0h0m0s
New
Shell


Shell - Konsole
Session Edit View Settings Help
Network List (First Seen)
Info
Network Details
Name : OSG
SSID : OSG
Server : localhost:2501
BSSID : 00:A0:F8:9C:20:9B
Carrier : IEEE 802.11b
Manuf : Symbol
Model : Unknown
Matched : 00:A0:F8:00:00:00/FF:FF:FF:00:00:00
Max Rate: 11.0
First : Mon Jul 12 14:17:43 2004
Latest : Mon Jul 12 14:19:20 2004
Clients : 1
Type : Access Point (infrastructure)
Info :
Channel : 1
WEP : No
Beacon : 100 (0.102400 sec)
Packets : 12
Data : 4
LLC : 8
Crypt : 0
Weak : 0
Data : 2k (2228B)
Signal :
Quality : 0 (best 0)
Power : 54 (best 62)
Noise : 50 (best 47)
IP Type : UDP (4 octets)
IP Range: 193.130.242.1
Min Loc : N/A
Max Loc : N/A
Range : N/A
Found IP 192.168.42.102 for Steventon::00:40:95:03:A7:1E via TCP
Battery: AC charging 75% 0h0m0s
New
Shell

Kismet vs. Netstumbler

- Kismet places 802.11 card in RFmon mode, which allows full capture of data from all networks on all channels (sequentially)
- Netstumbler uses firmware on the 802.11 card to discover networks seen by the card
  - Active monitoring - Netstumbler is “noisy”
  - Netstumbler does not detect “cloaked” networks
  - Netstumbler does not capture data - only network names

Kismet - hardware

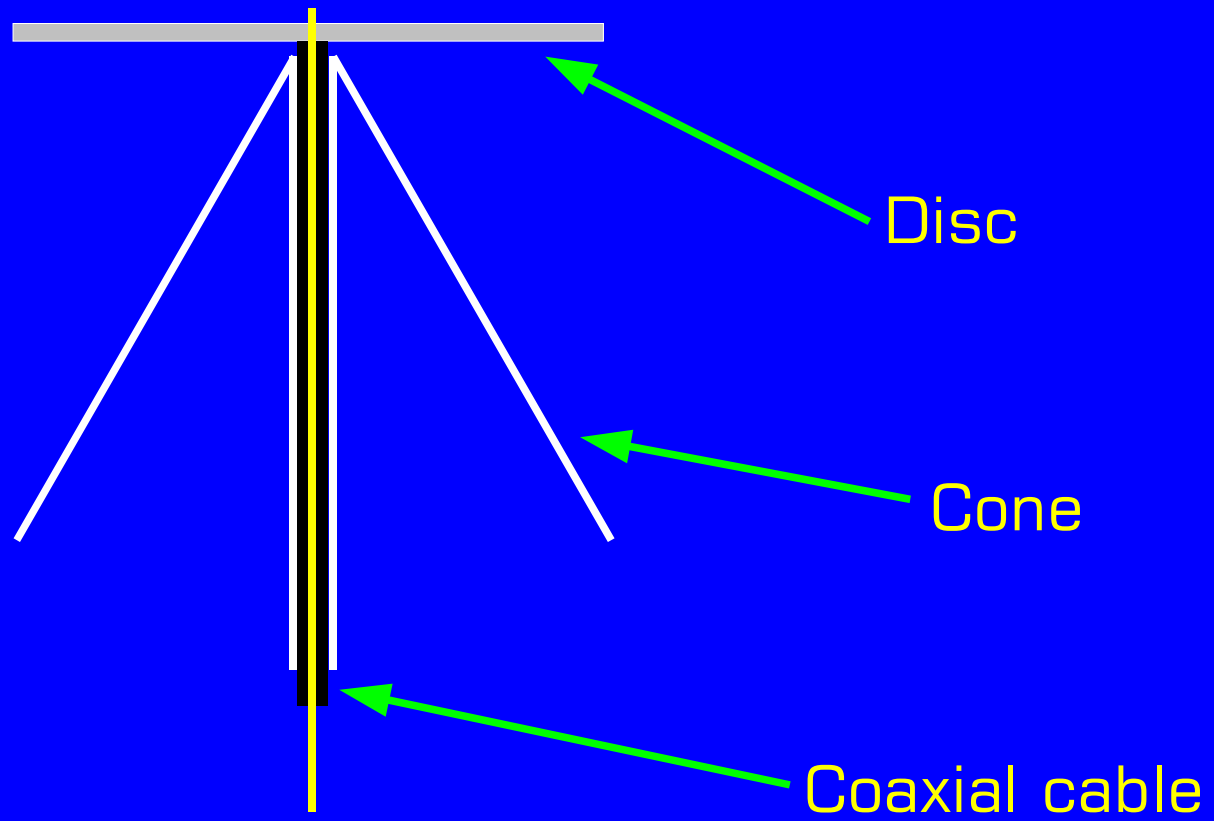
- Fundamental requirement is 802.11 card!
  - PCI
  - PCMCIA
  - USB
- Must support RFmon mode
  - eg: based on Prism2 chipset
- Some USB adapters
  - Netgear MA-111

