



# Ethical Hacking and Countermeasures

Version 6

## Module XX

Hacking Wireless Networks

# Scenario

Clients of Xbrokerage Inc. are furious. None of them are able to logon to its portal. Xbrokerage had recently introduced this portal as an add-on service through which clients could track their shares and trade online.

Being a customer-friendly firm, Xbrokerage allowed wireless access within its office premises.

- Are wireless networks more prone to attacks?
- What could have been a vulnerable point?



## Wi-fi users, beware

*Hackers prowl public hot spots in order to steal your valuable data*

By Joseph De Avila

THE WALL STREET JOURNAL

Monday, February 4, 2008

Next time you are sitting in a hotel lobby checking e-mail on your laptop, be careful: The "businessman" in the next lounge chair may be tracking your every move.

Many Wi-Fi users don't know that hackers posted at hot spots can steal personal information out of the air relatively easily. And savvy criminal hackers aren't settling for just access to credit cards, bank accounts and other personal financial information; they love to sneak into your company's network, too.

Whether you're using a Wi-Fi hot spot at a hotel, airport or cafe, "you've got to assume that anything you are doing is being monitored," said Shawn Henry, the deputy assistant director of the FBI's cybercrimes division.

Home Wi-Fi networks are vulnerable, too, but it is far more fruitful for a hacker to pitch his tent in a busy hotel lobby or convention-center lounge where he can collect data from dozens of users. And Wi-Fi hot spots have proliferated, multiplying the potential targets for hackers. There were 66,921 hot spots in the United States last year, up 56 percent from 2006, according to JiWire Inc., an advertising company. T-Mobile USA Inc. has 8,700 hot spots across the nation in such places as Starbucks and Borders Books & Music. AT&T Inc. has 10,000 hot spots in such places as McDonald's, Barnes & Noble and Coffee Bean & Tea Leaf.

Henry said that businesses that offer Wi-Fi, such as hotels, often don't know that their networks have been breached and many times don't report incidents they know about for fear of bad publicity. Users are frequently unaware they have been hacked. As a result, there aren't solid figures on the number of wireless-hacking incidents. But the FBI for several years has received reports from educational institutions, private security companies, and other federal and local law-enforcement agencies about such attacks.

While the chances any one person will be hacked aren't high, the payoff for criminals can be great, said Tom Brennan, a manager for AccessIT Group, which assesses companies' security vulnerabilities.

In early 2006, when he was working for a different company, Brennan helped a financial institution determine how its data network had been breached. An employee working on a laptop in Midtown Manhattan's Bryant Park used what he thought was a publicly available Wi-Fi signal to get Internet access. But the signal he used had been set up by a hacker. When the employee reached his company's network, the hacker nabbed the employee's corporate user name and password.

Source: <http://www.journalnow.com/>

Copyright © by EC-Council

All Rights Reserved. Reproduction is Strictly Prohibited



TM

# Security News

[The Register](#) » [Security](#) » [Enterprise Security](#) »

Original URL: [http://www.theregister.co.uk/2007/10/18/cafe\\_latte\\_wi-fi\\_attack/](http://www.theregister.co.uk/2007/10/18/cafe_latte_wi-fi_attack/)

## Cafe Latte attack steals credentials from Wi-Fi clients

By [John Leyden](#)

Published Thursday 18th October 2007 18:40 GMT

Hackers have refined a new technique for breaking into Wi-Fi networks protected by the aging Wired Equivalent Privacy (WEP).

The so-called 'Cafe Latte' attack aims to retrieve the WEP keys from the PCs of road warriors. The approach concentrates its attack on wireless clients, as opposed to earlier attacks that cracked the key on wireless networks after sniffing a sufficient amount of traffic on a network.

"At its core, the attack uses various behavioral characteristics of the Windows wireless stack along with already known flaws in WEP," explains Vivek Ramachandran, a security researcher at AirTight Networks, who will [demonstrate](http://toorcon.org/2007/event.php?id=25) (<http://toorcon.org/2007/event.php?id=25>) the approach at the Toorcon hacking conference in San Diego this weekend (19-21 October). "Depending upon the network configuration of the authorised network we will show that it is possible to recover the WEP key from an isolated Client within a time slot ranging between just a few minutes to a couple of hours."

Source: <http://www.theregister.co.uk/>

Copyright © by **EC-Council**  
All Rights Reserved. Reproduction is Strictly Prohibited

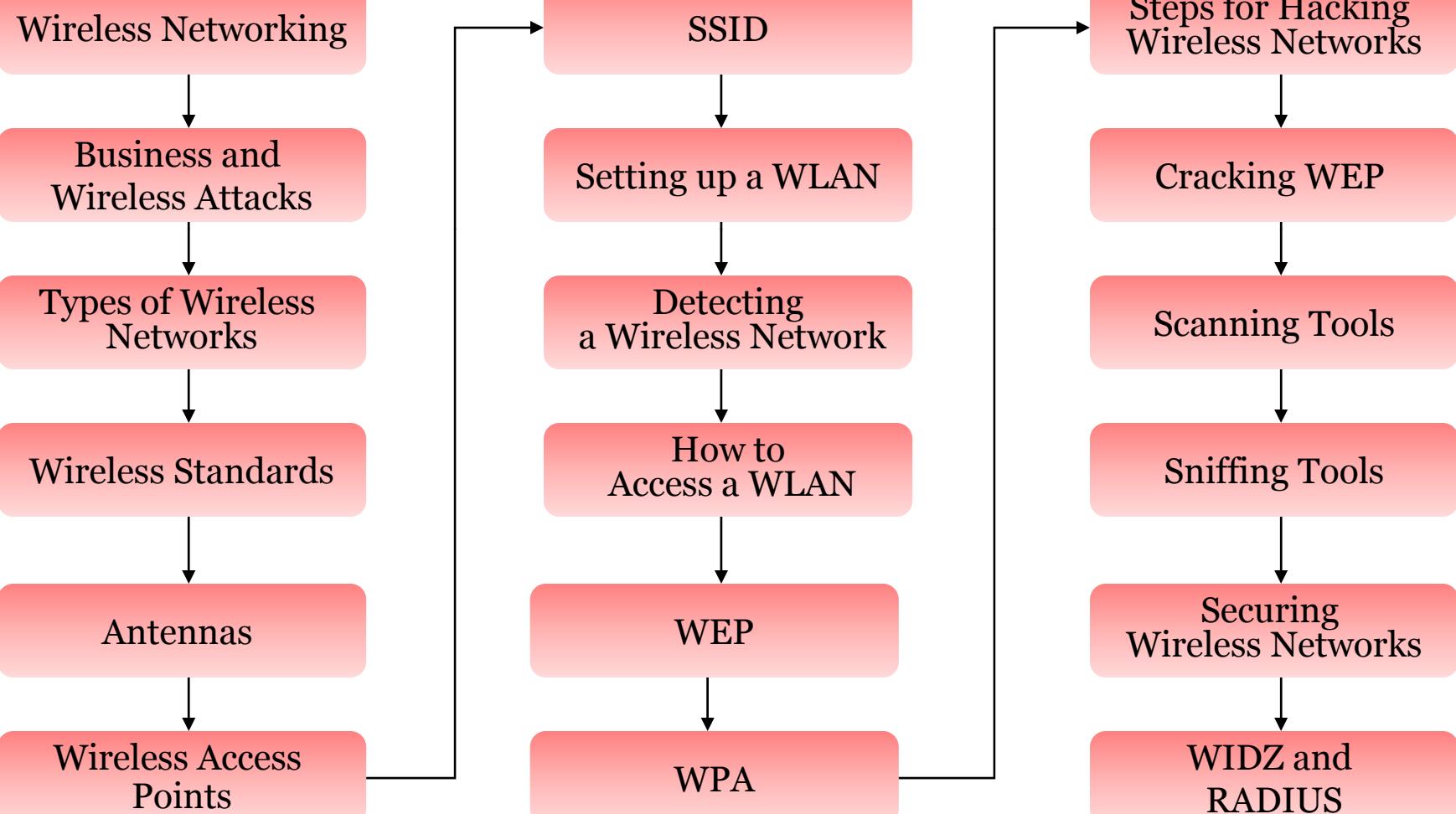


TM

# Module Objective

This module will familiarize you with :

- Concept of Wireless Networking
- Effects of Wireless Attacks on Business
- Types of Wireless Networks
- Wireless Standards
- Antennas
- Wireless Access Points
- SSID
- Setting up a WLAN
- Detecting a Wireless Network
- How to Access a WLAN
- Wired Equivalent Privacy
- Wi-Fi Protected Access
- Steps for Hacking Wireless Networks
- Cracking WEP
- Tools for Scanning
- Tools for Sniffing
- Securing Wireless Networks
- WIDZ and RADIUS





# Introduction to Wireless

# Introduction to Wireless Networking

Wireless networking technology is becoming increasingly popular and at the same time has introduced several security issues

The popularity of wireless technology is driven by two primary factors: convenience and cost

A Wireless Local Area Network (WLAN) allows workers to access digital resources without being locked to their desks

Laptops can be carried to meetings, or even to Starbucks, and connected to a wireless network. This convenience has become more affordable



# Wired Network vs. Wireless Network

Wired networks offer more and better security options than wireless

More thoroughly established standards with wired networks

Wireless networks are much more equipment-dependent than wired networks

It is easier to implement security policies on wired networks



# Effects of Wireless Attacks on Business

As more and more firms adopt wireless networks, security becomes more crucial

Business is at high risk from whackers (wireless hackers) who do not require physical entry into a business network to hack, but can easily compromise the network with the help of freely available tools

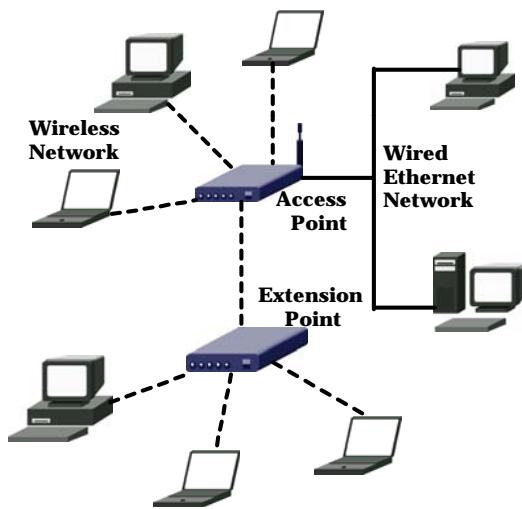
Warchalking, Wardriving, and Warflying are some of the ways in which a whacker can assess the vulnerability of a firm's network



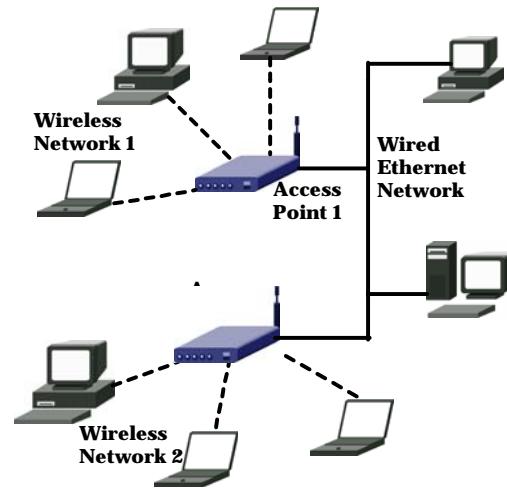
# Types of Wireless Network



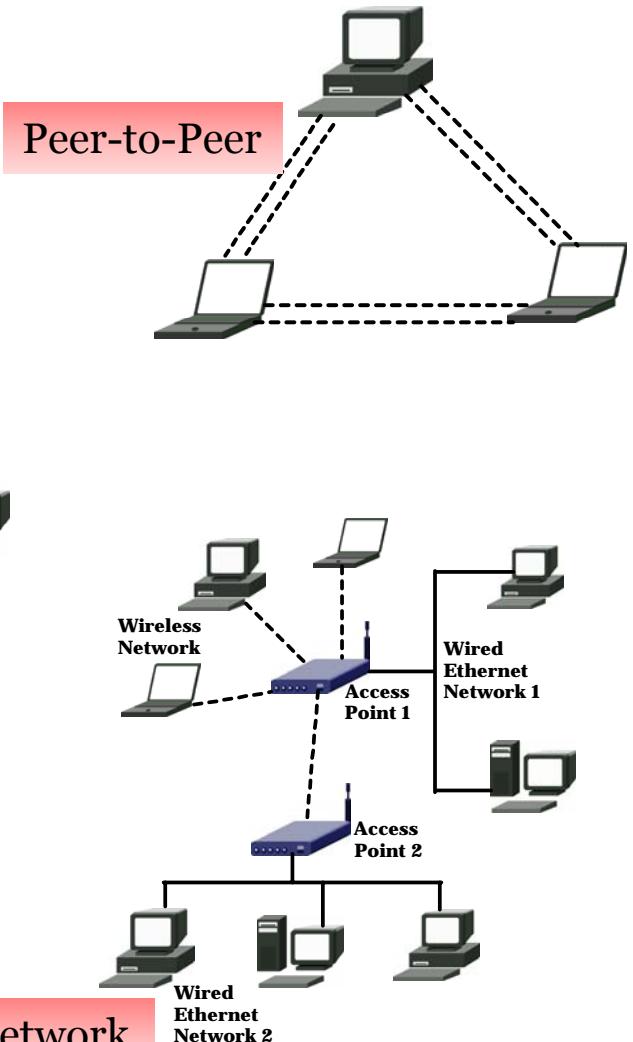
There are four basic types:



Extension to a wired network



Multiple access points



LAN-to-LAN wireless network

# Advantages and Disadvantages of a Wireless Network

## Advantages:

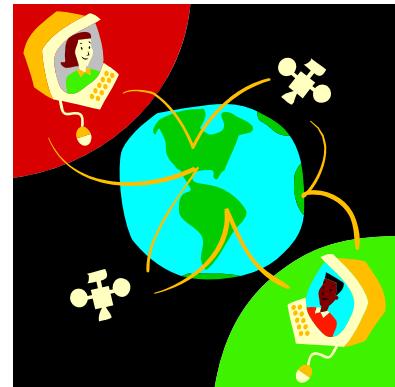
- Mobility (easy)
- Cost-effective in the initial phase
- Easy connection
- Different ways to transmit data
- Easy sharing



## Disadvantages:

- Mobility (insecure)
- High cost post-implementation
- No physical protection of networks
- Hacking has become more convenient
- Risk of data sharing is high





# Wireless Standards

# Wireless Standards



The first wireless standard was 802.11

It defines three physical layers:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)
- Infrared

802.11a: More channels, high speed, and less interference

802.11b: Protocol of Wi-Fi revolution, de facto standard

802.11g: Similar to 802.11b, only faster

802.11i: Improves WLAN security

802.16: Long distance wireless infrastructure

Bluetooth: Cable replacement option

900 MHz: Low speed, coverage, and backward compatibility





TM

# Wireless Standard: 802.11a

802.11a works at 40mhz in the 5g hz range

It's theoretical transfer rate is of up to 54 mpbs

It's actual transfer rates is of about 26.4 mbps

It is limited in use because it is almost a line of sight transmittal that necessitates multiple WAPs (wireless access points)

It cannot operate in same range as 802.11b/g

It is absorbed more easily than other wireless implementations

# Wireless Standard: 802.11b – “WiFi”

WiFi operates at 20 MHz in the 2.4 GHz range

It is the most widely used and accepted form of wireless networking

It has theoretical speeds of upto 11 mbps

Actual speeds depend on implementation:

- 5.9 mbps when TCP (Transmission Control Protocol) is used (error checking)
- 7.1 mbps when UDP (User Datagram Protocol) is used (no error checking)



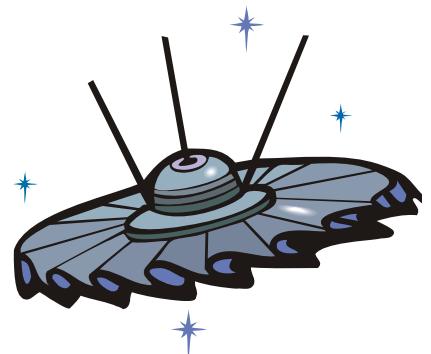
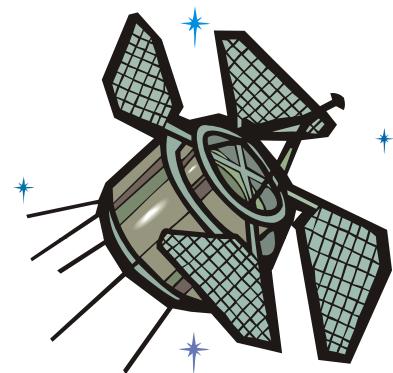
It can transmit upto 8 kms in the city

# Wireless Standard: 802.11b – “WiFi” (cont'd)

802.11b – “WiFi” is not as easily absorbed as 802.11a signal

It can cause or receive interference from:

- Microwave ovens (microwaves in general)
- Wireless telephones
- Other wireless appliances operating in the same frequency



# Wireless Standard: 802.11g

802.11g operates at the same frequency range as 802.11b

It has theoretical throughput of 54 Mpbs

Actual transmission rate is dependent on several factors, but averages 24.7 mbps

Logical upgrade from 802.11b wireless networks – backwards compatibility

It suffers from same limitations as 802.11b network

System may suffer significant decrease in network speeds if network is not completely upgraded from 802.11b



# Wireless Standard: 802.11i

802.11i is a standard for wireless local area networks that provides improved encryption for networks that use the popular 802.11a, 802.11b & 802.11g standards

The 802.11i standard was officially ratified by the IEEE in June, 2004

Security is made up of three factors:

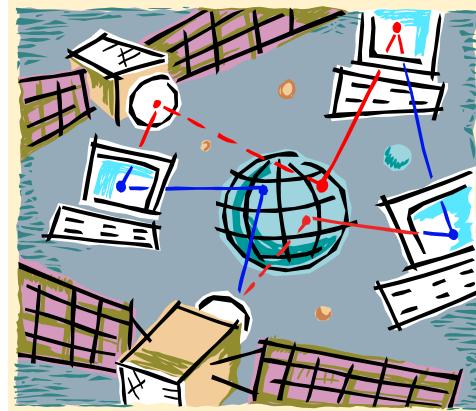
- 802.1x for Authentication (EAP and Authentication Server)
- Robust Security Network (RSN) to keep track of associations
- Counter-Mode/CBC-Mac Protocol (CCMP) to provide confidentiality, integrity, and origin authentication



# Wireless Standard: 802.11n

The 802.11n standard, which will be based on multiple-in/multiple out (MIMO) technology, is expected to boost throughput to potentially well over 100 Mbps





# Wireless Concepts and Devices



# Related Technology and Carrier Networks

CDPD: Cellular Digital Packet Data (TDMA)

1xRTT on CDMA (Code Division Multiple Access): Mobile phone carrier networks

GPRS: General Packet Radio Service on GSM (Global System for Mobile Communications)

FRS (Family Radio Service) and GMRS (General Mobile Radio Service): Radio services

HPNA (Home Phone Networking Alliance) and Powerline Ethernet: Non-traditional networking protocols

802.1x: Port security for network communications

BSS (Basic Service Set): Access point ~ bridges wired and wireless network

IBSS (Independent Basic Service Set): Peer-to-peer or ad-hoc operation mode

# Antennas

Antennas are important for sending and receiving radio waves

They convert electrical impulses into radio waves and vice versa

There are two types of antennas:

- Omni-directional antennas
- Directional antennas

Can antennas are also popular in the wireless community and are used mostly for personal use



# CEH Cantenna



**What is a Cantenna?**

If you've never heard of a Cantenna, don't worry your not alone. A Cantenna is simply an inexpensive version of the long range antennas used by wireless internet providers and mobile phone companies. It is ideally suited for sending or receiving wireless signals in the 2.4 GHz ISM band (802.11b). Now, with your own Cantenna you can extend the range of your wireless network or connect to other wireless networks in your neighborhood.

**FEATURES:**

**The Can**  
Our engineers have optimized can length and diameter for maximum signal strength and distance. Made from light-weight metal.

