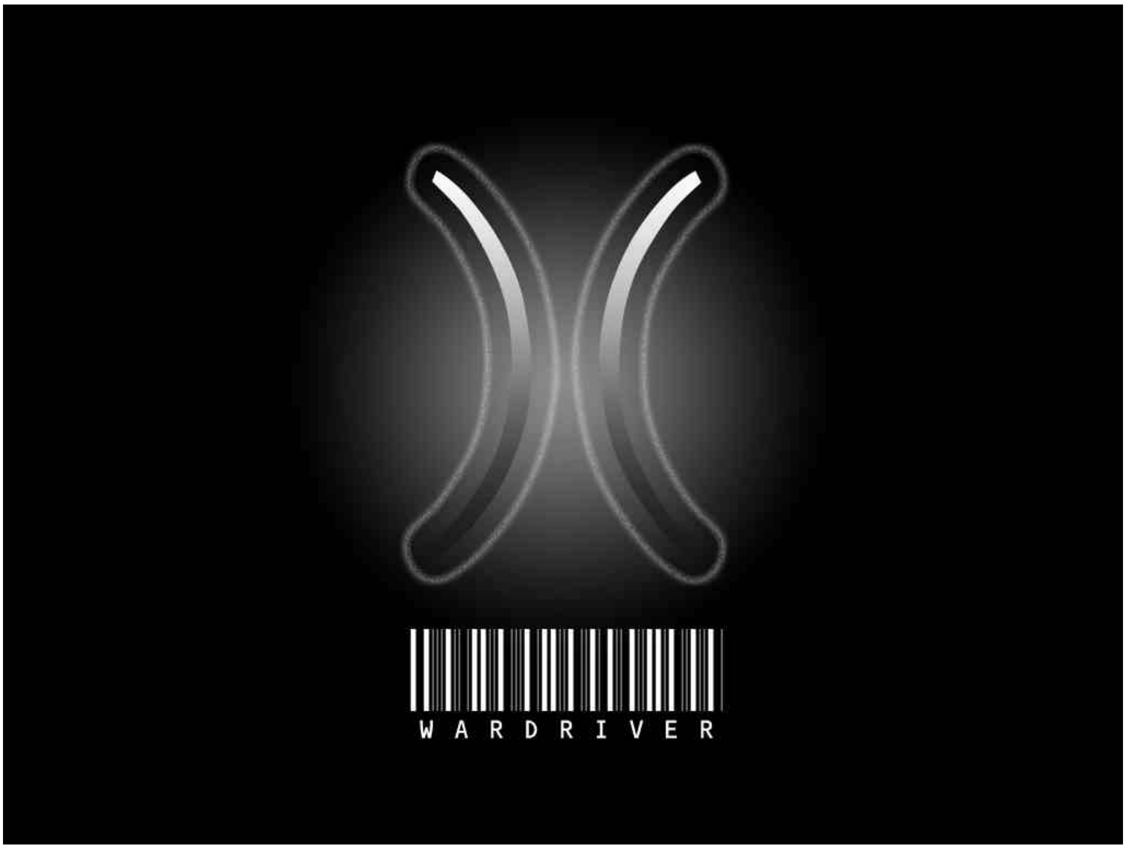
God de Vader
Godje@skynet.be
http://users.skynet.be/multibox

Version 1.0

WARDRIVING MANUAL



WARDRIVING MANUAL 1

DISCLAIMER 3

REQUIREMENTS: 4

WHAT DO I NEED IN HARDWARE? 4
A LAPTOP. 4
A WIRELESS LAN CARD 4
EXTRA: A GPS WITH CONNECTION CABLE 4
EXTRA: A CAR POWER SUPPLY IS USEFULL 5
EXTRA: TWEAKED ANTENNA 5

SOFTWARE 6

WHAT YOU NEED 6

DRIVING AROUND 7

GPS CONFIGURATION 7
SOUND IS BETTER THEN VIEW 8
READY? 9
WHAT NOW? 9
ACCESS POINT FOUND 10
OPTION ONE PROTECTED AP 10
OPTION TWO OPEN AP 11
IF YOU DON'T GET AN DHCP IP ADDRESS… 12
WHY THESE SETTINGS? 12
WHAT IF IT DOESN'T WORK? 12

SCANNING THE NETWORK 13

STARTING LOOK AT LAN 14
WHAT DO I DO IF I FOUND A NON PROTECTED PC ON A NETWORK 17

Disclaimer

This document is created to show you how to scan for public access points. This means points that are legal to use! Detecting Access points and bring them in map is legal. Accessing local networks from home users isn’t. However it is possible to use the same procedures on home networks you should keep in mind that it is not legal!

The scope of this document is to explain in easy words the what and about on war driving. You can see it as a regular manual for your microwave … if you warm your milk with it … no problem, if you use it to dry your dog … it is a problem so use the manual for what it is intended to!

This document may be freely distributed however I would love it if my name and website remain in the document !!!

I put the document on line in:
PDF
DOC
RTF

You can find them on HTTP://USERS.SKYNET.BE/MULTIBOX

However you must know that some actions are not allowed in some countries so please verify all this before you start using this document.