Long range antennas

- Wardriving works best with omnidirectional antenna
  - PCMCIA built-in is not much good
    - Very short range
  - PCI built-in is better (but not great)
  - External antennas
    - Discone
    - Pringles / soup tin cantenna
    - Parabolic reflector

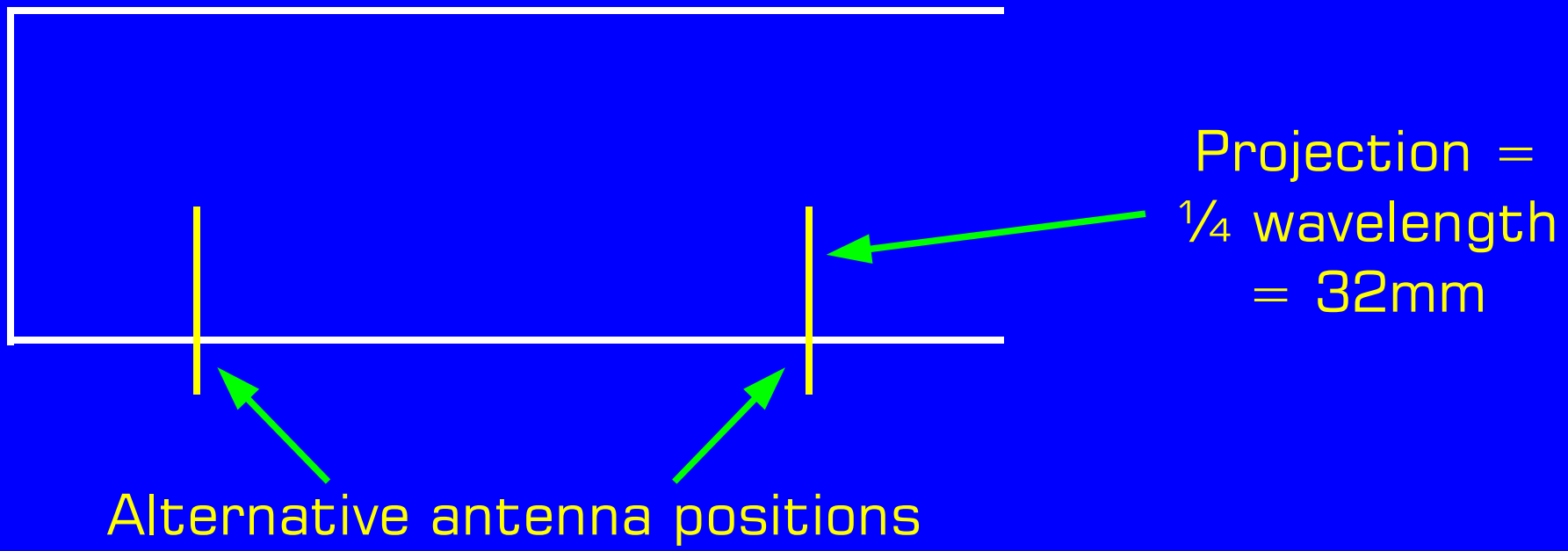
Discone antenna

- Good “flat” omnidirectional reception



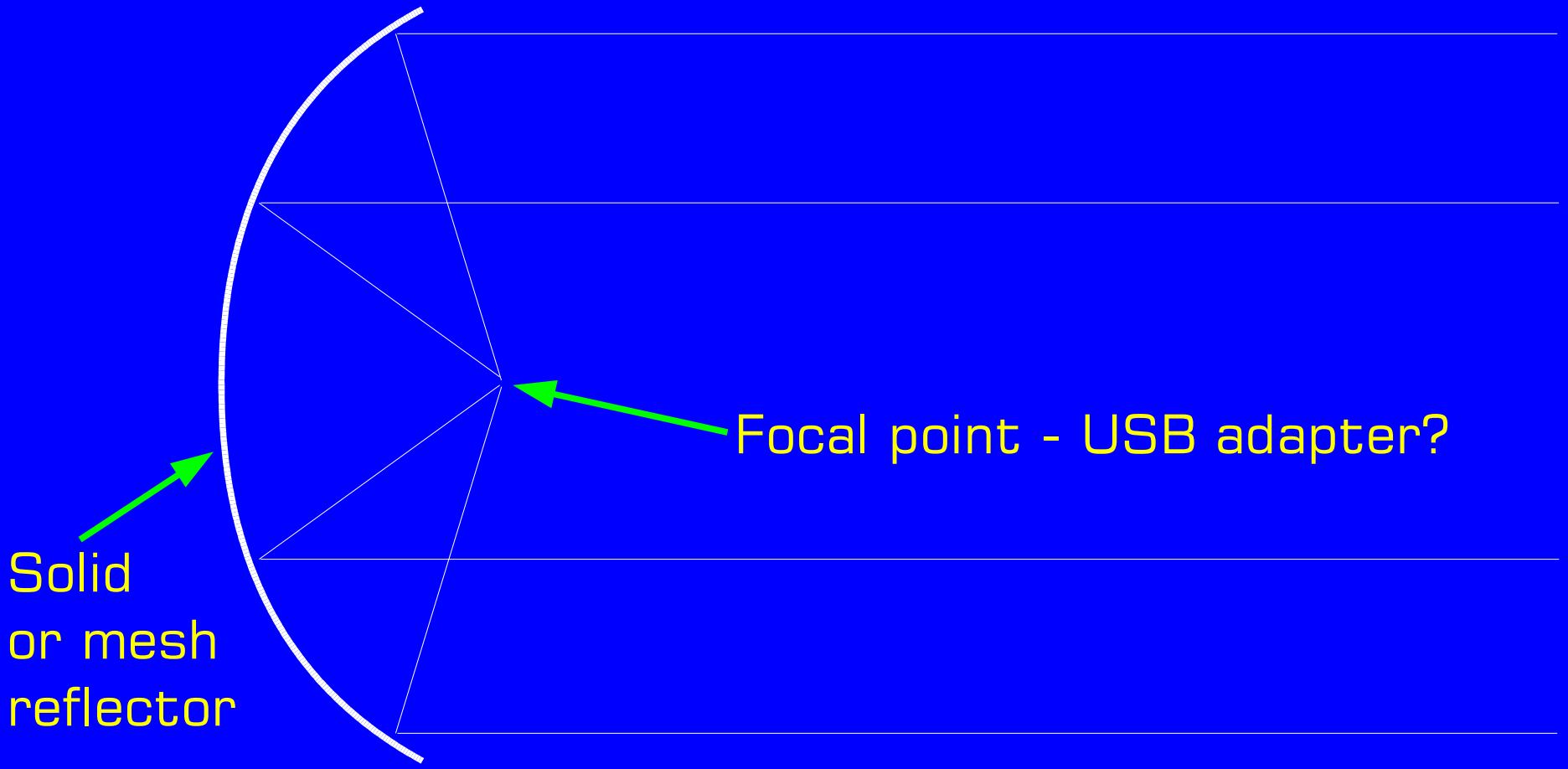
Pringles / soup tin cantenna

- Directional - increases signal:noise ratio



Parabolic reflector antenna

- Highly directional - very long range



Choosing the right antenna

- Wardriving - omnidirectional receiver
  - Discone works well
  - Cantenna not ideal
  - Parabolic can be used to scan from a fixed point
- Network interception / hijacking - directional receive + transmit
  - Distance depends on location (car park / hilltop?)
  - Discone not good
  - Cantenna / parabolic depending on distance