**Connector (n-female)**  
Connect to your Super Cantenna with industry standard cables and connectors.

**Mounting Socket**  
Cantenna is designed with a socket for easy mounting on camera tripods and other mounting hardware.

Includes instructions and red plastic protection lid.

**BUY IT NOW!**



Above, a side-by-side photograph of the Super Cantenna and Pringles can is shown.



Increase the range of your wireless connection with the Super Cantenna. All Cantenna parts are engineered to be compatible with 802.11b Wireless Networks.

# Wireless Access Points



An access point is a piece of wireless communications hardware that creates a central point of wireless connectivity



Similar to a “hub,” the access point is a common connection point for devices in a wireless network



Wireless access points must be deployed and managed in common areas of the campus, and they must be coordinated with telecommunications and network managers

# SSID

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity

An SSID acts as a single shared identifier between access points and clients

Security concerns arise when the default values are not changed, as these units can be easily compromised

A non-secure access mode allows clients to connect to the access point using the configured SSID, a blank SSID, or an SSID configured as “any”



Beacon frames broadcast the SSID:

- Helps users to locate available networks
- Layer 2 management frames
- Networks without BFs are called “closed networks”:
  - Simply means that the SSID is not broadcast anymore
  - Weak attempt at security through obscurity, to make the presence of the network less obvious
  - BSSIDs are revealed as soon as a single frame is sent by any member station
  - Mapping between SSIDs and BSSIDs is revealed by several management frames that are not encrypted



# Is the SSID a Secret

Stations looking for an access point send the SSID they are looking for in a "probe request"

Access points answer with a "probe reply" frame, which contains the SSID and BSSID pair

Stations wanting to become part of a BSS send an association request frame, which also contains the SSID/BSSID pair in cleartext:

- As do reassociation requests (see next slides) and their response

Therefore, the SSID remains secret only on closed networks with no activity

Closed networks are mainly inconvenient to legitimate users



# Setting up a WLAN

The channel and service set identifier (SSID) must be configured when setting up a WLAN in addition to traditional network settings such as IP address and a subnet mask

The channel is a number between 1 and 11 (between 1 and 13 in Europe) and it designates the frequency on which the network will operate

The SSID is an alphanumeric string that differentiates networks operating on the same channel

It is essentially a configurable name that identifies an individual network. These settings are important factors when identifying WLANs and sniffing traffic



# Authentication and Association

To become part of a BSS, a station must first authenticate itself to the network:

- Then, it will request association to a specific access point



The access point is in charge of authentication and is accepting the association of the station:

- Unless an add-on authentication system (e.g., Radius) is used



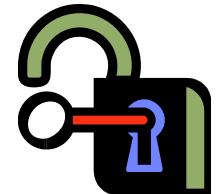
MAC address is trusted as giving the correct identity of the station or access point:

- How can this be abused?

# Authentication Modes

Authentication is done by:

- A station providing the correct SSID
- Or, through “the shared key authentication:
  - Access point and all base stations share a secret encryption key which is:
    - Difficult to deploy
    - Difficult to change
    - Difficult to keep secret
    - No accountability
  - A station encrypting with **WEP**; a challenge text provided by the access point
  - An eavesdropper gaining both the plaintext and the ciphertext by:
    - Performing a known plaintext attack
    - This authentication which helps to crack WEP encryption





# The 802.1X Authentication Process

For 802.1X authentication to work on a wireless network, AP must be able to securely identify traffic from a particular wireless client

This identification is accomplished by using authentication keys that are sent to the AP and the wireless client from the RADIUS server

When a wireless client (802.1X supplicant) comes within the range of the AP (802.1X authenticator), the simplified process as given in the next slide occurs:

# The 802.1X Authentication Process (cont'd)

- 1 • The AP point issues a challenge to the wireless client
- 2 • The wireless client responds with its identity
- 3 • The AP forwards the identity to the RADIUS server using the uncontrolled port
- 4 • The RADIUS server sends a request to the wireless station via the AP specifying the authentication mechanism to be used
- 5 • The wireless station responds to the RADIUS server with its credentials via the AP
- 6 • The RADIUS server sends an encrypted authentication key to the AP if the credentials are acceptable
- 7 • The AP generates a multicast/global authentication key encrypted with a per-station unicast session key, and transmits it to the wireless station



## WEP and WPA

# Wired Equivalent Privacy (WEP)

WEP is a component of the IEEE 802.11 WLAN standards

Its primary purpose is to provide confidentiality of the data on wireless networks at a level equivalent to wired LANs

Wired LANs typically employ physical controls to prevent unauthorized users from connecting to the network and viewing data

In a wireless LAN, the network can be accessed without physically connecting to the LAN

IEEE chose to employ encryption at the data link layer to prevent unauthorized eavesdropping on a network

- This is accomplished by encrypting data with the RC4 encryption algorithm



# Wired Equivalent Privacy (cont'd)

Cryptographic mechanism is used to defend against threats

It is developed without :

- Academic or public review
- Review from cryptologists



It has significant vulnerabilities and design flaws

Only about a quarter to a third of wireless access points use WEP:

- Tam et al. 2002
- Hamilton 2002
- Pickard and Cracknell 2001, 2003



TM

# Wired Equivalent Privacy (cont'd)

WEP is a stream cipher:

- It uses RC-4 to produce a stream of bytes that are XORed with the plaintext
- The input to the stream cipher algorithm is an "initial value" (IV) sent in plaintext and a secret key
- IV is 24 bits long
- Length of the secret is either 40 or 104 bits, for a total length for the IV and secret of 64 or 128 bits
- Marketing publicized the larger number, implying that the secret was a 64 or 128 bit number, in a classical case of deceptive advertising:
  - How else can you call a protection that is 16.8 million times weaker than advertised?

# WEP Issues

CRC32 is not sufficient to ensure complete cryptographic integrity of a packet

- By capturing two packets, an attacker can reliably flip a bit in the encrypted stream, and modify the checksum so that the packet is accepted

IV's are 24 bits

- An AP broadcasting 1500 byte packets at 11 Mb/s would exhaust the entire IV Space in five hours



Known Plaintext Attacks

- When there is IV Collision, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet

## Dictionary Attacks

- WEP is based on a password

## Denial of Services

- Associate and Disassociate messages are not authenticated

Eventually, an attacker can construct a decryption table of reconstructed key streams

- With about 24 GB of space, an attacker can use this table to decrypt WEP Packets in real-time





TM

# WEP Issues (cont'd)

A lack of centralized key management makes it difficult to change WEP keys with any regularity

IV is a value that is used to randomize the key stream value and each packet has IV value

- The standard only allows 24 bits, which can be used within hours at a busy AP
- IV values will be reused

The standard does not dictate that each packet must have a unique IV, so vendors use only a small part of the available 24-bit possibilities

- A mechanism that depends on randomness is not random at all and attackers can easily figure out the key stream and decrypt other messages



TM

# WEP - Authentication Phase

When a wireless station wants to access a network, it sends a probe request packet on all channels so that any AP in range will respond

The AP responds with packets containing the AP's SSID and other network information

- When open system authentication (OSA) is configured, the station will send an authentication request to the AP and the AP will make an access decision based on its policy
- When shared key authentication (SKA) is configured, the AP will send a challenge to the station and the station encrypts it with its WEP key and sends it back to the AP
  - If the AP obtains the challenge value, the station is authorized

The Requesting Station sends the challenge text

The Receiving Station:

- Decrypts the challenge using the same shared key
- Compares it to the challenge text sent earlier
- If they match, an acknowledgement is sent
- If they do not match, a negative authentication notice is sent

Once acknowledged, the transmission is sent



Requesting Station

Receiving Station



TM

# WEP - Association Phase

After the authentication phase, the station will send an association request packet to the AP

If the AP has a policy to allow this station to access the network, it will associate the station to itself by placing the station in its association table

A wireless device has to be associated with an AP to access network resources, and not just authenticated

The authentication and association phases authorize the device, and not the user

There is no way to know if an unauthorized user has stolen and is using an authorized device



TM

# WEP Flaws

Two basic flaws undermine its ability to protect against a serious attack:

No defined method for encryption key distribution

- Pre-shared keys were set once at installation and are rarely (if ever) changed

Use of RC4 which was designed to be a one-time cipher and not intended for multiple message use

- As the pre-shared key is rarely changed, the same key is used over and over
- An attacker monitors traffic and finds enough examples to work out the plaintext from message context and with knowledge of the ciphertext and plaintext, he/she can compute the key

# What is WPA

WPA is not an official IEEE standard, but will be compatible with the upcoming 802.11i security standard

It (Wi-Fi Protected Access) is a data encryption method for 802.11 WLANs

It resolves the issue of weak WEP headers, which are called initialization vectors (IVs)

It is designed to be a software upgrade

With WPA, the rekeying of global encryption keys is required



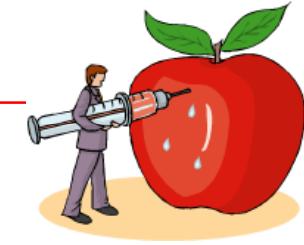
## Wi-Fi Protected Access:



- Stop-gap solution that solves issues related to the WEP encryption itself:
  - IVs are larger (48 bits instead of 24)
  - Shared key is used more rarely:
    - Used to negotiate and communicate "temporal keys"
    - "Temporal keys" are used to encrypt packets instead
  - Does not solve issues with the management frames
  - Collision avoidance mechanism can still be exploited
  - Can be supported by most of the 802.11b hardware

### Denial-of-service attack:

- Attacker injects or corrupts packets
- IV and message hash are checked before MIC to reduce the number of false positives
- Only way around this is to use WEP



### Pre-shared key dictionary attack:

- Weak passphrase is used to generate pre-shared key
- Comprises of 14 characters or less that form words
- More than 14 characters that do not form words are almost impossible to crack



# WEP, WPA, and WPA2



WEP is weak and fails to meet any of its goals



WPA fixes most of WEP's problems, but adds some new vulnerabilities



WPA2 is expected to make wireless networks as secure as wired networks

# WPA2 Wi-Fi Protected Access 2

WPA2 is compatible with the 802.11i standard

It provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm

It offers two modes of operation:

- Enterprise: Verifies network users through a server
- Personal: Protects unauthorized network access by utilizing a set-up password



## Features:

- WPA2 authentication
- WPA2 key management
- Temporal Key management
- Michael Algorithm
- AES support
- Supporting a mixture of WPA and WEP wireless clients





# Attacks and Hacking Tools

# Terminologies

**WarWalking** – Walking around to look for open wireless networks



**Wardriving** – Driving around to look for open wireless networks

**WarFlying** – Flying around to look for open wireless networks

**WarChalking** – Using chalk to identify available open networks

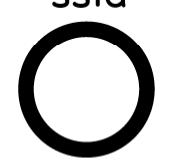


**Blue jacking** – Temporarily hijacking another person's cell phone using Bluetooth technology

**Global Positioning System (GPS)** – It can be used to help map the open networks that are found

# WarChalking

let's warchalk..!

KEY	SYMBOL
OPEN NODE	ssid  bandwidth
CLOSED NODE	ssid 
WEP NODE	ssid      access contact  bandwidth

[blackbeltjones.com/warchalking](http://blackbeltjones.com/warchalking)

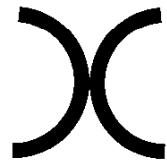


[www.warchalking.org](http://www.warchalking.org)



# WarChalking

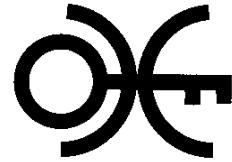
## Proposed New Signs



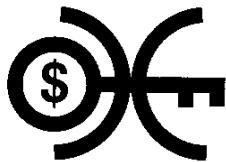
Unrestricted access



AP with MAC filtering



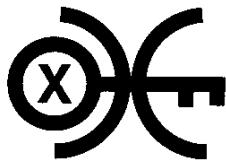
Open access with restrictions



Pay for access AP



AP with WEP

AP with multiple access controls  
(not for public use)

AP with closed ESSID



Honeypot

# WarChalking



# WarChalking



# Authentication and (Dis)Association Attacks

Any station can impersonate another station or access point and attack or interfere with the authentication and association mechanisms:

- As these frames are not encrypted, the difficulty is trivial

Disassociation and deauthentication frames:

- A station receiving one of those frames must redo the authentication and association processes
- With a single short frame, an attacker can delay the transmission of data and require the station and real access point to redo these processes:
  - This takes several frames to perform



# WEP Attack

WEP attack takes at least 10,000 packets to discover the key

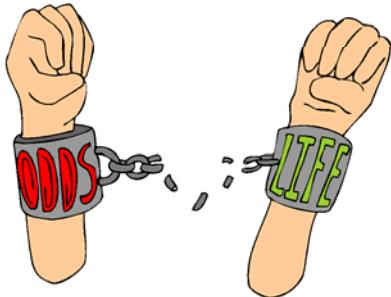
- A large amount of known data is the fastest way of determining as many key streams as possible

Wep Weggie (part of BSD-Airtools) can be used to generate a large number of small packets:

- The information may be as innocuous as the fields in the protocol header or the DNS name query
- Monitoring is passive and therefore undetectable
- Simple tools and instructions are readily available to recover the key



# Cracking WEP



## Passive attacks:

- The presence of the attacker does not change traffic, until WEP has been cracked



## Active attacks:

- Active attacks increase the risk of being detected, but are more capable
- If an active attack is reasonable (i.e., the risk of detection is disregarded), the goal is to stimulate traffic:
  - Collects more pads and uses of weak IVs
  - Some attacks require only one pad

# Weak Keys (a.k.a. Weak IVs)

Some IVs can reveal information about the secret key depending upon how RC4 is used in WEP:

- Mathematical details out of the scope of this material

## Attack

- FMS (Fluhrer et al. 2001) cryptographic attack on WEP
- Practicality demonstrated by Stubblefield et al. (2001)
- Collection of the first encrypted octet of several million packets
- Exploits:
  - WEPcrack (Rager 2001)
  - Airsnort (Bruestle et al. 2001)
- Key can be recovered within a second (after collecting the data)



# Problems with WEP's Key Stream and Reuse

Secret key never changes, only the initialization vectors



Initialization vectors are sent unencrypted

If two messages with the same initialization vector are intercepted it is possible to obtain the plaintext

Initialization vectors are commonly reused

Initialization vectors can be used up in less than 1 hour

Attackers can inject a known plaintext and re-capture the ciphertext

It leaves WEP susceptible to replay attacks

# Automated WEP Crackers

## AiroPeek (Commercial)

- Easy-to-use, flexible, and sophisticated analyzer

## WEPCrack, AirSnort

- Implementations of the FMA attack

## NetStumbler

- This is a popular network discovery tool, with GPS support. It does not perform any cracking. A Mac OS equivalent is named "iStumbler"

## KisMAC

- This is a Mac OS X tool for network discovery and cracking WEP with several different methods

## Kismet

- Swiss-army knife



# Pad-Collection Attacks



There is (should be) a different pad for every encrypted packet that is sent between an AP and a station

By mapping pads to IVs, you can build up a table and skip the RC4 step:

- The stream is never longer than 1500 bytes (the maximum Ethernet frame size)
- The 24 bit-IV provides  $16,777,216$  ( $256^3$ ) possible streams, so all the pads can fit inside  $25,165,824,000$  bytes (23.4 GB)

You never have to have the WEP key:

- Once you have a complete table, it is as good as having the WEP key

# XOR Encryption

0 XOR 0 = 0

1 XOR 0 = 1

1 XOR 1 = 0

(z XOR y) XOR z = y

(z XOR y) XOR y = z

Works independently when z or y is the "plaintext," "pad," or "ciphertext"

1101 Plaintext  
XOR 1001 Keystream

0100 Ciphertext



# Stream Cipher

Given an IV and secret key, the stream of bytes (pad) produced is always the same:

- Pad XOR plaintext = ciphertext

If an IV is ever reused, then the pad is the same



Knowing all pads is equivalent to knowing the secret

## Application to WEP:

- The pad is generated from the combination between the IV and the WEP key passed through RC4
- Knowing all pads is equivalent to knowing the 40 or 104-bit secret:
  - "Weak" IVs reveal additional information about the secret

# WEP Tool: Aircrack

Aircrack is a 802.11 sniffer and WEP key cracker

It recovers 40-bit or 104-bit WEP key

It implements FMS attack with some new attacks

It supports Windows, Linux, and Mac OS



```
aircrack 2.1
aircrack 2.1 - (C) 2004 Christophe Devine

usage: aircrack <pcap filename(s)>

5 : debug - specify beginning of the key
4 : bruteforce fudge factor (current: 2)
3 : packet MAC filter: 00:00:00:00:00
2 : WEP key length in bits, current: 128
1 : read IVs from a specified pcap file
0 : start cracking (with 0 WEP IVs)

-> 1

<note: you can drag'n drop pcap files over aircrack.exe>
filename: as21.cap

Opening pcap file as21.cap
Choosing first WEP-encrypted BSSID = 00:0C:41:AB:18:B7
Reading packets: total = 287690, usable = 136987
```

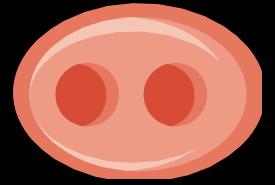
Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program which recovers keys when the data packets are captured

## The features of Aircrack-ng are:

- Better documentation(wiki, manpages) and support
- More cards/drivers supported
- More OS and platforms supported
- WEP dictionary attack
- Improved cracking speed
- Optimizations, other improvements, and bug fixing



# WEP Tool: AirSnort



AirSnort is a wireless LAN (WLAN) tool that recovers encryption keys on 802.11b WEP networks

It operates by passively monitoring transmissions and computing the encryption key when enough packets have been gathered

It runs under Linux, and requires that the wireless NIC be capable of rf monitor mode, and that it passes monitor mode packets up via the PF\_PACKET interface



Source: <http://airsnort.shmoo.com/>



TM

# AirSnort: Screenshot 1

The image displays two windows of the AirSnort software, version 1.2.1, running on different operating systems.

**Top Window (Windows XP):**

- Scan Settings:** Scan mode selected, Network device set to \\Device\\(552C5A49-62D3-4, Driver type set to DWL-650.
- Crack Breadth:** 40 bit crack breadth is set to 3, and 128 bit crack breadth is set to 2.
- Network Devices:** A list of nearby wireless access points (BSSIDs) is shown:

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	Unique	PW: Hex	PW: ASCII
	00:A0:B0: [REDACTED]		Y	Sun Nov 13 7B:14:82		1	493	135	0	135		
	FF:FF:FF			Sun Nov 13 00:00:00			6	0	0	0		
	00:07:40: [REDACTED]			Sun Nov 13 00:00:00			4	0	0	0		
	00:0F:66: [REDACTED]		Y	Sun Nov 13 00:00:00		6	6	0	0	0		

**Bottom Window (Ubuntu):**

- Scan Settings:** Scan mode selected, Network device set to ath1, Driver type set to Host AP/Orinoco.
- Crack Breadth:** 40 bit crack breadth is set to 3, and 128 bit crack breadth is set to 2.
- Network Devices:** A list of nearby wireless access points (BSSIDs) is shown:

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	Encrypted	Interesting	Unique	PW: Hex	PW: ASCII
	00:03:2F:suse	suse	Y	Sun Aug 13 20:20:9E	1	1	14144	13839	0	11238		
	FF:FF:FF			Sun Aug 13 00:00:00			1	0	0	0		

**Buttons at the bottom of the bottom window:**

- Start
- Stop
- Clear



TM

# AirSnort: Screenshot 2

The screenshot shows the AirSnort interface running on a Windows operating system. The main window displays a list of wireless networks (BSSIDs) with their names, card types, and various statistics. A secondary window, titled 'Terminal', shows a command-line session with several commands entered.