I just offer the information please don’t move anything to my side. I just write this manual to show you how some people get access to AP’s and please use this information in a rather positive way.

REQUIREMENTS:

This documents covers the PC Version only for the moment. For Pocket PC etc I can't help … the reason?

I DON'T HAVE A POCKET PC so any questions about that please.✍

What do I need in Hardware?

A Laptop.

To run al the applications, every laptop that is kind of capable of running Windows 2000 or XP is fine. Windows 98 should work to but it is kind of limited in network tools. Optimal machine has a 400 Mhz. Or above CPU and 128 MB ram.

A Wireless LAN card

It needs a Wireless LAN card or a wireless USB.
There exist PCMCIA cards in 11 MBIT from about 20 €/$ an USB 11 MBIT exists for about 30 €/$. The USB is sometimes fun because you can place it on your dash bord however a PCMCIA exists until 54 MBIT. Speed is the limit. I use an external USB Because I didn't have a PCMCIA free.

The ideal network card (NIC: Network Interface Cars) is a 54 mbit model with the possibility of an external antenna. However a non-expansive solution runs good enough.

!!! SELECT DHCP !!! in the TCPIP Protocol !!! of your network settings !!!

EXTRA: A GPS With connection cable

There are several GPS Devices possible. I Prefere the ones from Garmin http://www.garmin.com I have good experiances with the EMAP.

A GPS is not required only if you want to put the AP's (AP: ACCESS POINTS) on a mapsoftware like Microsoft Mappoint or Microsoft Autoroute Express. (Some others should do the same I'll investigate and give feedback in later versions of this manual)

EXTRA: A Car power supply is usefull

A laptop needs power… most of them run on 20 volts … a car only has 12. No problem. Or you buy a power inverter that makes 110 or 220 volts from your cigarette lighter or you buy at your laptop vender a power supply to run the laptop in the car. (Dell has it for example).

If you choose the first option a 70 watt does the job perfectly fine. In most cases it's les expansive to buy an inverter!

However if you put disks and screen in standby you will do like 4 or 5 houres with most modern laptops … But take care … you are addicted before you know ✍

EXTRA: Tweaked Antenna

Some adapters allow external antenna some other you can tweak. The tweaking of an antenna is not integrated in the scope of this document. Search google wireless tweaked antenna or some popular wardriver forums. Maybe I make a manual for antenna's later on … We'll see the succes of this document ✍

Software

What you need

PROGRAMNAME	*WHAT IS IT*	*WHERE DOWNLOAD*
NETSTUMBLER	AP Detection software FREEWARE	http://www.netstumbler.com
Look @ Lan	Network scanning and monitoring FREEWARE	http://www.lookatlan.com
WDRIVER	Wardriver Help tool FREEWARE	http://users.skynet.be/Multibox

Oh look … it's all freeware ✍ Remember always … software is like sex … it's better when it's free ✍

And for the dumbo's over here … to run this software you must have an OS installed I prefere Windows XP or 2000 due to it's good plug and play capabillities.

Everything Installed? You're ready … yes indeed that fast.

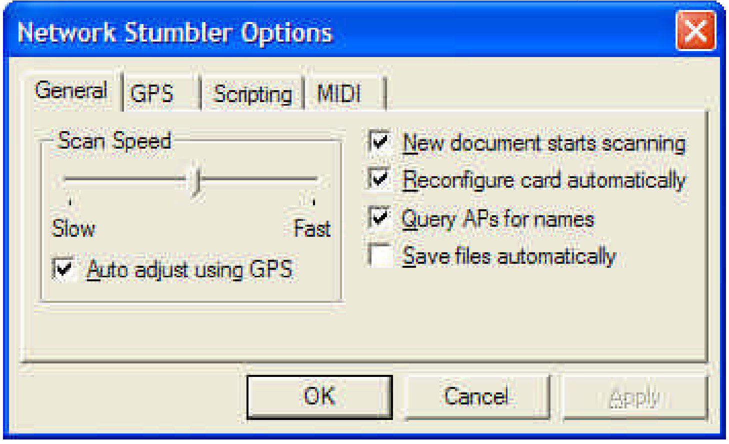
Driving around

Start you pc and run netstumbler… everything in this document is based on a started PC ✍

GPS Configuration

Select in the menu (upper of the application like FILE EDIT VIEW etc) the option EDIT Select there the OPTIONS

If you have a GPS Connected use these settings:



Scan Speed: Slow – Fast

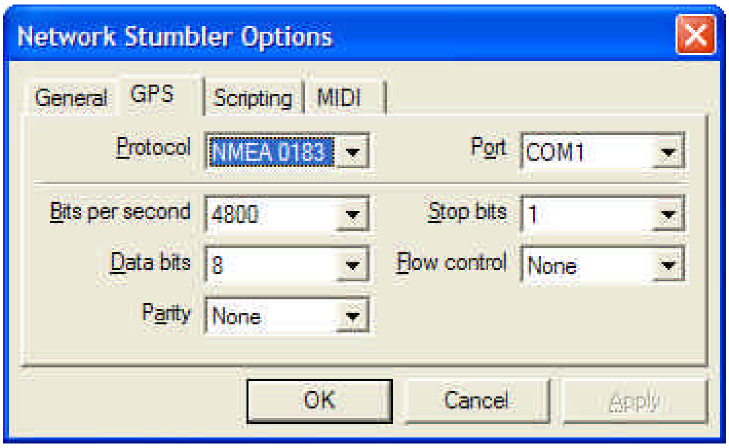
☑ Auto adjust using GPS

☑ New document starts scanning

☑ Reconfigure card automatically

☑ Query APs for names

☐ Save files automatically



Protocol: NMEA 0183

Port: COM1

Bits per second: 4800

Stop bits: 1

Data bits: 8

Flow control: None

Parity: None

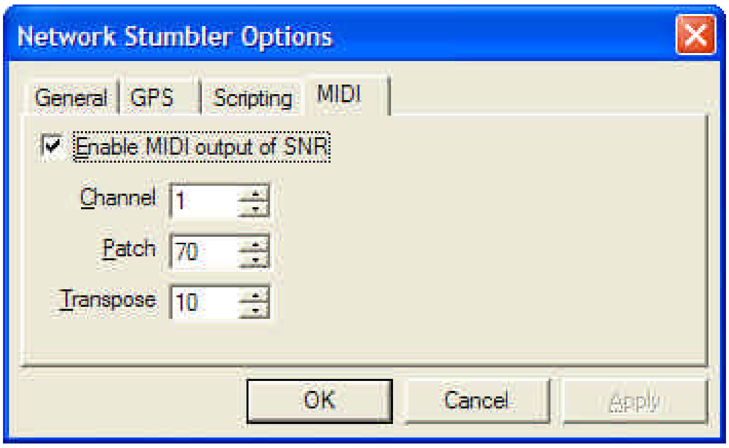
The port you choose the one the GPS receiver is attached. Setup your GPS Receiver to send in NMEA Format this is the standard.

Sound is better then view

Avoid watching the screen … it can cost your live so don't do it!
You can enable sound beeps. When you have low reception you have a low beep on high reception a high beep ✍

Select in the menu (upper of the application like FILE EDIT VIEW etc) the option EDIT
Select there the OPTIONS

Set these settings



☑ Enable MIDI output of SNR

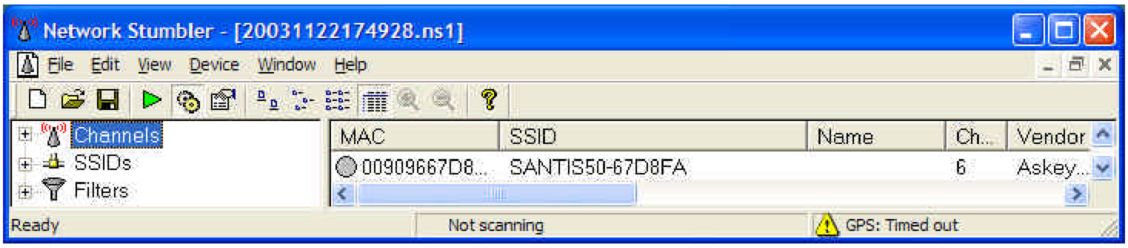
Channel 1

Patch 70

Transpose 10

I left the sound on standard you can change the instrument en stuff however ... I just want a beep ✍

Ready?


Network Stumbler - [20031122174928.ns1]
File Edit View Device Window Help
Channels
SSIDs
Filters

MAC	SSID	Name	Ch...	Vendor
00909667D8...	SANTIS50-67D8FA		6	Askey...

Ready | Not scanning | GPS: Timed out

Once everything works you will see downstairs in the STATUS BAR

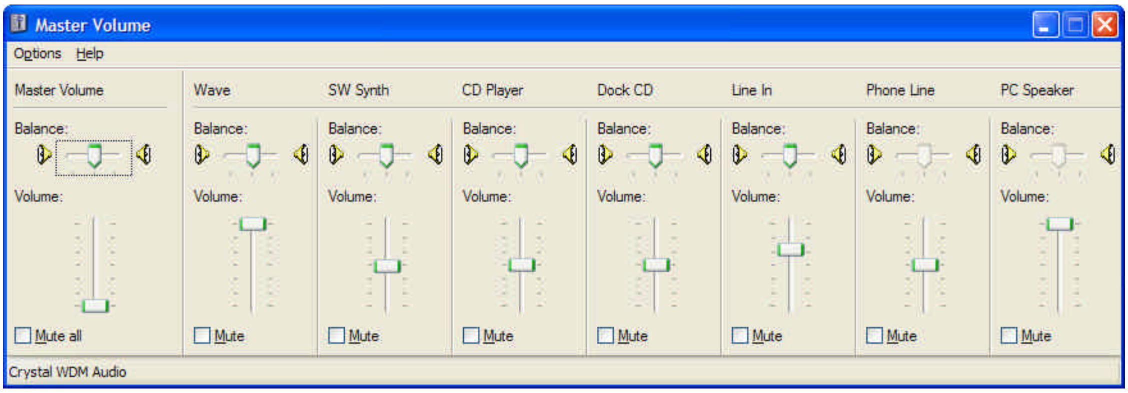
READY SCANNING GPS NO FIXED POINT OR POSITION

(My screenshot has no GPS and not scanning)

What now?