Wireless network security

- 64-bit or 128-bit key
  - 40 or 104 'secret' bits, plus 24 'public' bits
  - 24 public bits are “Initialisation Vector”
- First bytes of IP header are predictable
  - “Known plaintext” attack
- Stream cipher
  - plaintext -XOR- key = cryptotext
  - plaintext -XOR- cryptotext = key

Wireless network (in)security

- Weak keys
  - 2^24 Initialisation Vectors = 16 million
  - ~9000 indicate "weak keys"
    - Weak keys are easier to guess
- 802.11 does not say how IV should change
  - Some vendors start at zero and increment
  - Some choose (pseudo) random numbers
  - Random is worse because IVs will start to be reused after only 50% of the time!

Wireless network insecurity

- 24 bit IV
  - 16 million possible IVs
  - 1500 bytes per packet (max)
  - 11Mbits per second
  - IVs repeat after 5 hours!
- Less busy network - takes more time
- Smaller packets - takes less time
- WEP is guaranteed crackable, with purely passive sniffing, in a short time

GPSdrive

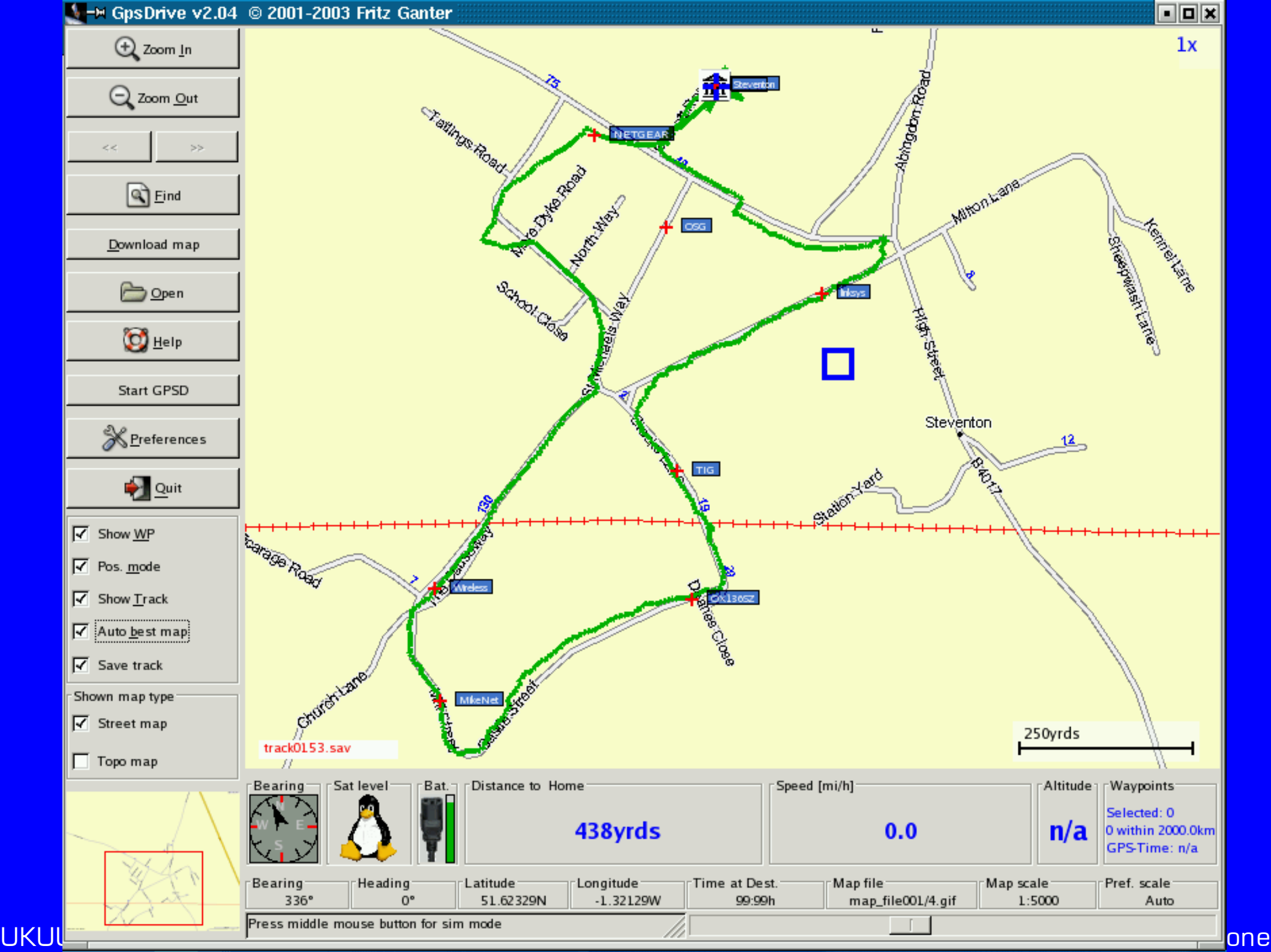
- GPSdrive is a completely independent package from Kismet, but includes Kismet support
- GPSdrive displays position, velocity, track, waypoints, places on a moving-map display
- GPSdrive is not a route-planning system
  - Doesn't tell you where to go, shows you where you've been
- Places can be stored in MySQL database
  - Also in plain text files