**Main Window (AirSnort):**

C	BSSID	Name	WEP	Last Seen	Last IV	Chan	Packets	crypt	resti	PW: Hex	PW: ASCII
00:06:25:7F:90:55	linksys			00:00:00	1	50	0	0	0		
00:02:2D:8D:1F:DE	Verizon Wi-Fi			00:00:00	1	77	0	0	0		
FF:FF:FF:FF:FF:FF				00:00:00	1	222	0	0	0		
00:02:2D:8D:1E:50	Verizon Wi-Fi			00:00:00	4	104	0	0	0		
00:90:4B:21:43:68	SurfandSip			00:00:00	11	3	0	0	0		
00:03:93:EB:F6:61	Apple Network abf661			00:00:00	10	5	0	0	0		
00:06:C6:B0:0B:62	loki	Y		00:00:00	11	2	0	0	0		
00:09:5B:47:B7:24	Wireless	Y		00:00:00	11	1	0	0	0		
00:02:2D:8A:14:69	Verizon Wi-Fi			00:00:00	1	18	0	0	0		
00:06:25:7B:86:D7	linksys1	Y		00:00:00	1	2	0	0	0		
00:50:F2:7A:FB:98	MSHOME			00:00:00	6	3	0	0	0		
00:07:85:B4:10:9D	tsunami	Y		00:00:00	6	19	0	0	0		
00:06:25:8D:EC:63	linksys			00:00:00	6	2	0	0	0		
00:06:25:8D:BE:6F	faithexchange	Y		AA:AA:03	10	11	3	0	0		
00:04:5A:2F:DA:A3		Y		00:00:00	9	7	0	0	0		
00:30:F1:10:1C:02	FAITHEXCHANGE			00:00:00	2	12	0	0	0		
00:40:05:C8:19:60	default			00:00:00	6	2	0	0	0		
00:0C:CE:1D:13:14	tsunami	Y		00:00:00	6	2	0	0	0		
00:05:5D:25:64:46	default			00:00:00	6	10	0	0	0		
00:00:08:AD:00:F8	default	Y		00:00:00	6	2	0	0	0		
00:50:18:0C:D4:A2	www.valmandel.com	Y		00:00:00	10	6	0	0	0		
00:06:25:B6:50:F5		Y		EB:80:DF	10	1	1	0	0		
00:40:05:BE:8D:08				00:00:00	6	6	0	0	0		
00:40:96:58:AF:7D	qbeairlan			00:00:00	6	34	0	0	0		
52:66:14:8A:D6:97	hp			00:00:00	6	4	0	0	0		
00:40:96:56:62:51	qbeairlan			00:00:00	6	24	0	0	0		
00:40:96:56:39:72	qbeairlan			00:00:00	6	75	0	0	0		
00:09:5B:40:66:27	WASOSLTDNY			00:00:00	6	3	0	0	0		
00:40:96:56:59:08	qbeairlan			00:00:00	6	38	0	0	0		
00:40:05:DE:60:EA	default			00:00:00	6	1	0	0	0		
00:40:05:DF:79:FB	WSAY			00:00:00	6	5	0	0	0		
00:40:96:58:65:EA	tmobile			00:00:00	1	4	0	0	0		
00:02:8A:0E:31:42				00:00:00	8	21	0	0	0		
00:60:1D:F0:D7:BA				00:00:00	3	4	0	0	0		
00:06:25:C3:99:E1				00:00:00	7	85	0	0	0		

**Terminal Window:**

```
root@ec2-54-227-254-145:~# ./ec/ec_dissecto
root@ec2-54-227-254-145:~# ./ec/ec_doppleganger
root@ec2-54-227-254-145:~# ./ec/ec_fingerprint
root@ec2-54-227-254-145:~# ./ec/ec_forge ./src/ec_p
root@ec2-54-227-254-145:~# ./src/ec_vbuf
root@ec2-54-227-254-145:~# ./src/ec_interfa
root@ec2-54-227-254-145:~# ./src/ec_ncurses/
root@ec2-54-227-254-145:~# ./src/inte
root@ec2-54-227-254-145:~# ./src/inte_sniff_da
root@ec2-54-227-254-145:~# ./sbin
root@ec2-54-227-254-145:~# ./lib/ettercap
root@ec2-54-227-254-145:~# ./bin
```

# WEP Tool: WEPCrack

WEPCrack is an open source tool for breaking 802.11 WEP secret keys

This tool is an implementation of the attack described by Fluhrer, Mantin, and Shamir in the paper “*Weaknesses in the Key Scheduling Algorithm of RC4*”

While AirSnort has captured the media attention, WEPCrack was the first publicly available code that demonstrated the above attack

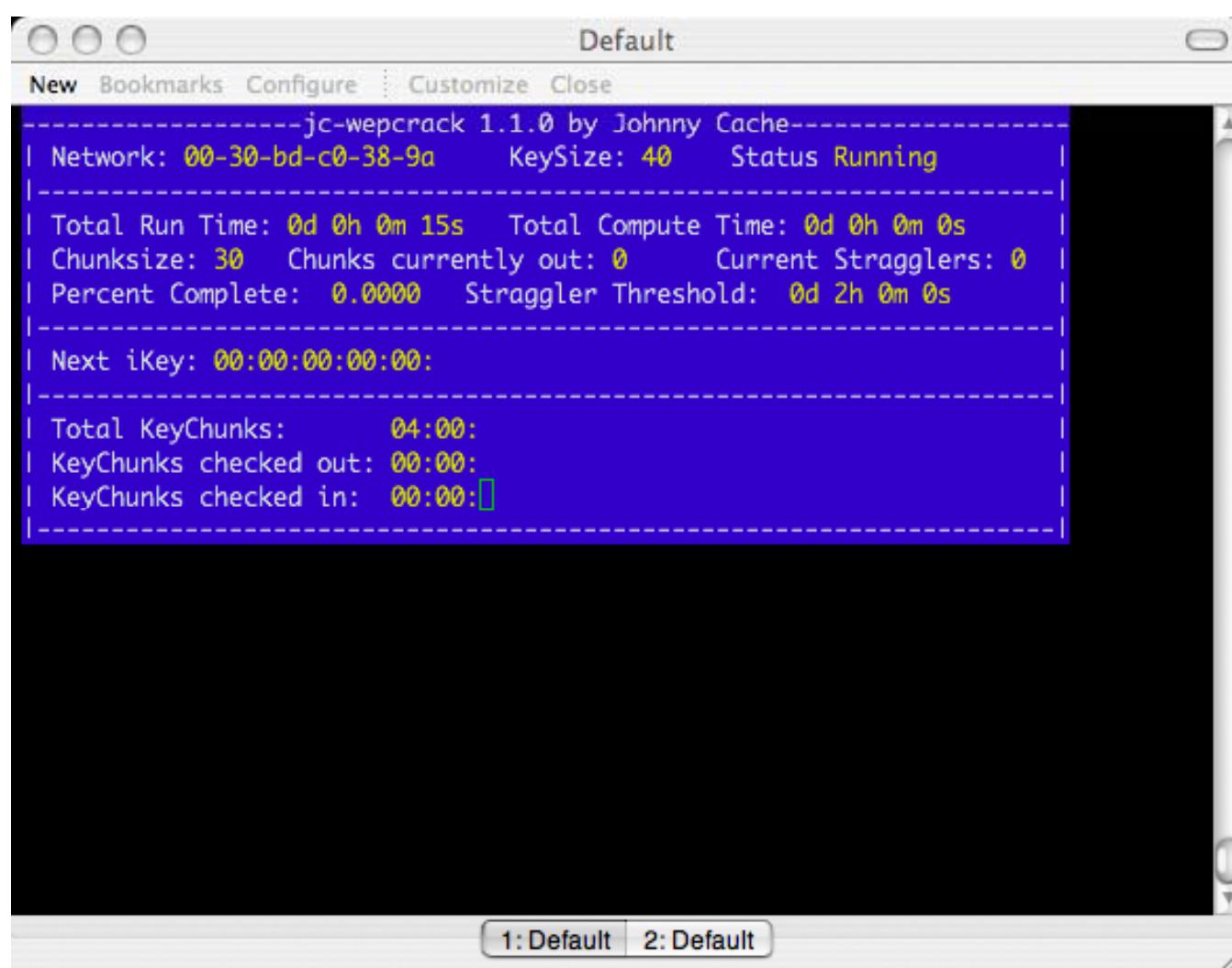
The current tools are Perl-based and are composed of the following scripts:

- WeakIVGen.pl
- prism-getIV.pl
- WEPCrack.pl



Source: [wepcrack.sourceforge.net](http://wepcrack.sourceforge.net)

# WEPCrack: Screenshot



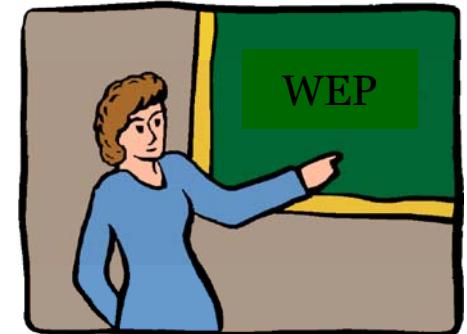
# WEP Tool: WepLab

WepLab is a tool designed to teach how WEP works, what different vulnerabilities it has, and how they can be used in practice to break a WEP protected wireless network

WepLab acts as a WEP Security Analyzer and a WEP Key Cracker

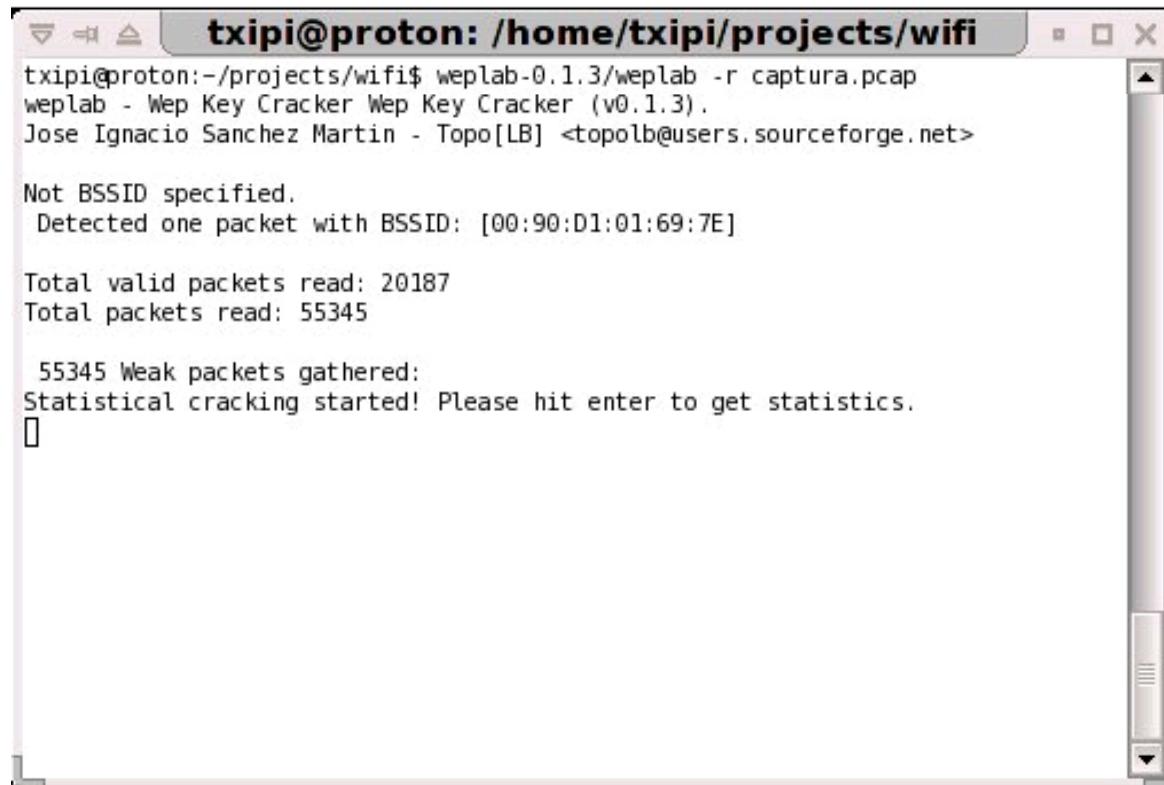
WepLab tries to break the WEP key using several known attacks:

- Bruteforce
- Dictionary
- Statistical attacks



# WepLab: Screenshot 1

WepLab starting to crack a pcap file by a statistical attack



```
txipi@proton: /home/txipi/projects/wifi
txipi@proton:~/projects/wifi$ weplab-0.1.3/weplab -r captura.pcap
weplab - Wep Key Cracker Wep Key Cracker (v0.1.3).
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users.sourceforge.net>

Not BSSID specified.
Detected one packet with BSSID: [00:90:D1:01:69:7E]

Total valid packets read: 20187
Total packets read: 55345

55345 Weak packets gathered:
Statistical cracking started! Please hit enter to get statistics.
[]
```

# WepLab: Screenshot 2

WepLab showing progress information in a statistical attack

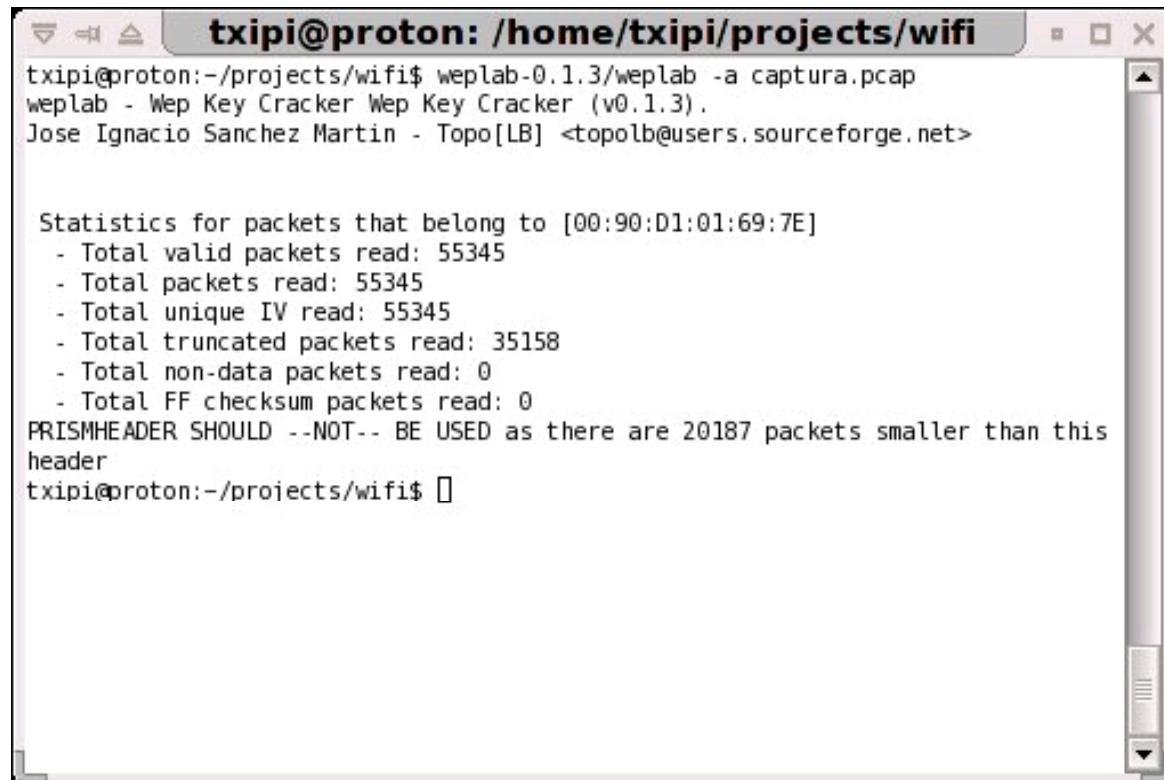
```
txipi@proton: /home/txipi/projects/wifi
Total valid packets read: 20187
Total packets read: 55345

55345 Weak packets gathered:
Statistical cracking started! Please hit enter to get statistics.

1016576 keys tested
4297 branch taken
17230 c/s
72 b/s
Key: 66:a1:2d:ef:ff
Key: 00:00:00:00:00
Attack 1 current weaks :byte 0 (1),byte 1 (3),byte 2 (2),byte 3 (1),byte 4 (0),
Attack 2 current weaks :byte 0 (0),byte 1 (0),byte 2 (0),byte 3 (0),byte 4 (0),
Attack 3 current weaks :byte 0 (1),byte 1 (0),byte 2 (1),byte 3 (0),byte 4 (0),
Attack 10 current weaks :byte 0 (3),byte 1 (2),byte 2 (0),byte 3 (0),byte 4 (0),
Attack 11 current weaks :byte 0 (0),byte 1 (0),byte 2 (0),byte 3 (0),byte 4 (0),
Attack 12 current weaks :byte 0 (1),byte 1 (0),byte 2 (0),byte 3 (2),byte 4 (0),
Attack 13 current weaks :byte 0 (0),byte 1 (2),byte 2 (0),byte 3 (0),byte 4 (0),
Attack 17 current weaks :byte 0 (116),byte 1 (116),byte 2 (114),byte 3 (62),byte
4 (0),
```

# WepLab: Screenshot 3

WepLab showing analyzing process information of a pcap file



```
txipi@proton:~/projects/wifi$ weplab-0.1.3/weplab -a captura.pcap
weplab - Wep Key Cracker Wep Key Cracker (v0.1.3).
Jose Ignacio Sanchez Martin - Topo[LB] <topolb@users.sourceforge.net>

Statistics for packets that belong to [00:90:D1:01:69:7E]
- Total valid packets read: 55345
- Total packets read: 55345
- Total unique IV read: 55345
- Total truncated packets read: 35158
- Total non-data packets read: 0
- Total FF checksum packets read: 0
PRISMHEADER SHOULD --NOT-- BE USED as there are 20187 packets smaller than this
header
txipi@proton:~/projects/wifi$
```



TM

# Attacking WPA Encrypted Networks

WPA utilizes a 256-bit pre-shared key or a passphrase that can vary in length from eight to sixty-three bytes

Short passphrase-based keys (less than 20 bytes) are vulnerable to the offline dictionary attack

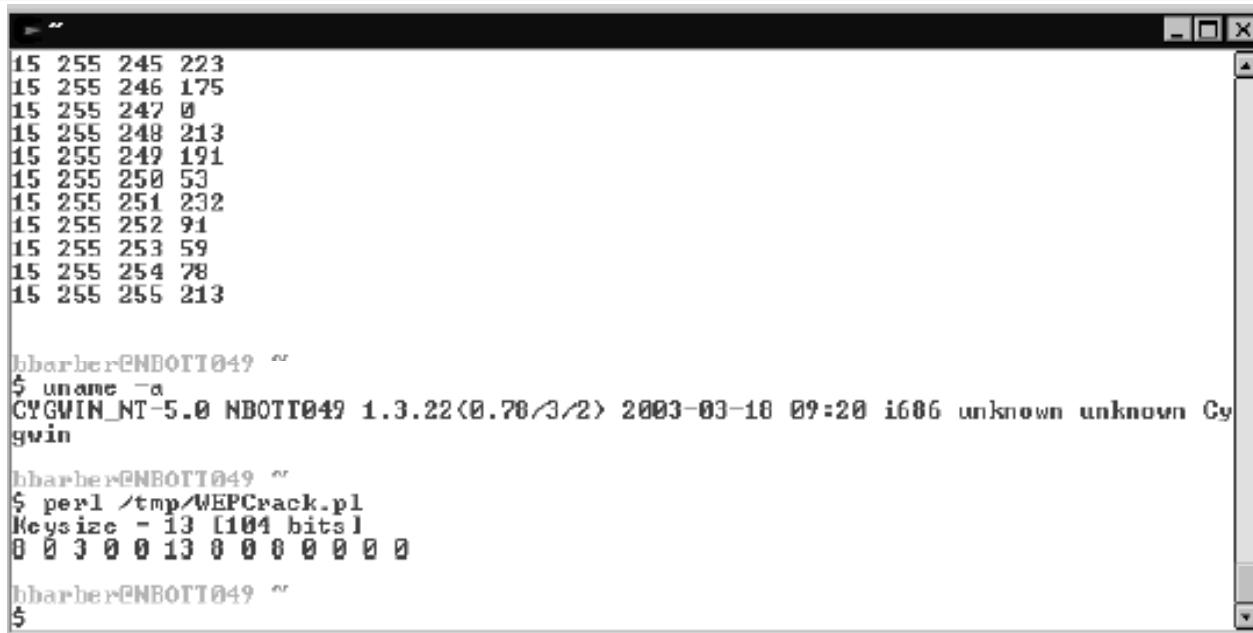
The pre-shared key that is used to set up the WPA encryption can be captured during the initial communication between the access point and the client card