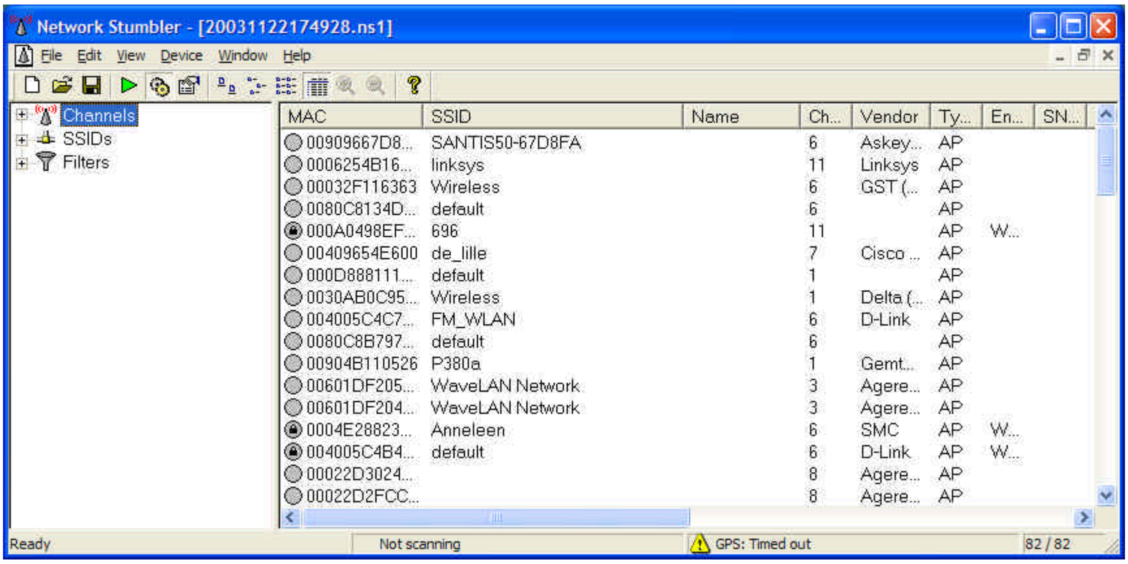
Start driving around … If you can't drive a car …
http://www.shopforthecar.co.uk/driving-lessons.php
HIHIHIHIHIHI

Ok so far the jokes … So you start driving around and you will notice beeps. Get used to the irritating sound however you can always put down the volume a bit of you synthesizer:



It is the master and the SW Synthesizer that make the sound louder or softer. TAKE CARE NOT THE WAVE ✍ Wave volume gives the sound if an AP is found.

Access point found



MAC	SSID	Name	Ch...	Vendor	Ty...	En...	SN...
○ 00909667D8...	SANTIS50-67D8FA		6	Askey...	AP		
○ 0006254B16...	linksys		11	Linksys	AP		
○ 00032F116363	Wireless		6	GST (...	AP		
○ 0080C8134D...	default		6		AP		
◉ 000A0498EF...	696		11		AP	W...	
○ 00409654E600	de_lille		7	Cisco ...	AP		
○ 000D888111...	default		1		AP		
○ 0030AB0C95...	Wireless		1	Delta (...	AP		
○ 004005C4C7...	FM_WLAN		6	D-Link	AP		
○ 0080C8B797...	default		6		AP		
○ 00904B110526	P380a		1	Gemt...	AP		
○ 00601DF205...	WaveLAN Network		3	Agere...	AP		
○ 00601DF204...	WaveLAN Network		3	Agere...	AP		
◉ 0004E28823...	Anneleen		6	SMC	AP	W...	
◉ 004005C4B4...	default		6	D-Link	AP	W...	
○ 00022D3024...			8	Agere...	AP		
○ 00022D2FCC...			8	Agere...	AP		

The AP’s that are available have a green bullet in front. Then you have two options:

Option One Protected AP

When in the small green bullet you see this LOCKER symbol well then it’s a protected AP. Most use WEP. If you see this you need a key to enter to this net. These are always commercial or private AP’s and never public. Hacking WEP or any security is illigal and not the scope of this document. If you have interests in this don’t ask me. I don’t know anything about cracking WEP and even if I knew I would never distribute it. (However I don’t have clue so …)