GPSdrive

- GPSdrive requires:
  - Computer (laptop is convenient)
  - GPS receiver (RS232 / USB connection)
- Maps can be pre-loaded, or added later
  - Not supplied with software
- Speech output supported via Festival
  - Commentary on distance from target, current speed, time
  - Calls out names of wireless networks as they are detected!

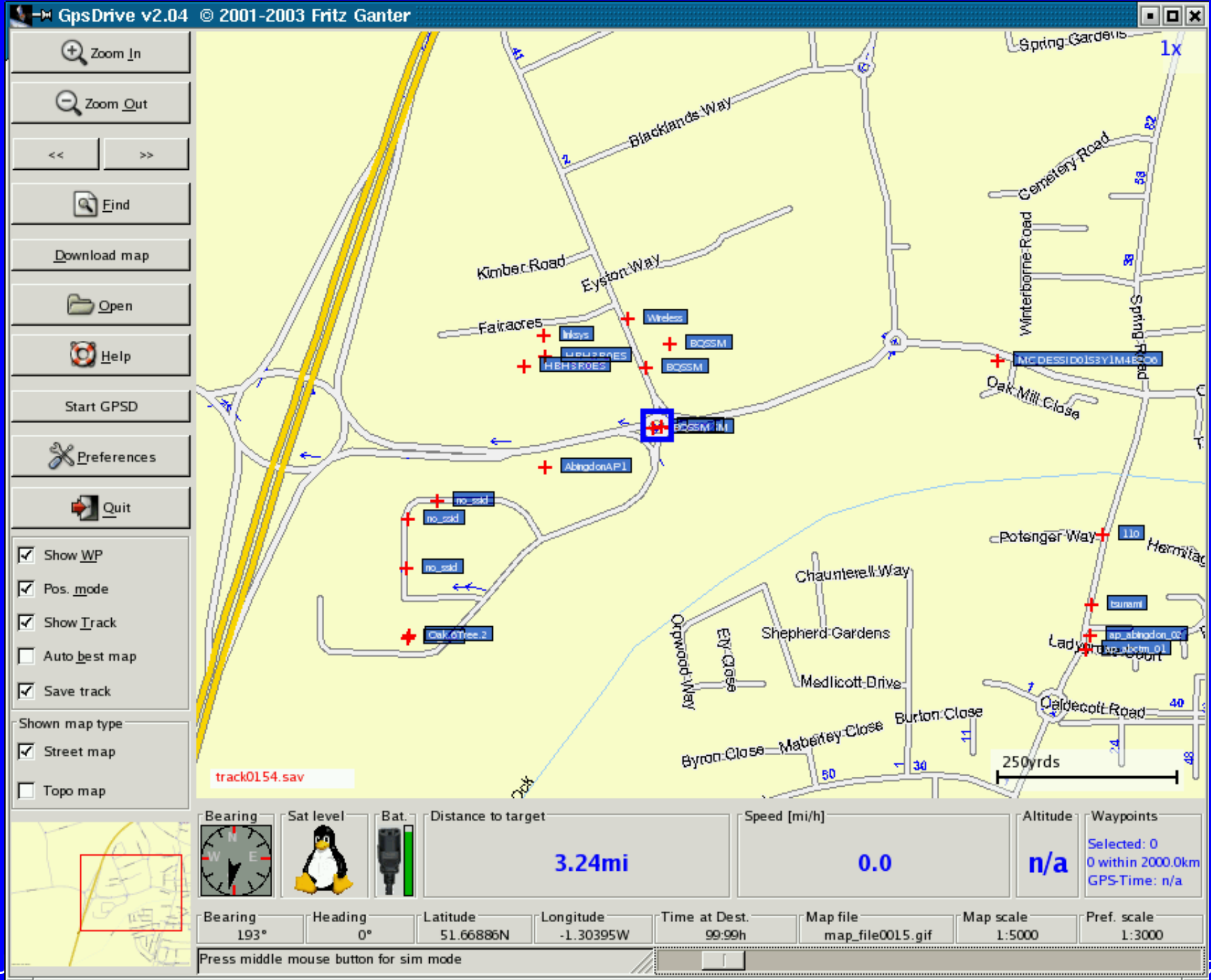
GPSdrive

- Additional features
  - Database supports multiple icon types
  - Includes speed cameras
  - Downloadable databases of speed camera locations
  - Speech synthesiser will call out distance to speed camera + current speed
    - Doesn't know area speed limits


GpsDrive v2.04 © 2001-2003 Fritz Ganter
Zoom In
Zoom Out
<<
>>
Find
Download map
Open
Help
Start GPSD
Preferences
Quit
Show WP
Pos. mode
Show Track
Auto best map
Save track
Shown map type
Street map
Topo map
1x
Steventon
NETGEAR
OSG
Mays
TIG
Wireless
OK136SZ
MikeNet
Tattings Road
Mike Dyke Road
North Way
School Close
St Michaels Way
Abingdon Road
Milton Lane
Sheepwash Lane
Kennel Lane
High Street
Steventon
B4017
Station Yard
Garage Road
Church Lane
Castle Street
Dianes Close
track0153.sav
250yrds
Bearing
Sat level
Bat.
Distance to Home
438yrds
Speed [mi/h]
0.0
Altitude
n/a
Waypoints
Selected: 0
0 within 2000.0km
GPS-Time: n/a
Bearing
336°
Heading
0°
Latitude
51.62329N
Longitude
-1.32129W
Time at Dest.
99:99h
Map file
map_file001/4.gif
Map scale
1:5000
Pref. scale
Auto