After capturing pre-shared key, it is easy to “guess” the WPA key using the same concepts that are used in any password dictionary attack

# Attacking WEP with WEPCrack on Windows using Cygwin

WEPCrack is a set of Open Source PERL scripts intended to break 802.11 WEP secret keys

Cygwin is a Linux-like environment for Windows that consists of a DLL (cygwin1.dll)



```
15 255 245 223
15 255 246 175
15 255 247 0
15 255 248 213
15 255 249 191
15 255 250 53
15 255 251 232
15 255 252 91
15 255 253 59
15 255 254 78
15 255 255 213

lbarber@NBOTT049 ~
$ uname -a
CYGWIN_NT-5.0 NBOTT049 1.3.22(0.70/3/2) 2003-03-18 09:20 i686 unknown unknown Cygwin

lbarber@NBOTT049 ~
$ perl /tmp/WEPCrack.pl
Keysize = 13 [104 bits]
0 0 0 0 13 0 0 0 0 0 0 0 0
lbarber@NBOTT049 ~
$
```

Executing WEPCrack.pl in Cygwin

# Attacking WEP with WEPCrack on Windows using PERL Interpreter

ActiveState ActivePerl ([www.activestate.com](http://www.activestate.com)), provides a robust PERL development environment that is native to Windows

WEPCrack was written so that it could be ported to any platform that has a PERL interpreter without modification



```
C:\>perl \cygwin\temp\WEPCrack.pl
Keysize = 13 [104 bits]
8 0 3 0 0 13 8 0 8 0 0 0 0
C:\>
```

Executing WEPCrack.pl at the Windows Command Prompt

# Tool: Wepdecrypt

Wepdecrypt is a Wireless LAN Tool

It guesses the WEP keys based on the active dictionary attack, key generator, and distributed network attack

It implements packet filters

It starts cracking with only one crypted packet

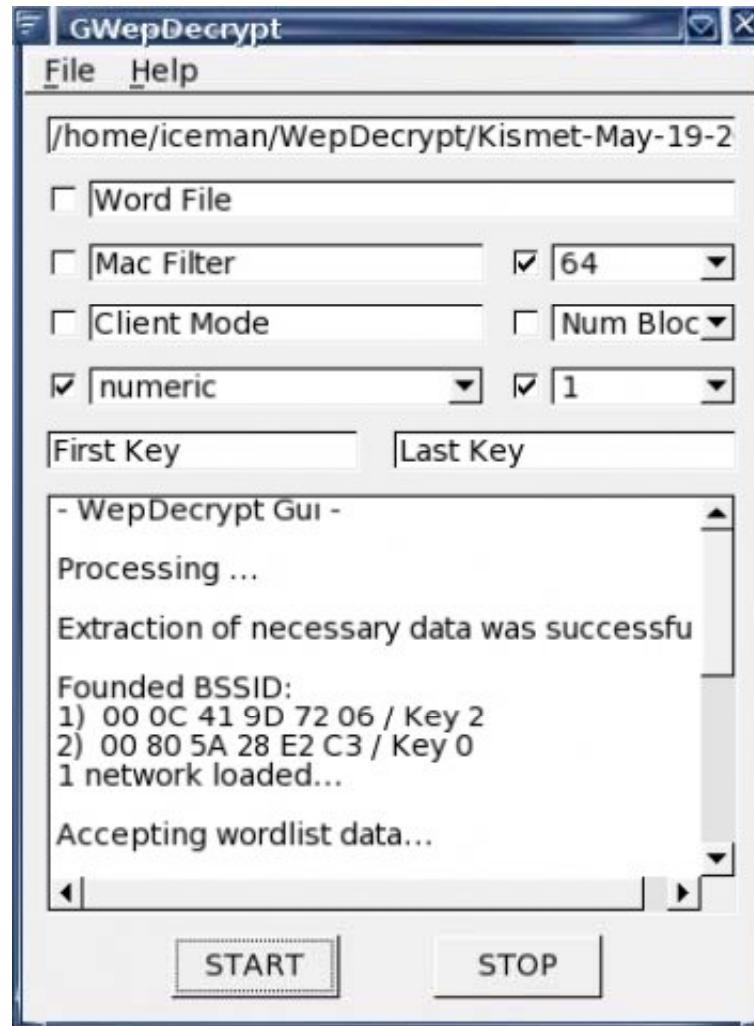
It has its own key generator

A dumpfile can be cracked over a network

It can act as both server and client



# Wepdecrypt: Screenshot



# WPA-PSK Cracking Tool: CowPatty

CowPatty tool is used as a brute force tool for cracking WPA-PSK, considered the “New WEP” for home Wireless Security

This program simply tries a bunch of different options from a dictionary file to see if one ends up matching what is defined as the Pre-Shared Key

The screenshot shows a terminal window titled '<Finished> - /root/cowpatty - Konsole'. The window displays the output of the CowPatty tool. It starts by calculating the PMK for the passphrase 'abc123abc123', showing the resulting hex bytes. Then, it calculates the PTK using the collected data and the calculated PMK, displaying the resulting hex bytes. Finally, it calculates the hmac-MD5 Key MIC for the frame, showing the resulting hex bytes. The text 'The PSK is "abc123abc123"' is displayed in red at the bottom. A status message at the bottom indicates '20 passphrases tested in 1.89 seconds: 10.60 passphrases/second'.

```
<Finished> - /root/cowpatty - Konsole
Session Edit View Bookmarks Settings Help
Calculating PMK for "abc123abc123".
PMK is
    7814 69bf 213b 11e2 6233 7001 f06a 5809 x.i.!;..b3p..jX.
    a1b6 4f75 ed9b d6fe 2c42 8fbc 781d 47d5 ..0u....,B..x.G.

Calculating PTK with collected data and PMK.
Calculated PTK for "abc123abc123" is
    e339 644d 2d34 d1fe 0e44 36de a031 e007 .9dM-4...D6..1..
    7a04 d6f9 ef2a 582e df9d e32e 2b67 351e z....*X.....+g5.
    c6ff e6dc 08cc 14de a62f e388 3a4c 4e65 ...../...:LN
    7a92 c646 1763 0cb9 494b 73fd 61d7 fad4 z..F.c..IKs.a...

Calculating hmac-MD5 Key MIC for this frame.
Calculated MIC with "abc123abc123" is
    3d1b bbf0 c4ae bacd dcba 75d3 efb2 5f66 =.....u....f

The PSK is "abc123abc123".

20 passphrases tested in 1.89 seconds: 10.60 passphrases/second
```

# 802.11 Specific Vulnerabilities

## Default SSIDs

- Many people fail to change the default SSID set by manufacturers
- Hackers recognize it and can assume that administrator has not given much time for securing wireless network

## Beacon Broadcast

- Base stations regularly broadcast its existence for end users to listen and negotiate a session
- Signals can be captured by anyone
- Wireless network SSID are known while connecting to the station

# Evil Twin: Attack

Evil twin is a home-made wireless access point which masquerades as a legitimate one to gather personal or corporate information without the end-user's knowledge

Attacker positions himself in the vicinity of a legitimate Wi-Fi access point and lets his computer discover what name and radio frequency the legitimate access point uses



Attacker then sends out his own radio signal, using the same name

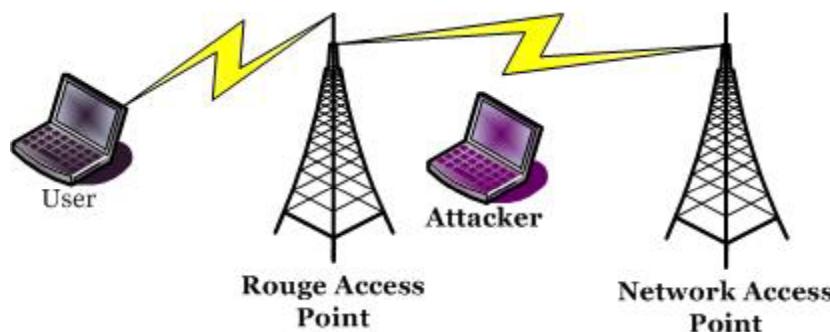
# Rogue Access Points

A rogue/unauthorized access point is one that is not authorized for operation by a particular firm or network

Tools that can detect rogue/unauthorized access points include NetStumbler and MiniStumbler

The two basic methods for locating rogue access points are:

- Beaconing/requesting a beacon
- Network sniffing: Looking for packets in the air



# Tools to Generate Rogue Access Points: Fake AP

Fake AP provides the means of hiding in plain sight, making it unlikely for an organization to be discovered

It confuses Wardrivers, NetStumblers, Script Kiddies, and other undesirables

Black Alchemy's Fake AP generates thousands of counterfeit 802.11b access points

It is a proof of concept released under the GPL

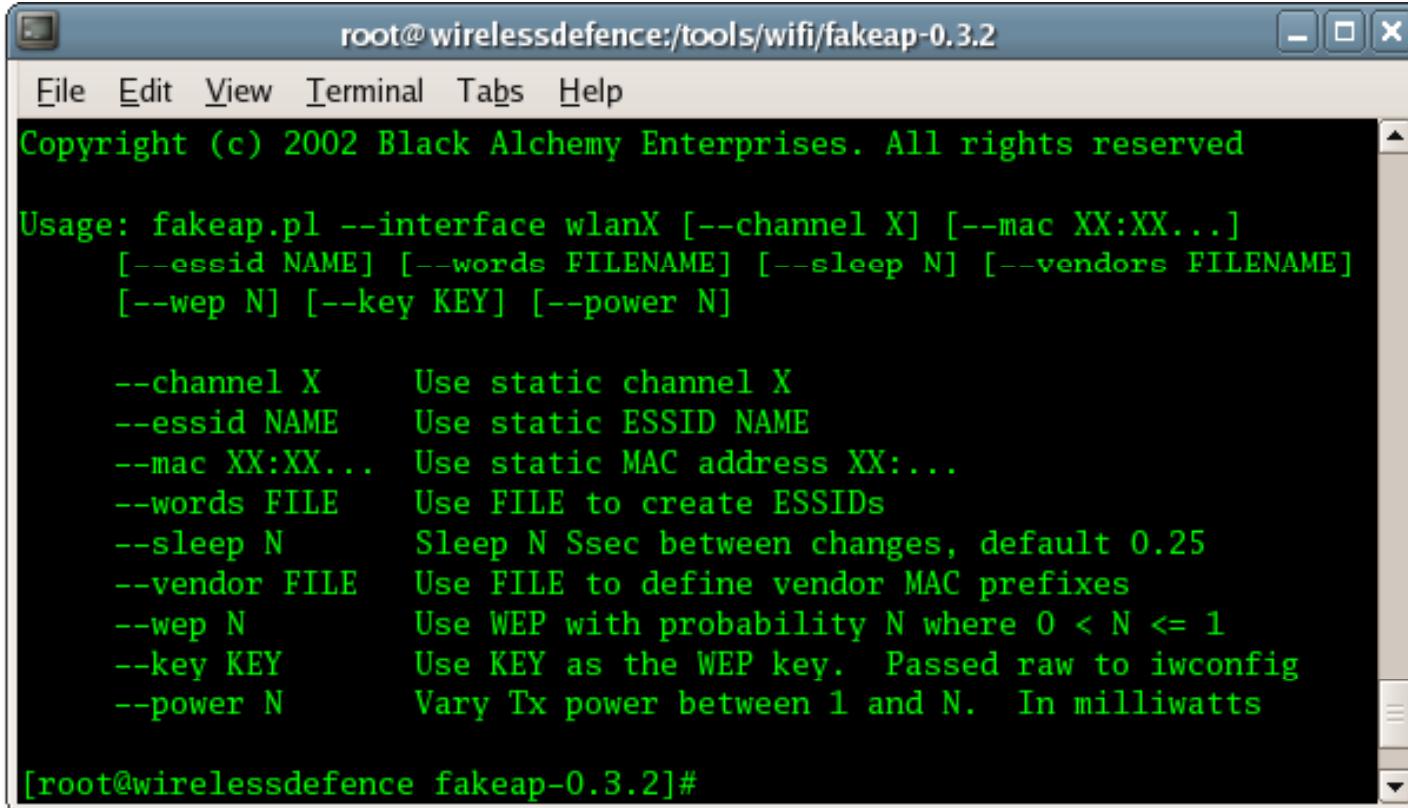
It runs on Linux and BSD versions



Source: <http://www.blackalchemy.to/>

Copyright © by EC-Council  
All Rights Reserved. Reproduction is Strictly Prohibited

# Fake AP: Screenshot



The screenshot shows a terminal window titled "root@wirelessdefence:/tools/wifi/fakeap-0.3.2". The window contains the following text:

```
root@wirelessdefence:/tools/wifi/fakeap-0.3.2
File Edit View Terminal Tabs Help
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

[root@wirelessdefence fakeap-0.3.2]#
```

# Tools to Detect Rogue Access Points: Netstumbler

NetStumbler is a Windows utility for WarDriving written by MariusMilner

Netstumbler is a high-level WLAN scanner. It operates by sending a steady stream of broadcast packets on all possible channels

Access points (APs) respond to broadcast packets to verify their existence, even if beacons have been disabled

NetStumbler displays:

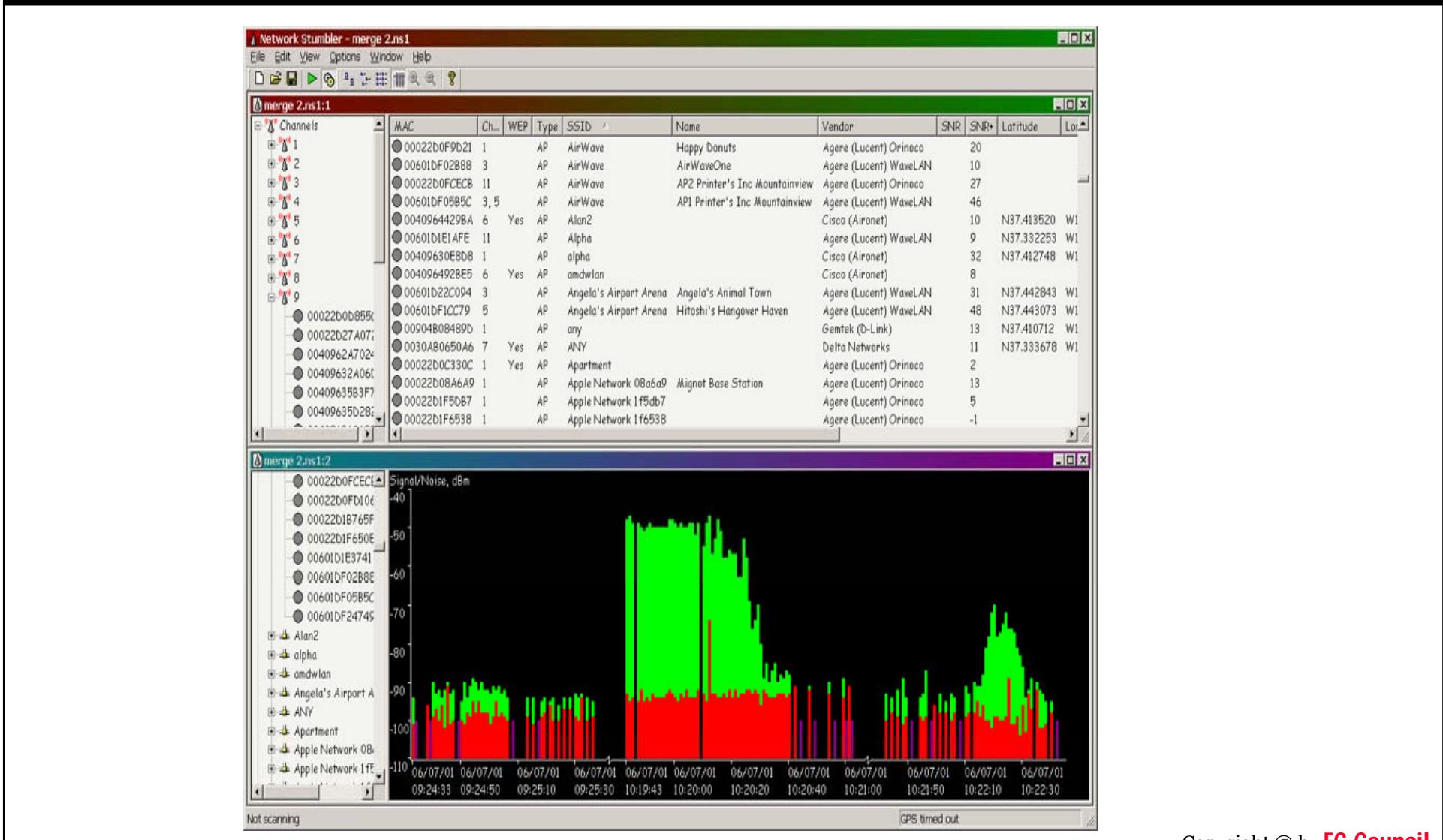
- Signal Strength
- MAC Address
- SSID
- Channel details





TM

# Netstumbler: Screenshot



# Tools to Detect Rogue Access Points: MiniStumbler

MiniStumbler is the smaller sibling of a free product called NetStumbler

By default, most WLAN access points (APs) broadcast their Service Set Identifier (SSID) to anyone who will listen. This flaw in WLAN is used by MiniStumbler

It can connect to a global positioning system (GPS)

The screenshot shows the MiniStumbler application window. At the top, it displays the title 'MiniStumbler' and the time '11:19'. The main area is a table with two columns: 'MAC' and 'SSID'. The 'MAC' column lists various MAC addresses, and the 'SSID' column lists the corresponding SSID names. The bottom of the window contains a toolbar with buttons for 'File', 'View', 'Opt', 'Spd', 'GPS', and other controls.