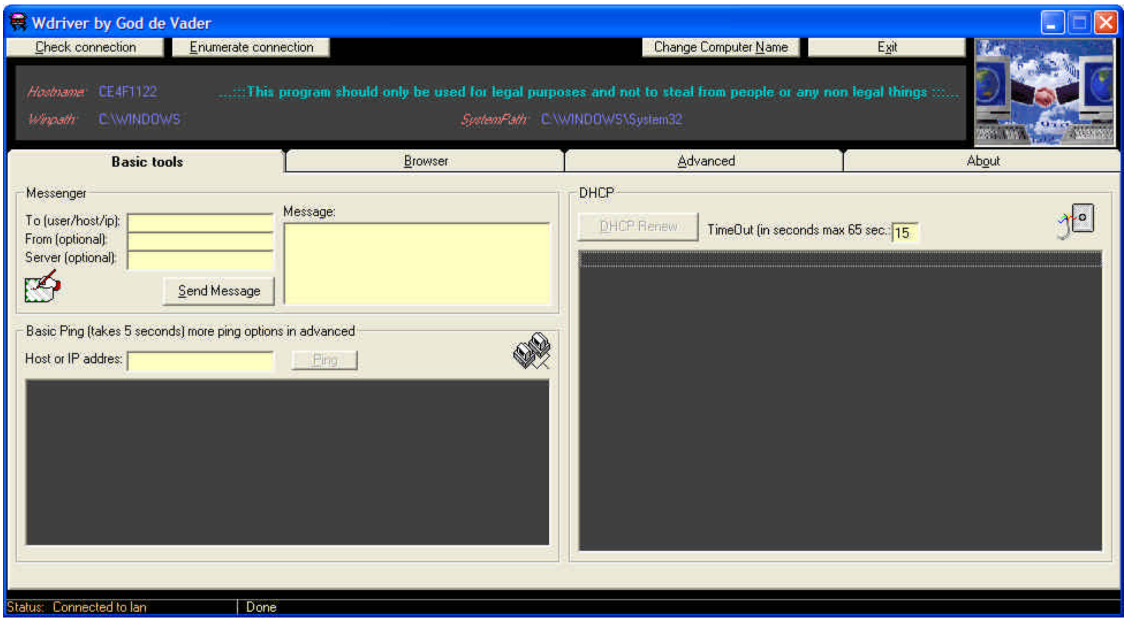
Option Two Open AP

If you have a blank green bullet … you are probably lucky ✍ big chance even.

Now park your car and keep the signal. (I didn’t find a manual on google on how to park a car however it’s not in the scope of this document)

Add your computer to the found wireless connection (via the connections in your start menu - > Wireless connection you will have a tab to add your pc to the wireless LAN!)

Start WDRIVER



Hostname: CE4F1122

Winpath: C:\WINDOWS

...:::This program should only be used for legal purposes and not to steal from people or any non legal things :::...

SystemPath: C:\WINDOWS\System32

TimeOut (in seconds max 65 sec.: 15

Status: Connected to lan | Done

Click the DHCP Renew Button

If everything is fine you should get after the timeout some information in the dark gray box under the DHCP Renew button. If you have received an IP Address you could start surfing … Normally it should work.

If you don’t get an DHCP IP Address…

Well then you can try forcing your Wireless adapter on a private IP range … Start using these settings

IP: 192.168.0.10
Subnet: 255.255.255.0
Gateway: 192.168.0.1
DNS1: 192.168.0.1

Why these settings?

Well the range of 192.168.x.x is the most common private IP range many people use it. By default most routers use the address 192.168.0.1 and they mostly do DNS forwarding so that’s the reason…

If this isn’t working you can try using these settings

IP: 10.0.0.10
Subnet: 255.0.0.0
Gateway: 10.0.0.1
DNS1: 10.0.0.1

This is another commonly used private IP range however subnet 255.0.0.0 is a huge range so for scanning it (as later shown in this manual)

What if it doesn’t work?

Just drive to the next access point … Some AP’s have MAC address protection enabled you can’t access them however everything looks fine you will not be able to connect to it!

Scanning the network

There is a way to scan the network to see other devices that are connected to the same LAN as where you are connected.