Press middle mouse button for sim mode

Kismet & GPSdrive in combination

- Kismet records network details
- GPSdrive displays network SSIDs at their locations on moving map
- Calls out names of networks as they are detected
- Encrypted & unencrypted (WEP / open) networks are displayed with different symbols
- Map can be recalled later to identify location of “interesting” networks


GpsDrive v2.04 © 2001-2003 Fritz Ganter
Zoom In
Zoom Out
<<
>>
Find
Download map
Open
Help
Start GPSD
Preferences
Quit
Show WP
Pos. mode
Show Track
Auto best map
Save track
Shown map type
Street map
Topo map
1x
Spring Gardens
Blacklands Way
Cemetery Road
Kimber Road
Eyston Way
Fairacres
Winterborne Road
Spring Road
Oak Mill Close
Potenger Way
Chaunterell Way
Shepherd Gardens
Medlicott Drive
Oxford Way
Ely Close
Byron Close
Mabeley Close
Burton Close
Caldecott Road
track0154.sav
250yrds
Bearing
Sat level
Bat.
Distance to target
3.24mi
Speed [mi/h]
0.0
Altitude
n/a
Waypoints
Selected: 0
0 within 2000.0km
GPS-Time: n/a
Bearing
193°
Heading
0°
Latitude
51.66886N
Longitude
-1.30395W
Time at Dest.
99:99h
Map file
map_file0015.gif
Map scale
1:5000
Pref. scale
1:3000
Press middle mouse button for sim mode

Resources

- Kismet

  http://www.kismetwireless.net
- GPSdrive

  http://gpsdrive.kraftvoll.at
- Festival speech synthesis
  - linked from GPSdrive site, but also at

  http://www.cstr.ed.ac.uk/projects/festival
- Google for Discone, Cantenna, "DIY 802.11"