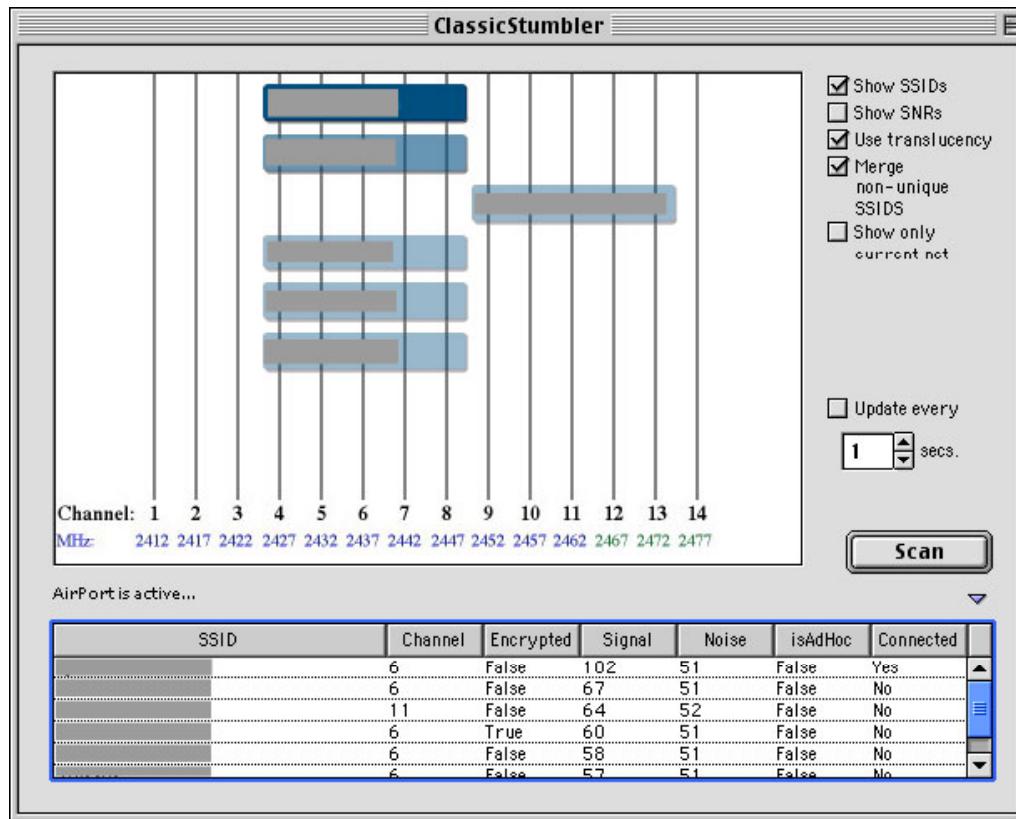
MAC	SSID
00022D09018F	WlanNetwork2
00022D0C4884	WlanNetwork1
0001037C01F9	3COM
0002B365E560	intelap
004005DE21A7	default
00409624D1D4	encomwireless
00409626296F	encomwireless
004096257026	Cybs500WireLess121
0040962628F8	Cybs500WireLess121
00022D01DC19	CalgaryZoo
F202A800E102	galaxy
00045AED6B65	linksys
00022D0029C91	Grand&Tow

Source: [www.netstumbler.com](http://www.netstumbler.com)

# ClassicStumbler

ClassicStumbler scans and displays the wireless access points information within range

It displays the information about the signal strength, noise strength, signal to noise ratio, and channel of the access point





TM

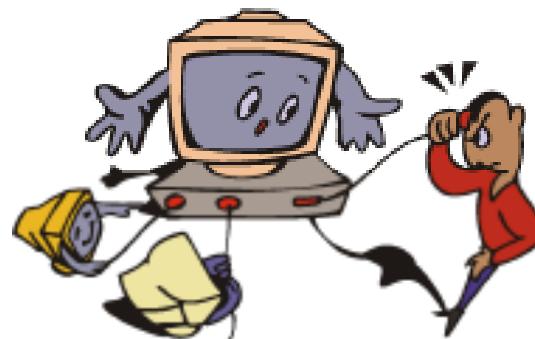
**CEH**

Certified Ethical Hacker

# AirFart

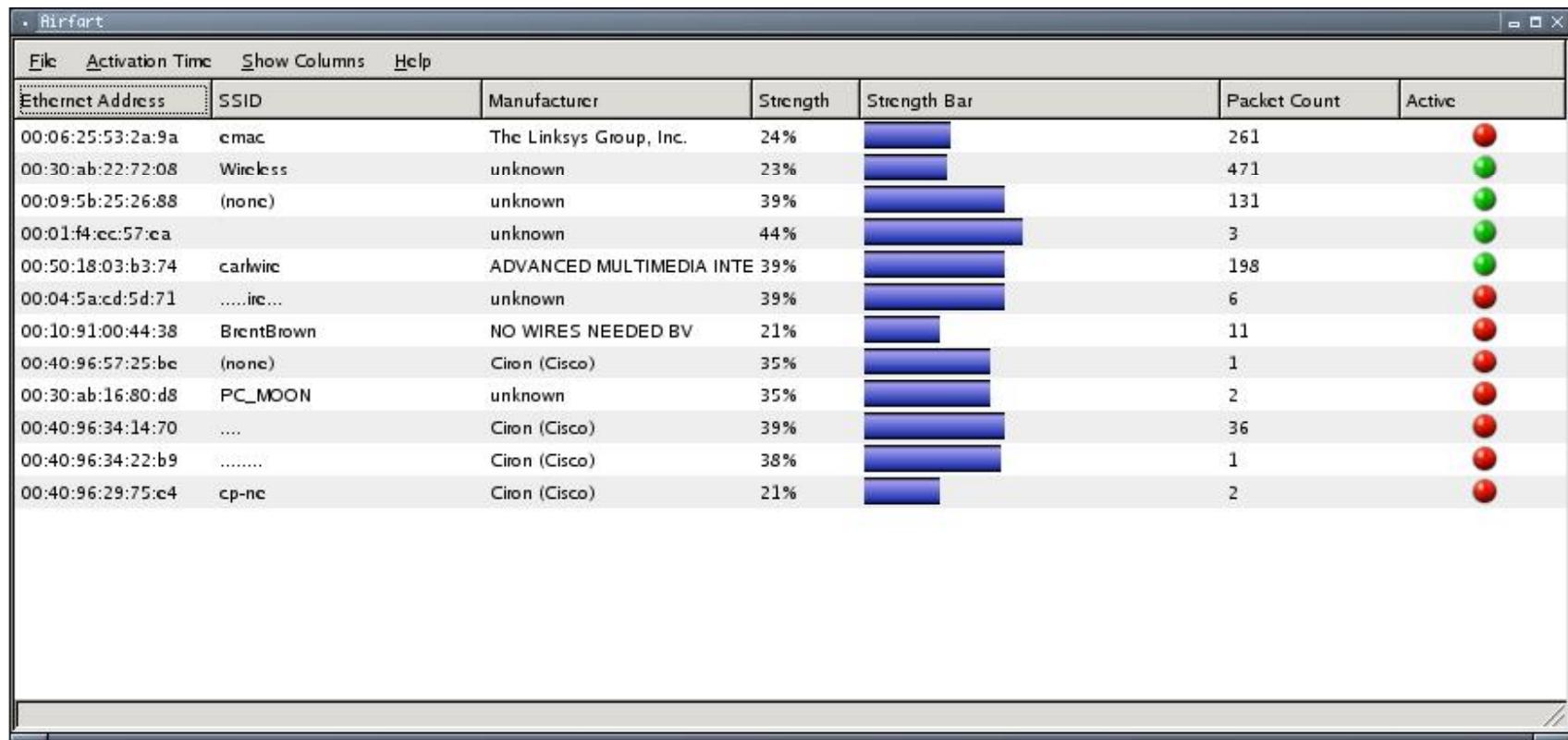
AirFart is used to detect wireless devices and calculate their signal strength

It implements a modular n-tier architecture with the data collection at the bottom tier and a graphical user interface at the top





# AirFart: Screenshot

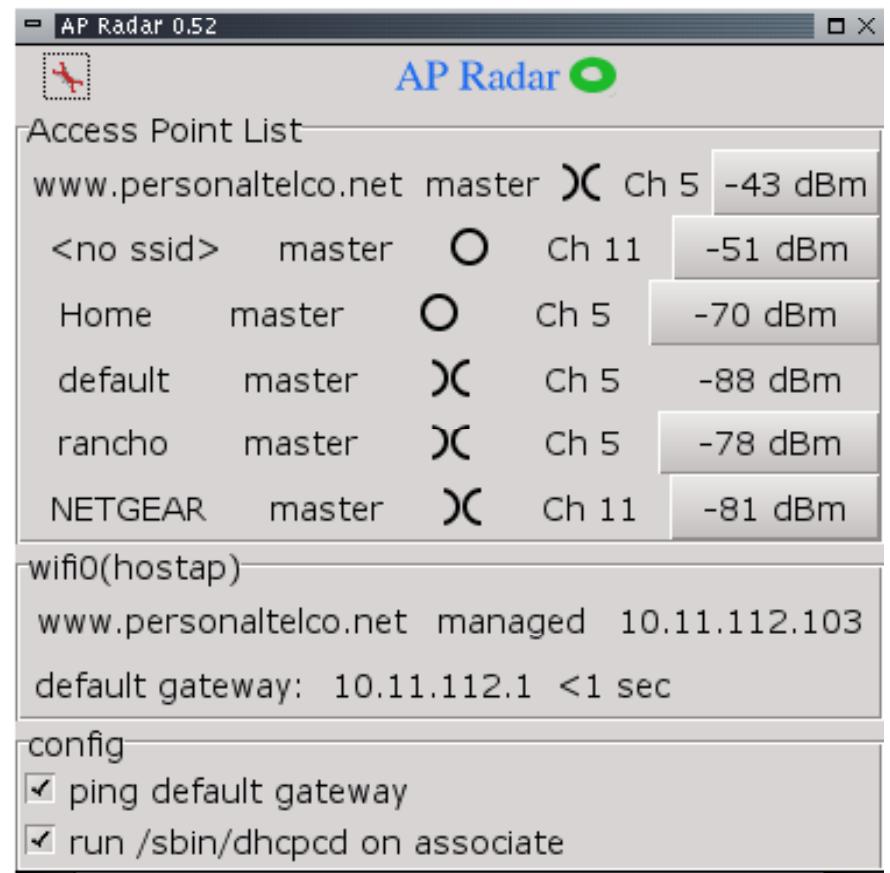


# AP Radar

AP Radar is a wireless profile manager which is based on Linux/GTK+ graphical netstumbler

It is meant to replace the manual process of running iwconfig and dhclient

AP Radar can be used to reconfigure different APs with ease



# Hotspotter

Hotspotter is an automatic wireless client penetration tool

It monitors the network passively for probe request frames to identify the preferred networks of Windows XP clients

Then hotspotter compares it to a list of common hotspot network names

It allows the client to authenticate when matched to a common hotspot name

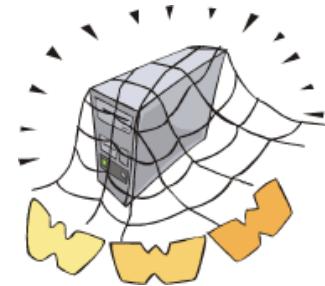


# Cloaked Access Point

Wireless network administrators ‘Cloak’ their access points by putting them in ‘Stealth’ mode

Cloaked access points are not detected by active scanners like NetStumbler

The only way to detect cloaked access point is by passive scanners like Kismet or Airsnort





TM

# WarDriving Tool: Shtumble

shtumble detects nearby access points, allows to select one, starts DHCP if appropriate (usually), and performs WEP or WPA or other custom config for known networks

```
shtumble help      Use 'q' to leave this help screen.

Use the up and down arrows (or 'j' and 'k') to move among the available
networks. Select one with the Enter key.

Green networks are open, or are known to you,
Yellow networks are open, but have a relatively weak
signal. Red networks are encrypted, and you don't know
(or haven't configured) the encryption key.

'r' will toggle the wireless radio on and off.
'd' will disconnect the wireless interface.
'l' will toggle whether all hidden nets will be listed, or only
    those which have been connected to before, and are in range now.
'c' will bring up an editor on the global config file.
'e' will bring up an editor for the selected network's config file.
'n' will bring up an editor for a new network's config file, after
    prompting you for its name.
'x' will let you delete an existing network configuration. This
    is rarely necessary.
'q' will quit the program. Network will remain connected.

shtumble ist:
Copyright 2004,2007 by Paul Fox, and is released under the GNU General
Public License, Version 2. A copy of GPLv2 is included in the shtumble
source script.
```

# Shtumble: Screenshot

```

Available networks:                               (use 'h' for Help)
Nothing to select

--- Current config for eth1 ---
ifconfig Link encap:Ethernet HWaddr 00:16:6F:B2:59:09
      UP BROADCAST MULTICAST MTU:1500 Metric:1
      RX packets:238 errors:41 dropped:132 overruns:0 frame:0
iwconfig radio off ESSID:"--"
      Mode:Managed Channel:0 Access Point: Not-Associated
      Link Quality:0 Signal level:0 Noise level:0
--- /etc/resolv.conf ---
search foxharp.boston.ma.us nameserver 192.168.111.11 nameserver
192.168.111.9
--- Default route(s) ---
0.0.0.0      192.168.111.1  0.0.0.0      UG      0      0      0 eth0
--- Last configuration output ---

```

Radio off, no networks in view

```

Available networks:                               (use 'h' for Help)
--> The Quick Brown Fox (71 dBm) encrypted
      Farrell (82 dBm) encrypted
      Apple Network 0e1a01 (83 dBm)

--- Current config for eth1 ---
ifconfig Link encap:Ethernet HWaddr 00:16:6F:B2:59:09
      inet addr:192.168.110.13 Bcast:192.168.110.255 Mask:255.255.255.0
      inet6 addr: fe80::216:6fff:feb2:5909/64 Scope:Link
      iwconfig IEEE 802.11b ESSID:"The Quick Brown Fox"
      Mode:Managed Frequency:2.437 GHz Access Point: 00:12:17:25:8E:9F
      Link Quality=59/100 Signal level=-65 dBm Noise level=-85 dBm
--- /etc/resolv.conf ---
search foxharp.boston.ma.us nameserver 192.168.111.11 nameserver
192.168.111.9
--- Default route(s) ---
0.0.0.0      192.168.110.1  0.0.0.0      UG      0      0      0 eth1
0.0.0.0      192.168.111.1  0.0.0.0      UG      0      0      0 eth0
--- Last configuration output (for net "The Quick Brown Fox") ---
Doing static configuration.
Done.

```

Associated, and a few networks available

# Temporal Key Integrity Protocol (TKIP)

Secret key is created during 4-way handshake authentication

It dynamically changes secret key

Function is used to create new keys based on the original secret key created during authentication

Initialization vectors increases to 48 bits

First 4 bits indicate QoS traffic class

Remaining 44 bits are used as a counter

Over 500 trillion key streams are possible

Initialization vectors are hashed

It is harder to detect key streams with the same initialization vectors



# LEAP: The Lightweight Extensible Authentication Protocol

Proprietary, closed solution:

- LEAP was started (without many details) by Cisco as unaffected by WEP vulnerabilities (Cisco 2002)

LEAP conducts mutual authentication:

- Client is assured that the access point is an authorized one
- Uses per-session keys that can be renewed regularly:
  - Makes the collection of a pad or weak IVs more difficult
  - Secret key can be changed before the collection is complete
- The user is authenticated, instead of the hardware:
  - MAC address access control lists are not needed
- LEAP requires an authentication server (RADIUS) to support the access points



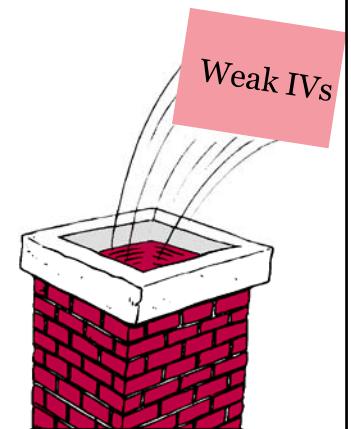
## Dictionary attacks

- Password-based scheme
- Passwords should be guessable (**Joshua Wright** 2003)



## LEAP access points do not use weak IVs

- Use MS-CHAP v2, show the same weaknesses as MS-CHAP (Wright 2003)
- There are many variants of the Extensible Authentication Protocol, such as EAP-TLS and PEAP



# LEAP Attack Tool: ASLEAP

ASLEAP is an hacking tool, released as a proof-of-concept to demonstrate weakness in LEAP and uses off-line dictionary attack to break LEAP passwords



## Features:

- Recovers weak LEAP passwords (duh)
- Can read live from any wireless interface in RFMON mode
- Can monitor a single channel, or perform channel hopping to look for targets
- Handles dictionary and genkeys files up to 4 TB in size

# Working of ASLEAP

This tool works as follows:

Scans the 802.11 packets by putting the wireless interface in RFMON mode



Hops channels to look for targets (WLAN networks that uses LEAP)



De-authenticates the users on LEAP networks forcing them to re-authenticate by providing their user name and password

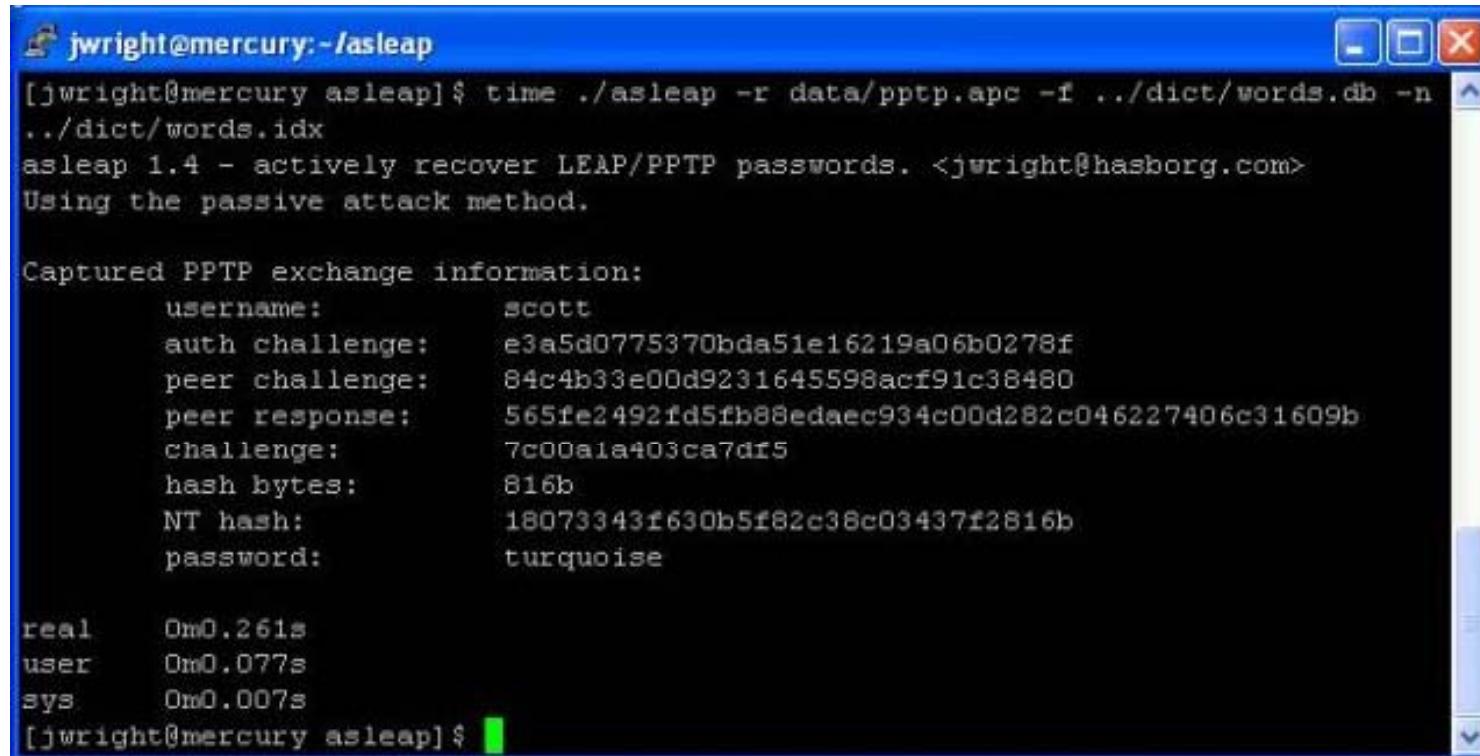


Records the LEAP exchange information to a libcap file



The information captured above is then analyzed offline and compared with values in dictionary to guess the password

# ASLEAP: Screenshot



```
jwright@mercury:~/asleap
[jwright@mercury asleap]$ time ./asleap -r data/pptp.apc -f ../dict/words.db -n
./dict/words.idx
asleap 1.4 - actively recover LEAP/PPTP passwords. <jwright@hasborg.com>
Using the passive attack method.

Captured PPTP exchange information:
    username:          scott
    auth challenge:    e3a5d0775370bda51e16219a06b0278f
    peer challenge:    84c4b33e00d9231645598acf91c38480
    peer response:     565fe2492fd5fb88edaec934c00d282c046227406c31609b
    challenge:         7c00a1a403ca7df5
    hash bytes:        816b
    NT hash:           18073343f630b5f82c38c03437f2816b
    password:          turquoise

real    0m0.261s
user    0m0.077s
sys     0m0.007s
[jwright@mercury asleap]$
```