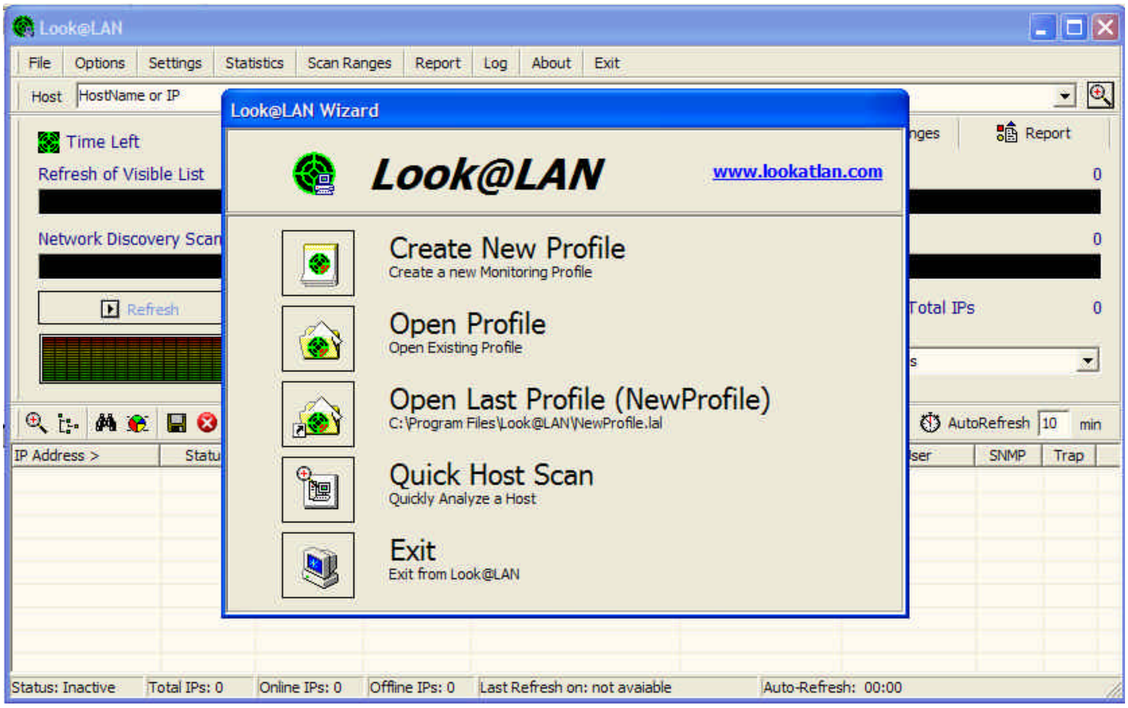
This is very interesting information and can be used to check out devices, PC's, servers etc. Don't use it to copy content from other people, don't use it to change configuration files, and don't use it for anything that's non-legal. If you copy things from other people it's equal to stealing. And yes there is a risk that they trace you because they know you MAC address (hardware address witch is fixed on every card) some people use a MAC spoofer or an exploit in windows to change the MAC address they sent out. The use of these kinds of tools is illigal however it makes it hard to trace you. But keep in mind that this is not the idea behind war driving. The idea is just driving and gathering information on networks not on personal stuff. If an AP is configured as DHCP without protection you can't know if it is a public AP or a non secured dumb user… so there you won't get troubles but hacking in to a network is not allowed.

The scanning is integrated in this document because it can give you global information on the network you are connected to like how many users are on line etc. It also allows you to gather SNMP (Simple Network Management Protocol) information. This allows you to see for example the uptime of the router, in and out traffic usage etc.

The program for scanning is LOOK @ LAN. The URL Can be found in chapter 1. Look at LAN is a freeware tool that listens to broadcast/multicast on the network and puts it in a GUI (list) once you have the list, you get a lot of options to gather information.

Starting Look at LAN

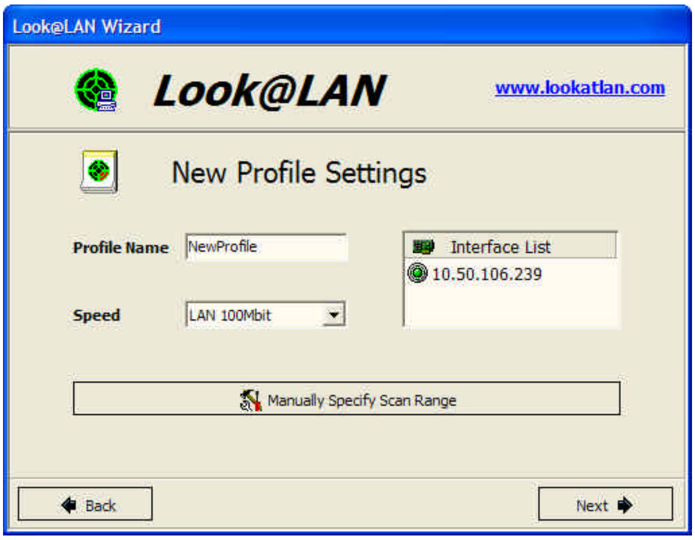
Make sure you are connected to a wireless network!



Status: Inactive | Total IPs: 0 | Online IPs: 0 | Offline IPs: 0 | Last Refresh on: not avaiable | Auto-Refresh: 00:00

This is the main view.

The wizard pops up you click the *Create New Profile* Button.



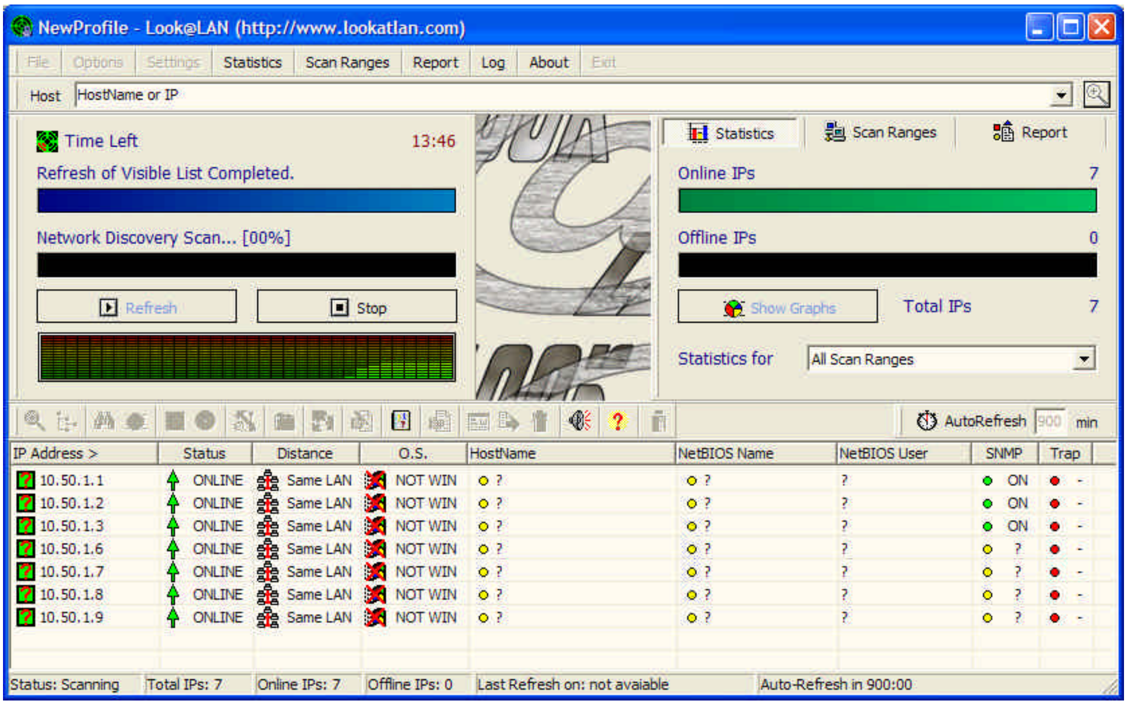
Profile Name: NewProfile

Speed: LAN 100Mbit

Interface List: 10.50.106.239

Now you see this next step in the wizard. On the right side you see the available interfaces. If you have more then one LAN card you maybe see multiple addresses. Make sure you pick the address of your wireless card (You get the IP address after you did the DHCP Renew in WDRIVER)

Then Click *NEXT*


NewProfile - Look@LAN (http://www.lookatlan.com)
File Options Settings Statistics Scan Ranges Report Log About Exit
Host
HostName or IP
Refresh
Stop
Statistics
Scan Ranges
Report
Show Graphs
AutoRefresh
900
min

Time Left 13:46

Refresh of Visible List Completed.

Network Discovery Scan... [00%]

Online IPs 7

Offline IPs 0

Total IPs 7

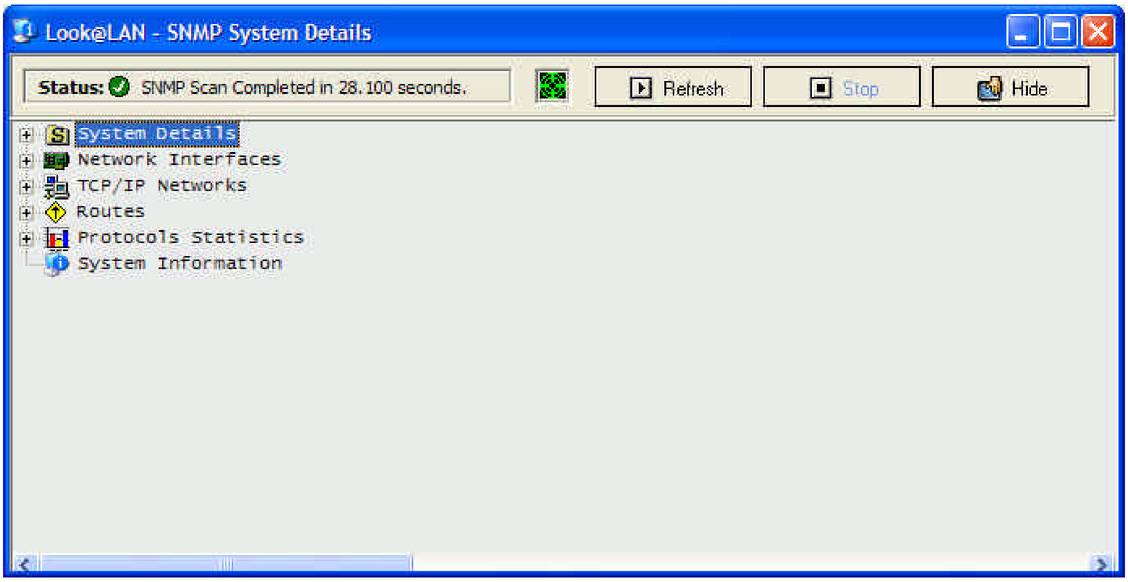
Statistics for All Scan Ranges

IP Address >	Status	Distance	O.S.	HostName	NetBIOS Name	NetBIOS User	SNMP	Trap
10.50.1.1	ONLINE	Same LAN	NOT WIN	○ ?	○ ?	?	● ON	● -
10.50.1.2	ONLINE	Same LAN	NOT WIN	○ ?	○ ?	?	● ON	● -
10.50.1.3	ONLINE	Same LAN	NOT WIN	○ ?	○ ?	?	● ON	● -
10.50.1.6	ONLINE	Same LAN	NOT WIN	○ ?	○ ?	?	○ ?	● -
10.50.1.7	ONLINE	Same LAN	NOT WIN	○ ?	○ ?	?	○ ?	● -
10.50.1.8	ONLINE	Same LAN	NOT WIN	○ ?	○ ?	?	○ ?	● -
10.50.1.9	ONLINE	Same LAN	NOT WIN	○ ?	○ ?	?	○ ?	● -

Status: Scanning | Total IPs: 7 | Online IPs: 7 | Offline IPs: 0 | Last Refresh on: not avaiable | Auto-Refresh in 900:00

Now it starts scanning. You will see in the left the remaining time…
Downstairs you get the list with other machines on your network.