TM

# Tool: Cain & Abel

Cain & Abel is a password recovery tool for Microsoft Operating Systems

It allows recovery of several kind of wireless network keys

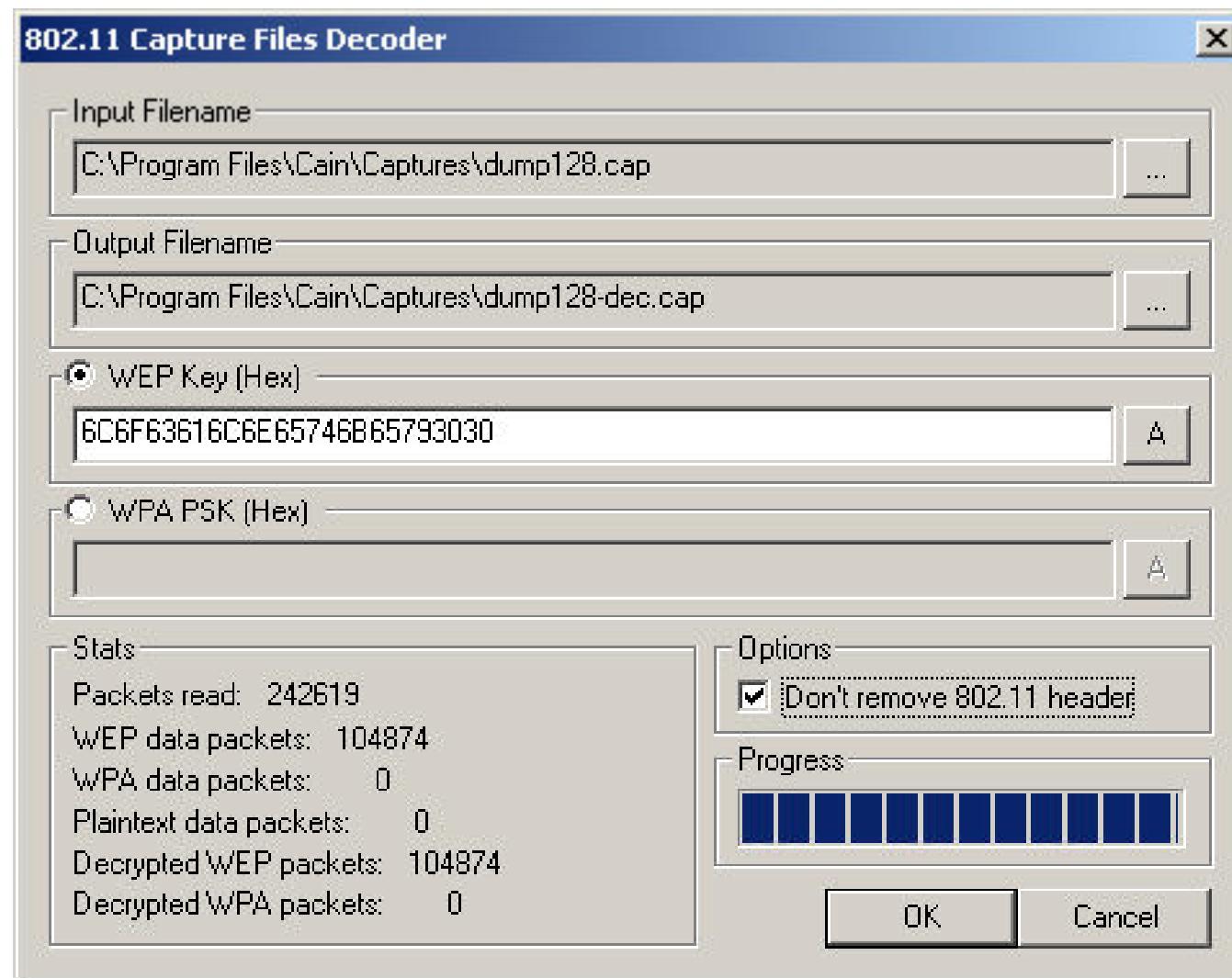
## Features:

- Password decoders to immediately decode encrypted passwords from several sources
- WEP Cracker can quickly recover 64-bit and 128-bit WEP keys if enough unique WEP IVs are available
- Wireless Scanner detects Wireless Local Area Networks (WLANs) using 802.11X
- 802.11 capture files decoder can decode wireless capture files from Wireshark and/or Airodump-ng containing WEP or WPA-PSK encrypted 802.11 frames
- Wireless zero configuration password dumper



TM

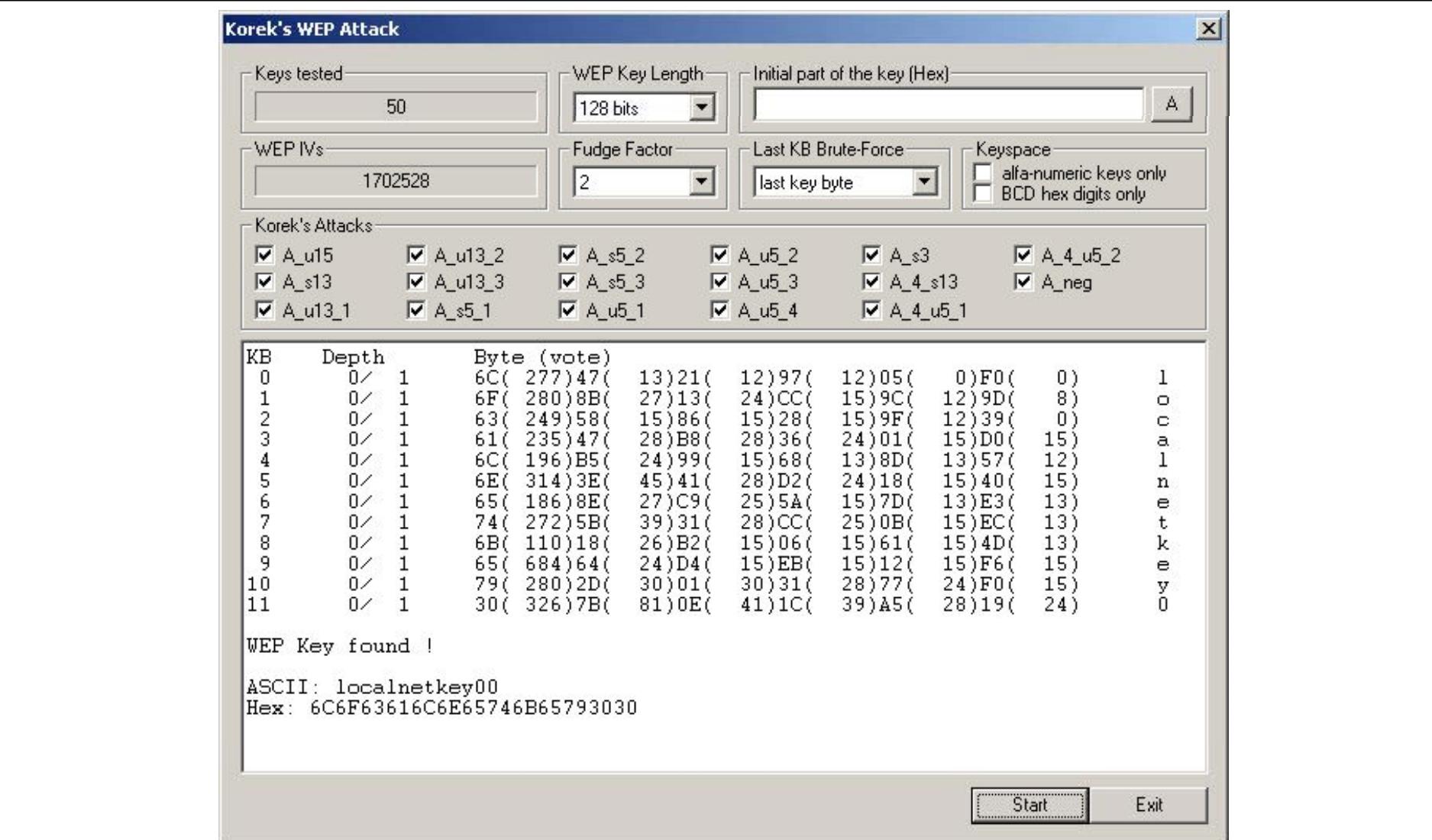
# Cain & Abel: Screenshot 1





TM

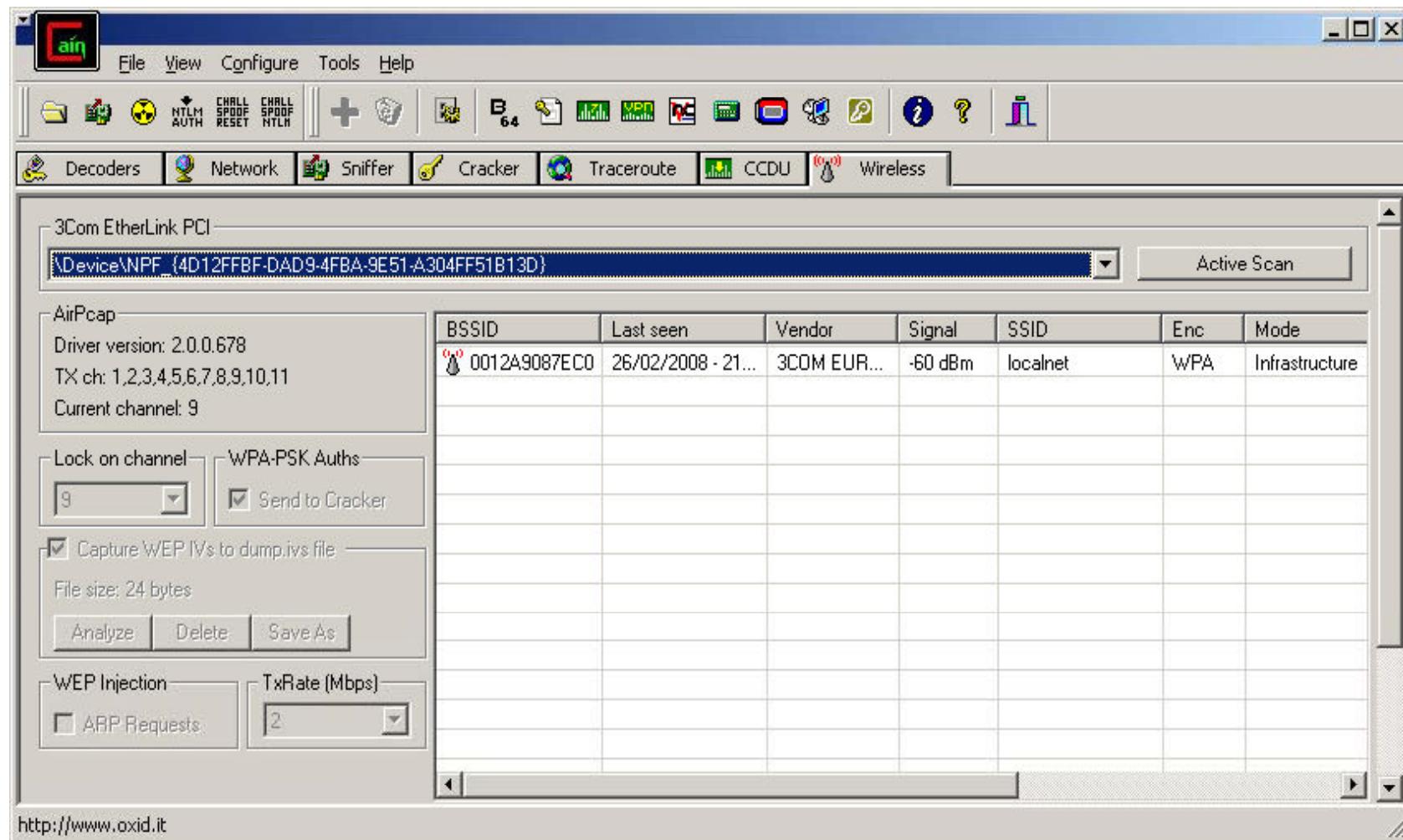
# Cain & Abel: Screenshot 2





TM

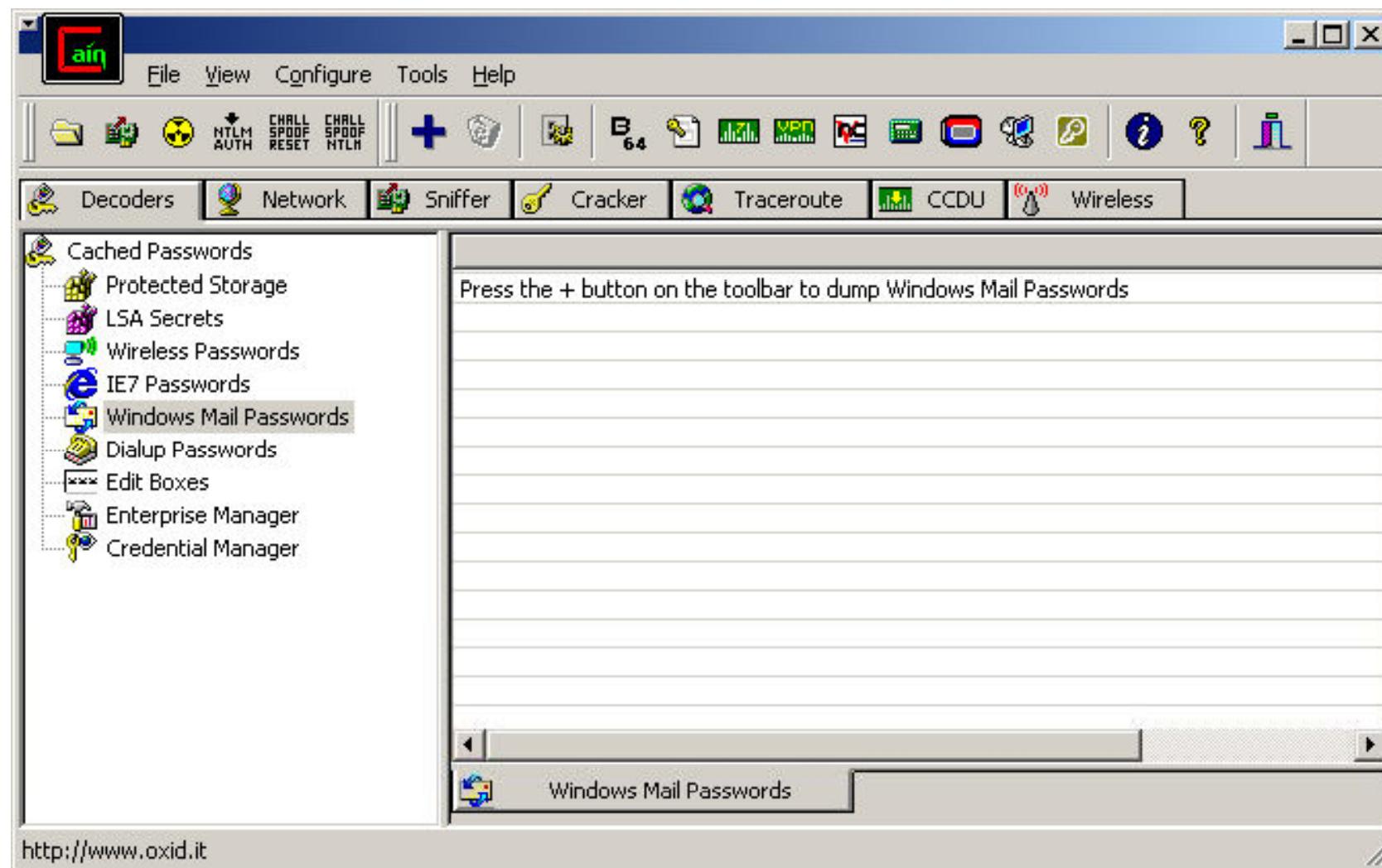
# Cain & Abel: Screenshot 3





TM

# Cain & Abel: Screenshot 4



# MAC Sniffing and AP Spoofing

Attackers can easily sniff MAC addresses because they must appear in the clear even when WEP is enabled

Attackers can use those advantages in order to masquerade as a valid MAC address by programming the wireless card and getting into the wireless network and using the wireless pipes

Spoofing MAC addresses is easy. Using packet-capturing software, attackers can determine a valid MAC address using one packet

To perform a spoofing attack, an attacker must set up an access point (rogue) near the target wireless network or in a place where a victim may believe that wireless Internet is available



# Defeating MAC Address Filtering in Windows

Changing MAC address is an easy job in Windows

Mostly wireless networking equipments send the MAC address as a clear text even if WEP is enabled

MAC address of machines in the wireless network can be sniffed using WireShark

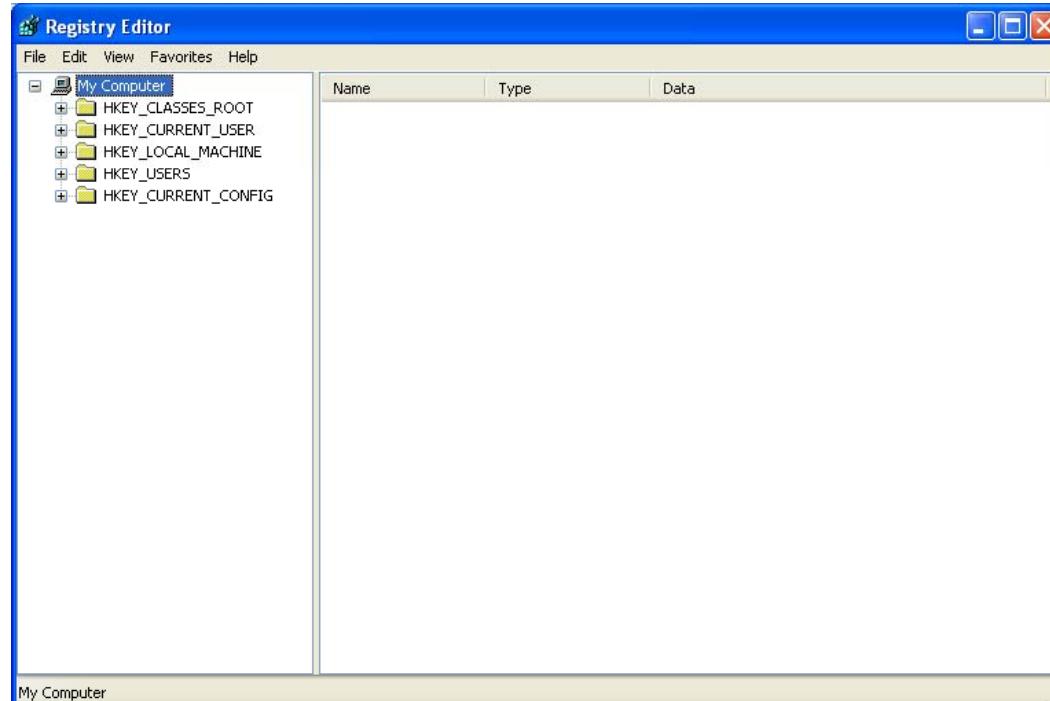
Next thing is to change your MAC address to the one in the 'allowed access' list



# Manually Changing the MAC Address in Windows XP and 2000

MAC address in Windows XP or 2000 can be changed by modifying Windows registry

Go to Start >> Run and type in regedit. It will start the Registry Editor





# Manually Changing the MAC Address in Windows XP and 2000 (cont'd)

Expand the HKEY\_LOCAL\_MACHINE>>System>>CurrentControlSet>>Control folders



Scroll down to the Class folder and expand it



Next, scroll down to the {4D36E972-E325-11CE-BFC1-08002bE10318} folder and expand it