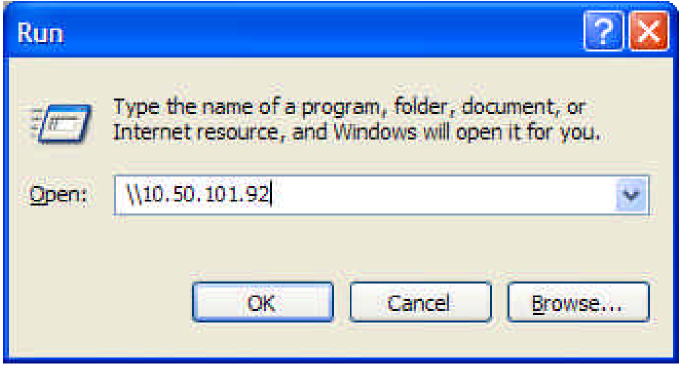
If the bullet SNMP is green you can double click it and get extra information on the device.



Status: SNMP Scan Completed in 28.100 seconds.

- System Details
- Network Interfaces
- TCP/IP Networks
- Routes
- Protocols Statistics
- System Information

If you find other (for example Windows PC's) you can just connect to them using you network explorer or \\<<server IP>> in your START RUN



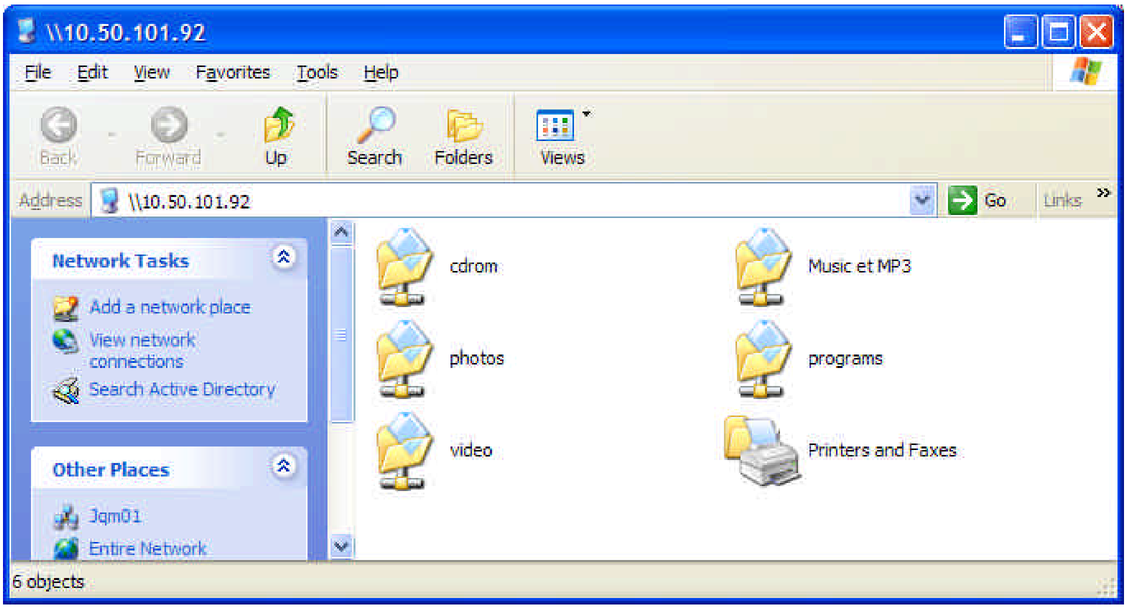
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: \\10.50.101.92

Once you clicked OK you should be able to connect to it. However copying anything from here on is not legal however most servers will ask a username and password so don't start playing, copying, deleting files or whatever.

THIS IS IN THE MANUAL SO YOU CAN TEST YOUR OWN LAN / WIFI ON SECURITY. TRY ALWAYS TO BREAK YOUR OWN SYSTEM SO YOU CAN LEARN HOW TO PROTECT IT !!!

Well I show you the results … of my run command



\\10.50.101.92

Address \\10.50.101.92

cdrom
Music et MP3
photos
programs
video
Printers and Faxes

6 objects

Well well well … you must keep in mind DON'T COPY !!!

What do I do if I found a non protected PC on a network

You can just shut up and leave it … but that doesn’t help the people too much isn’t it …

You can use WDRIVER to send a MESSENGER message

You can try to double click on the users printer if it is shared and print a small note on it. So when he is at his pc he will see it.

Don’t be to rough just tell the people that they may have a look at the security of their network.