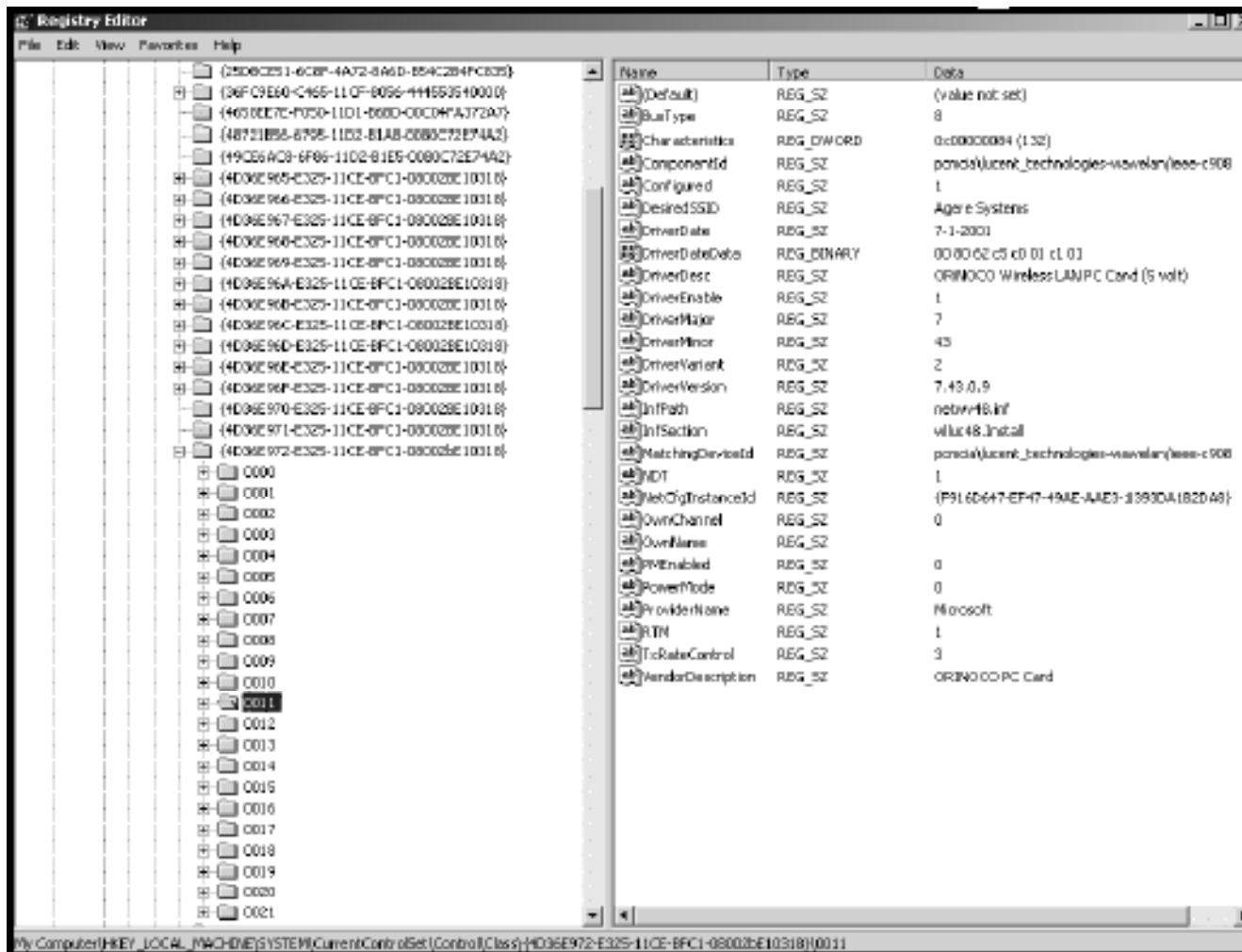


This folder contains the Windows XP Registry information regarding network adapters installed on your system



Scroll through each folder until you find your wireless network adapter

# Manually Changing the MAC Address in Windows XP and 2000 (cont'd)



# Manually Changing the MAC Address in Windows XP and 2000 (cont'd)

Choose Edit>>New >>String Value



This creates a new REG\_SZ string and prompts for a value. Type NetworkAddress



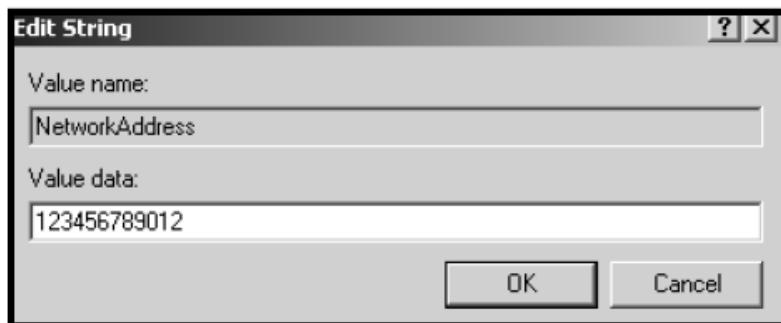
Right-click the NetworkAddress key that was just created and choose Modify



Enter the new MAC address you want to use in the Value Data field and click OK



The new MAC address is assigned as the system starts. Verify this by typing `ipconfig /all`

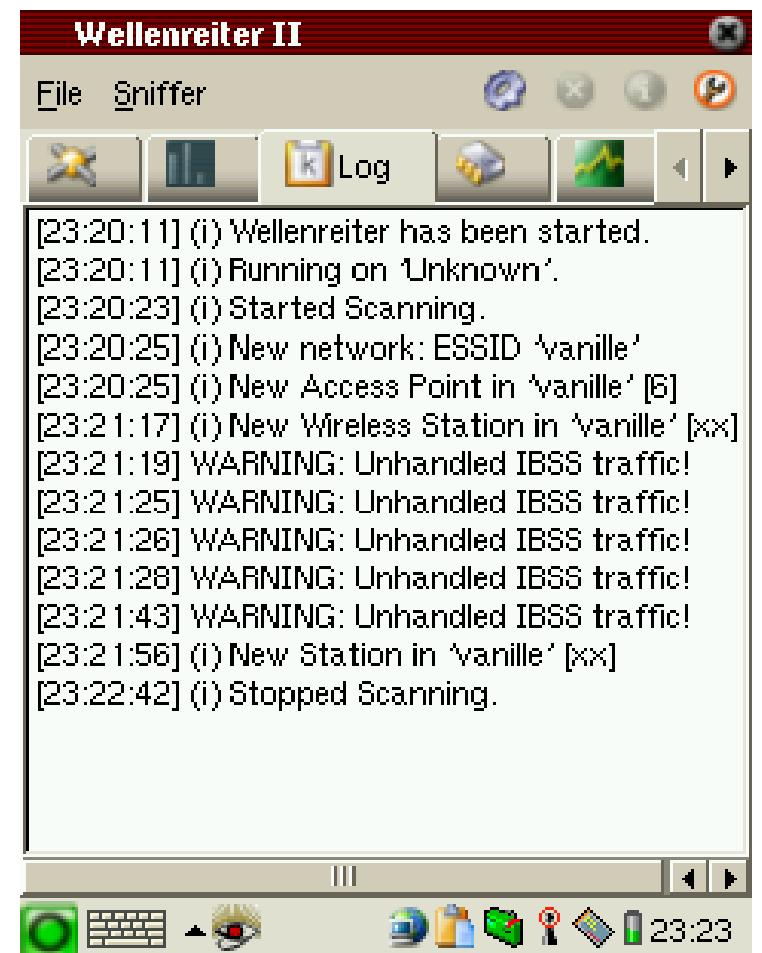


# Tool to Detect MAC Address Spoofing: Wellenreiter

Wellenreiter is a wireless network discovery and auditing tool

It can discover networks (BSS/IBSS) and detect ESSID broadcasting or non-broadcasting networks and their WEP capabilities and the manufacturer automatically

It also identifies traffic that is using a spoofed MAC address without relying on the MAC OUI information



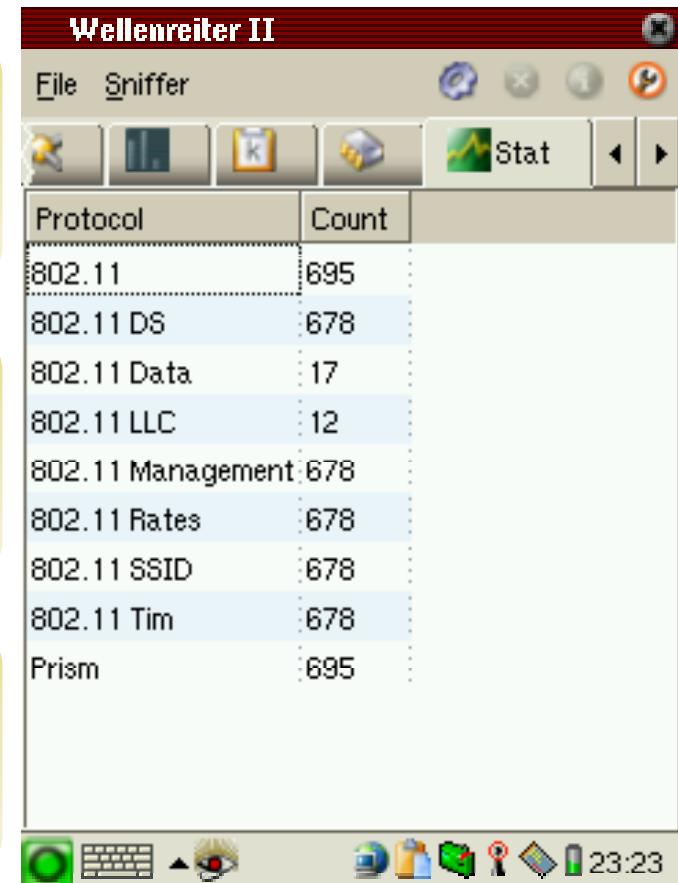
Source: <http://www.wellenreiter.net/>

# Tool to Detect MAC Address Spoofing: Wellenreiter (cont'd)

DHCP and ARP traffic is decoded and displayed to give further information about the networks

An Wireshark/tcpdump-compatible dumpfile and an application savefile are automatically created

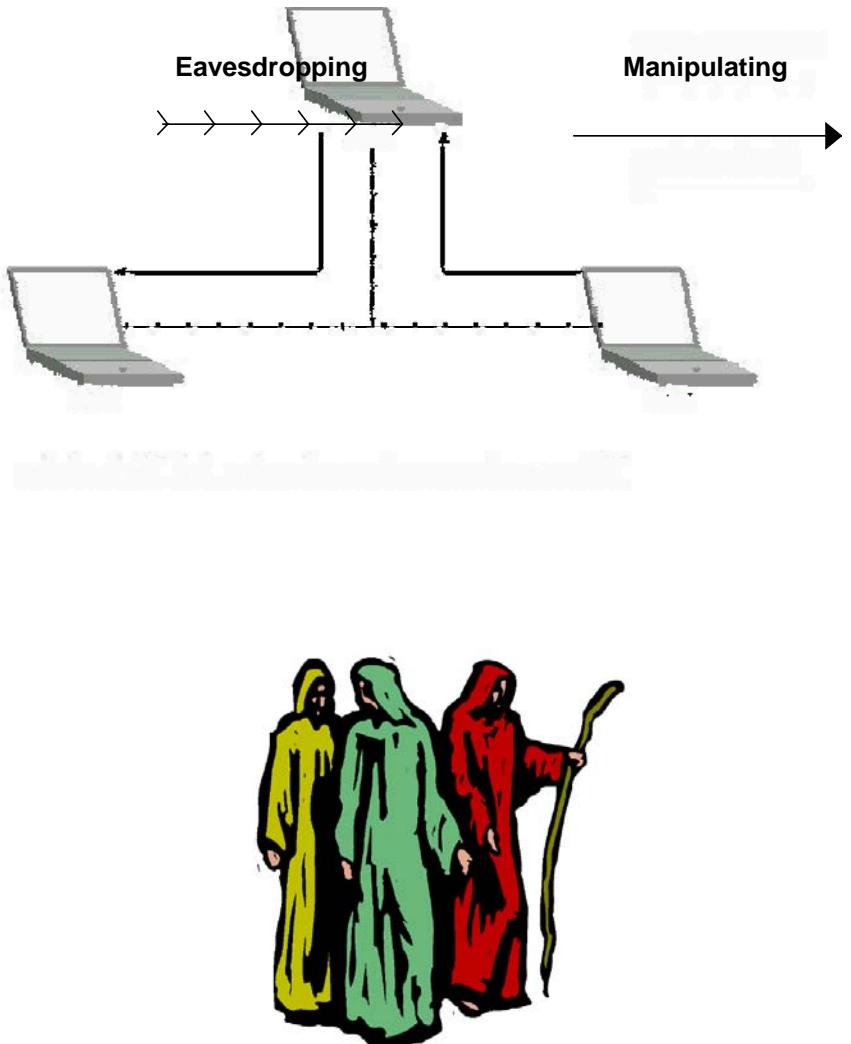
Using a supported GPS device and the gpsd location of the discovered networks can be tracked



# Man-in-the-Middle Attack (MITM)

Two types of MITM:

- Eavesdropping:
  - Happens when an attacker receives a data communication stream
  - Not using security mechanisms such as Ipsec, SSH, or SSL makes data vulnerable to an unauthorized user
- Manipulation:
  - An extended step of eavesdropping
  - Can be done by ARP poisoning



# Denial-of-Service Attacks

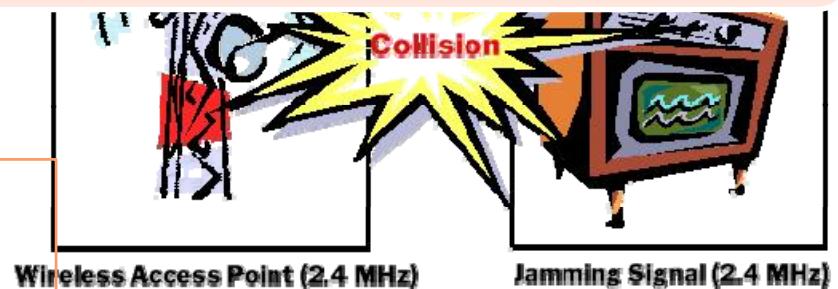
Wireless LANs are susceptible to the same protocol-based attacks that plague wired LANs

## Wireless DoS

WLANs send information via radio waves on public frequencies, making them susceptible to inadvertent or deliberate interference from traffic using the same radio band

### Types of DoS attacks:

- Physical Layer
- Data-Link Layer
- Network Layer



# DoS Attack Tool: Fatajack

Fatajack is a modified WLAN Jack that sends a deauth instead of an auth

This tool highlights poor AP security and works by sending authentication requests to an AP with an inappropriate authentication algorithm and status code. This causes most to drop the relevant associated session



# Hijacking and Modifying a Wireless Network

TCP/IP packets go through switches, routers, and APs

Each device looks at the destination IP address and compares it with the local IP addresses

If the address is not in the table, the device hands the packet to its default gateway

This table is a dynamic one that is built up from traffic passing through the device and through Address Resolution Protocol (ARP) notifications from new devices joining the network



# Hijacking and Modifying a Wireless Network (cont'd)



There is no authentication or verification of the validity of request received by the device

A malicious sends messages to routing devices and APs stating that his MAC address is associated with a known IP address

All traffic that goes through that device destined for the hijacked IP address will be handed off to the hacker's machine

# Phone Jammers

A cell-phone jammer transmits radio frequency signals similar to that used by cellular devices to cut off communications between cell phones and cell base stations

Jammer's signal has enough high power to cancel out cellular signals



Some of the high-end jammers block all frequency signals disabling switching over different network types

Range of the jammer depends on its power and the local environment ( $\approx 9m-1.6km$ )



Phone jamming is also known as Denial-of-service

# Phone Jammers (cont'd)

Jammers typically consists of:

- Antenna
- Circuitry
  - Voltage-controlled oscillator
  - Tuning circuit
  - Noise generator
  - RF amplification (gain stage)
  - Power supply



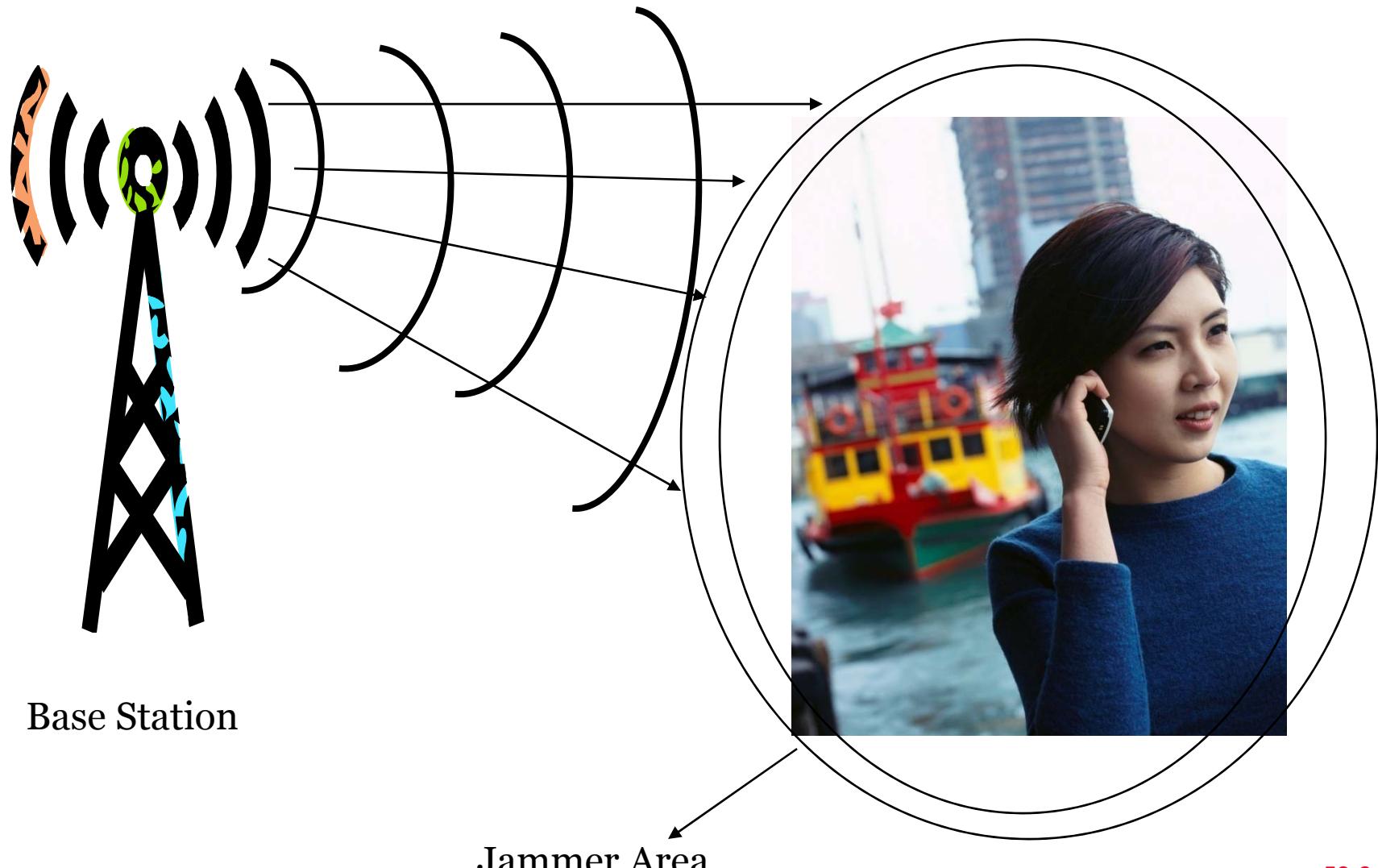
# Phone Jammers (cont'd)

Phone jammers provide solution for areas where cellular communications may cause inconvenience and violation of security policies as:

- Theatres and museums
- Lecture rooms, libraries, schools, and Universities
- Restaurants and public transport
- Places of Worship
- Recording studios
- Businesses (conferences, board of directors rooms, seminars, and meeting rooms)
- Government building and Government complexes
- Law enforcement facilities
- Police stations
- Drug enforcement facilities
- Prison facilities, jails, etc.
- Courts of law and court houses
- Military installations, military complexes, and military training centers



# Phone Jammers: Illustration



# Phone Jammer: Mobile Blocker

Mobile Blocker is an easy to use cost-effective solution for mobile communications control

## Features:

- LED On/Off power indicator
- Accessory antennas for omnidirectional or bi-directional blockage
- Optional remote switch enables immediate On/Off control of the transmitter



# Pocket Cellular Style Cell Phone Jammer

A pocket sized cell phone jammer

It can be used discreetly whilst in a pocket, bag, or even placed for others to see without alerting suspicion

It has an effective range of up to 20 metres



# 2.4Ghz Wi-Fi & Wireless Camera Jammer

Jammer for Wireless cctv cameras, Wi fi, Bluetooth. 100mw total output, range up to 10m

It is a 2.4 GHz jamming device utilizes unique and intelligent technology that will block video, the signals of wireless cameras, wireless LANs, and Bluetooth



## Features:

- Palm sized and portable
- Built-in rechargeable battery which can be used for upto 1.5 hours outdoors
- AC adaptor input for indoor use

# 3 Watt Digital Cell Phone Jammer

3 Watt Digital Cell Phone Jammer is a CXT-5 cell phone jammer

It prevents anyone in the surrounding area from operating a mobile phone

It achieves this by blocking BCCH between the handset and receiver of the system provider

3 Watt Digital Cell Phone Jammer is powered by a 12 volt mains adaptor

It can be used with a battery pack to enable the portable device and is simple to operate



# 3 Watt Quad Band Digital Cellular Mobile Phone Jammer

## Features:

- Strong, tough, robust, and high power output for industrial commercial usage
- Blocks noise or disturbance from unexpected cellular phone calls or text messages (SMS)
- Worldwide compatible
- Paralyzes cellular phone communication links within an effective area
- For use in meeting rooms, conference rooms, museums, galleries, theatres, concert halls etc
- Easy to install and operate
- Indoor and outdoor usage (not splash proof)
- Can be housed in a plastic container



## Features

- Strong, tough, robust, die-cast aluminum casing
- High power output for industrial commercial usage
- Blocks noise or disturbance from unexpected cellular phone calls or text messages (SMS)
- Worldwide compatible
- Paralyzes cellular phone communication links within an effective area
- Sphere coverage area with a radius of its effective distance
- For use in meeting rooms, conference rooms, museums, and galleries
- Easy to install and operate
- Indoor and outdoor usage
- Directional high gain patch antenna
- Anti-tamper proof antenna



# 40W Digital Cellular Mobile Phone Jammer

## Features

- Ultimate power phone jammer
- Strong, tough, robust, and die-cast aluminum casing
- High power output for industrial commercial usage
- Blocks noise or disturbance from unexpected cellular phone calls or text messages (SMS)
- Worldwide compatible
- Paralyze cellular phone communication links within an effective area
- Sphere coverage area with a radius of its effective distance
- For use in museums, galleries, theatres, concert halls etc.
- Easy to install and operate; plug and play
- Weatherproof high gain base station type antenna
- Dual inter cooler for ultimate performance



# Detecting a Wireless Network



Using an operating system, such as Windows XP or Mac with Airport, to detect available networks



Using handheld PCs (Tool: MiniStumbler)



Using passive scanners (Tool: Kismet, KisMAC)



Using active beacon scanners (Tool: NetStumbler, MacStumbler, iStumbler)



# Scanning Tools

# Scanning Tools

Kismet

PrismStumbler

MacStumbler

Mognet

WaveStumbler

StumbVerter

AP Scanner

Wireless Security Auditor

AirTraf

Wifi Finder

eEye Retina WiFi



# Scanning Tool: Kismet

Kismet is completely passive, capable of detecting traffic from APs and wireless clients alike (including NetStumbler clients) as well as closed networks

It requires 802.11b capable of entering RF monitoring mode. Once in RF monitoring mode, the card is no longer able to associate with a wireless network

It needs to run as root, but can switch to lesser privileged UID as it begins to capture

To hop across channels, run *kismet\_hopper -p*

Closed network with no clients authenticated is shown by <nssid> and is updated when client logs on

# Kismet: Screenshot

Network List—(Autofit)						
Name	T	W	Ch	Packts	Flags	Data Clnt
p@thf1nd3r	A	Y	06	171		70 35
<no ssid>	A	N	05	1		0 0
KrullNet1	A	Y	06	27		0 0
<b>linksys</b>	<b>A</b>	<b>N</b>	<b>06</b>	<b>81 FU4</b>		<b>8 2</b>
marley	A	N	06	312		17 1
<no ssid>	D	N	--	20	A2	20 18
! PARMAS	A	N	07	30		0 0
<no ssid>	A	Y	06	1		0 0
GRXWirelessNetwork	A	Y	06	2		0 0
! SECMAS	A	N	07	13		0 0
<no ssid>	D	N	--	1	A4	1 66
! <Lucent Outdoor Router>	O	N	--	267		267 1

Info  
Ntwrks  
105  
Pkts  
1258  
Cryptd  
Weak  
0  
Noise  
289  
Discrd  
289  
Pkts/s  
50

Elapsed  
000027

Status
Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP Found IP 159.139.90.1 for <no ssid>::00:04:76:BB:A7:04 via ARP Found IP 159.139.120.13 for <no ssid>::00:B0:D0:DE:60:E3 via TCP
Battery: AC charging 100% 0h0m0s

Source: [www.kismetwireless.net](http://www.kismetwireless.net)

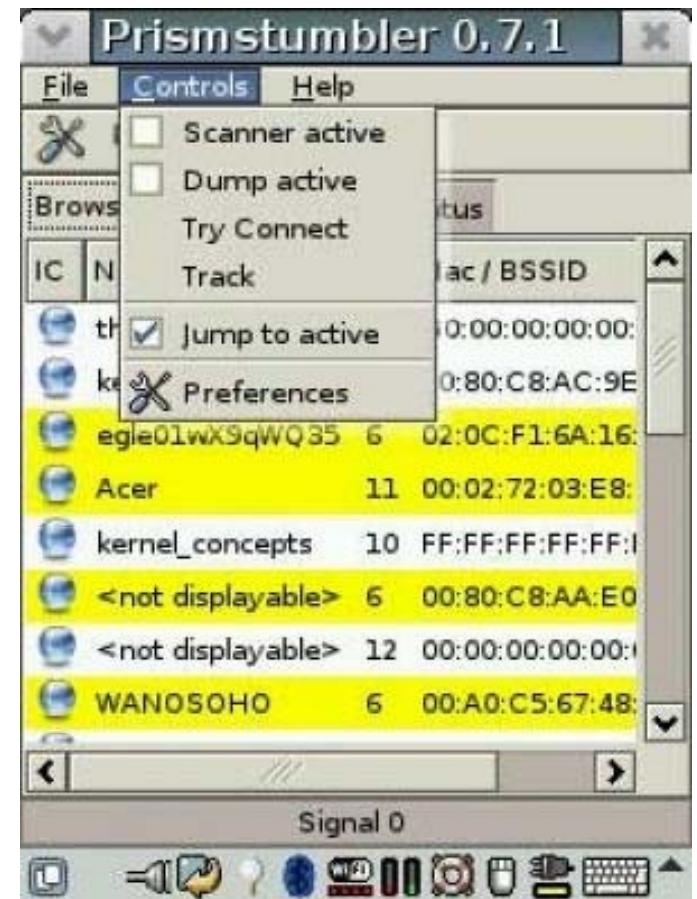
# Scanning Tool: Prismstumbler

Prismstumbler is a wireless LAN (WLAN) that scans for beacon frames from access points

It operates by constantly switching channels and monitors any frames received on the currently selected channel

The program was created by using ideas and codesnippets from prismdump, AirSnort, and Wireshark

Prismstumbler will also find private networks. Because the method used in Prismstumbler is receive only, it can also find networks with weaker signals and discover more networks



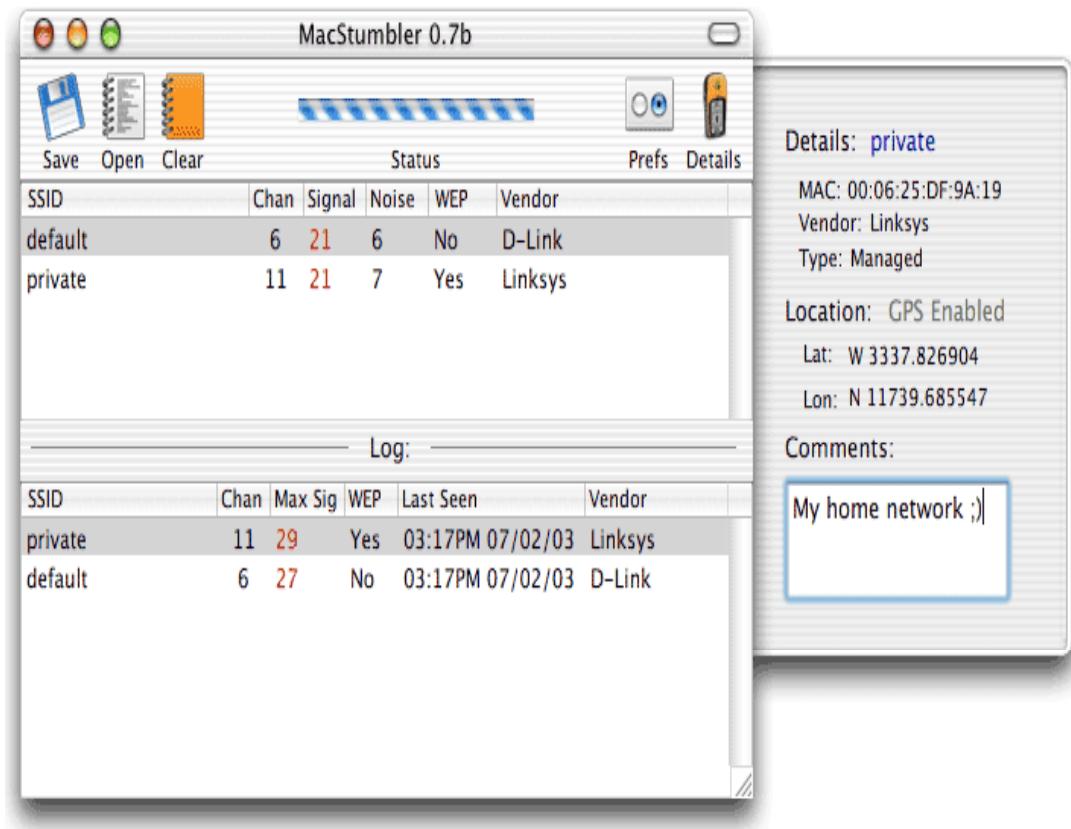
Source: <http://prismstumbler.sourceforge.net/>

# Scanning Tool: MacStumbler

MacStumbler is a utility used to display information about nearby 802.11b and 802.11g wireless access points

It is mainly designed to be a tool to help find access points while traveling or to diagnose wireless network problems

MacStumbler requires an Apple Airport Card and MacOS 10.1 or greater. MacStumbler does not currently support any kind of PCMCIA or USB wireless device



Source: <http://www.macstumbler.com/>

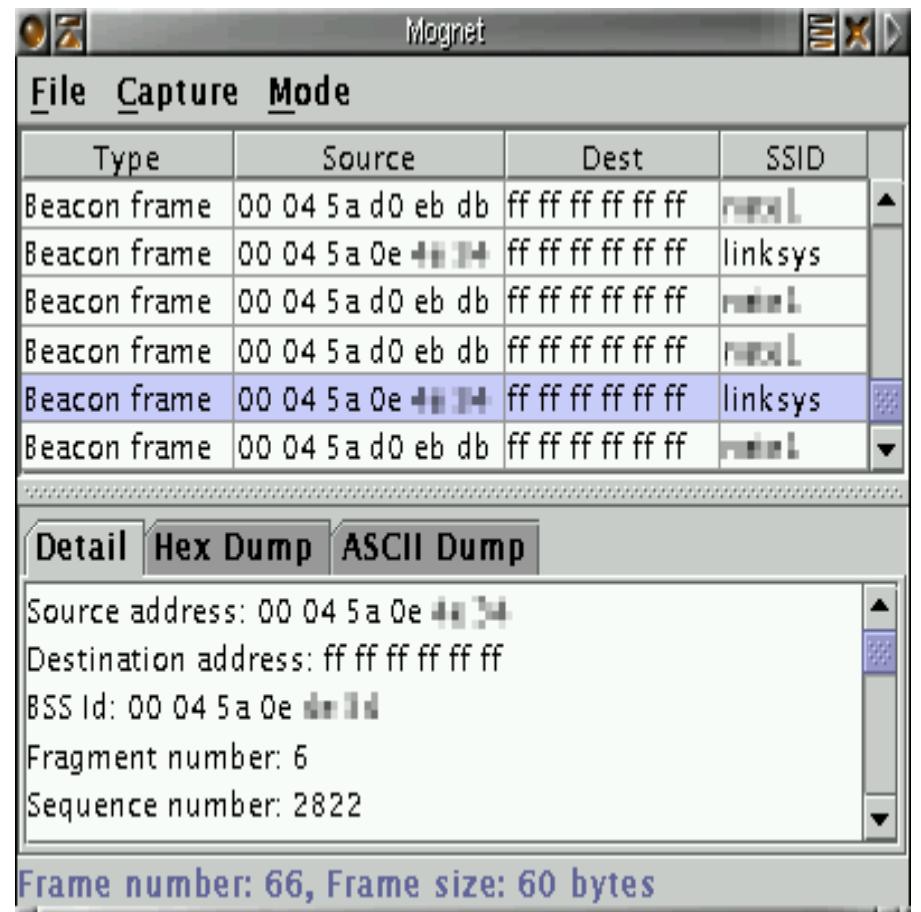
# Scanning Tool: Mognet



Mognet is a simple, lightweight 802.11b sniffer written in Java and available under the GPL

It features real-time capture output, support for all 802.11b generic and frame-specific headers, easy display of frame contents in hex or ASCII, text mode capture for GUI-less devices, and loading/saving capture sessions in libpcap format

Mognet requires a Java Development Kit 1.3 or higher and a working C compiler for native code compilation



Source: <http://www.node99.org/>

# Scanning Tool: WaveStumbler

WaveStumbler is a console-based 802.11 network mapper for Linux

It reports the basic AP information like channel, WEP, ESSID, and MAC

It consists of a patch against the kernel driver, orinoco.c, which makes it possible to send the scan command to the driver via the /proc/hermes/ethX/cmds file

The answer is then sent back via a netlink socket

WaveStumbler listens to this socket and displays the output data on the console

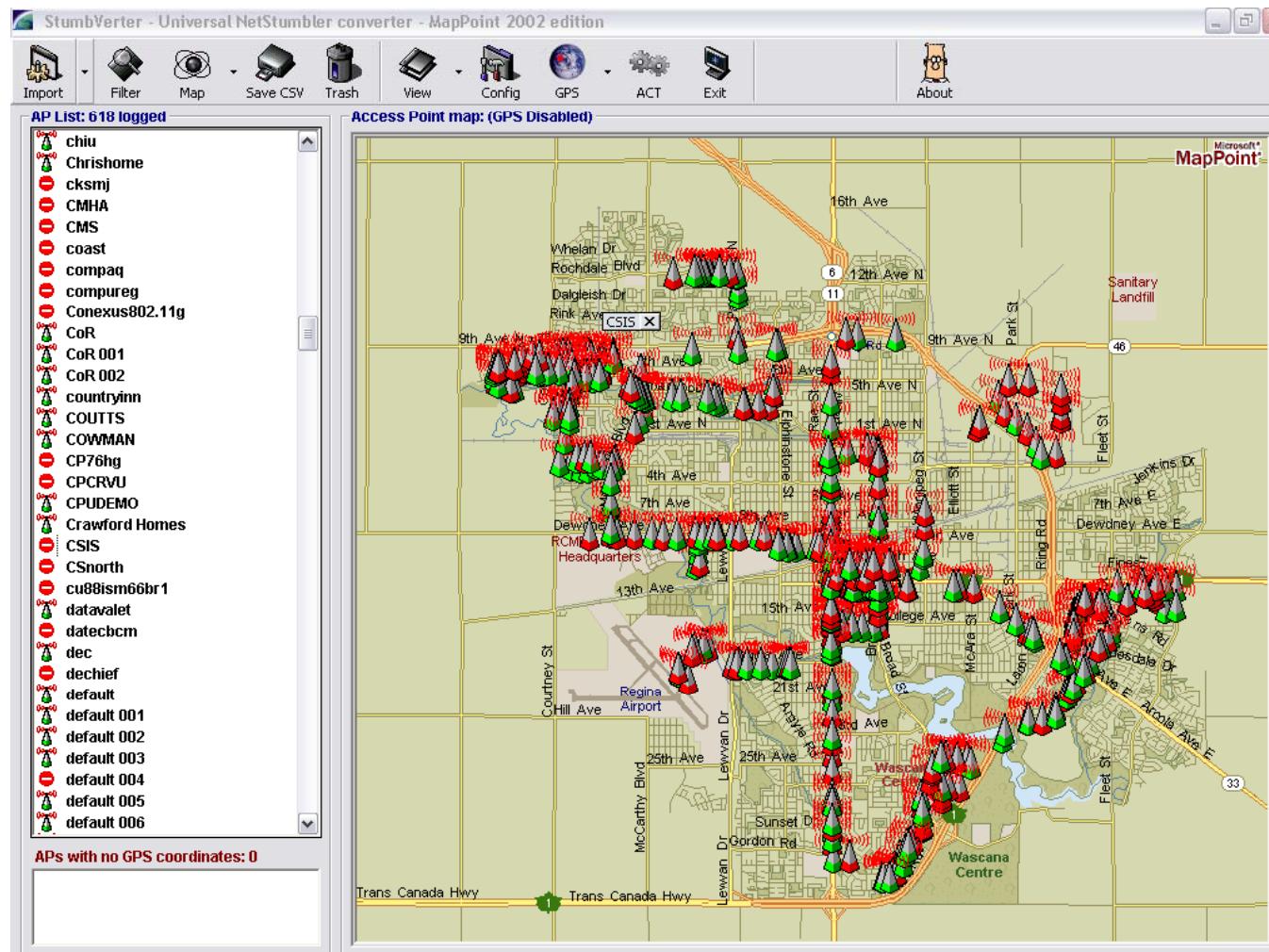


Source: <http://www.cquare.net/>



TM

# Stumbverter: Screenshot



# Scanning Tool: Netchaser for Palm Tops

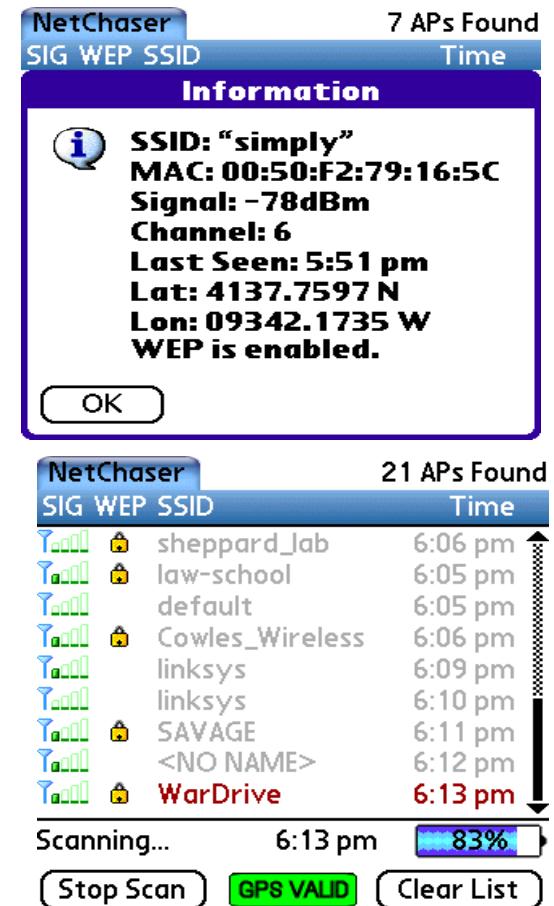
Find and easily connect to WiFi hotspots with your Palm handheld computer

## Access Point Info:

- AP MAC address
- AP SSID
- Signal strength
- Channel
- Loss-of-signal time and date display
- Latitude and longitude of strongest signal

## Full Logging Support:

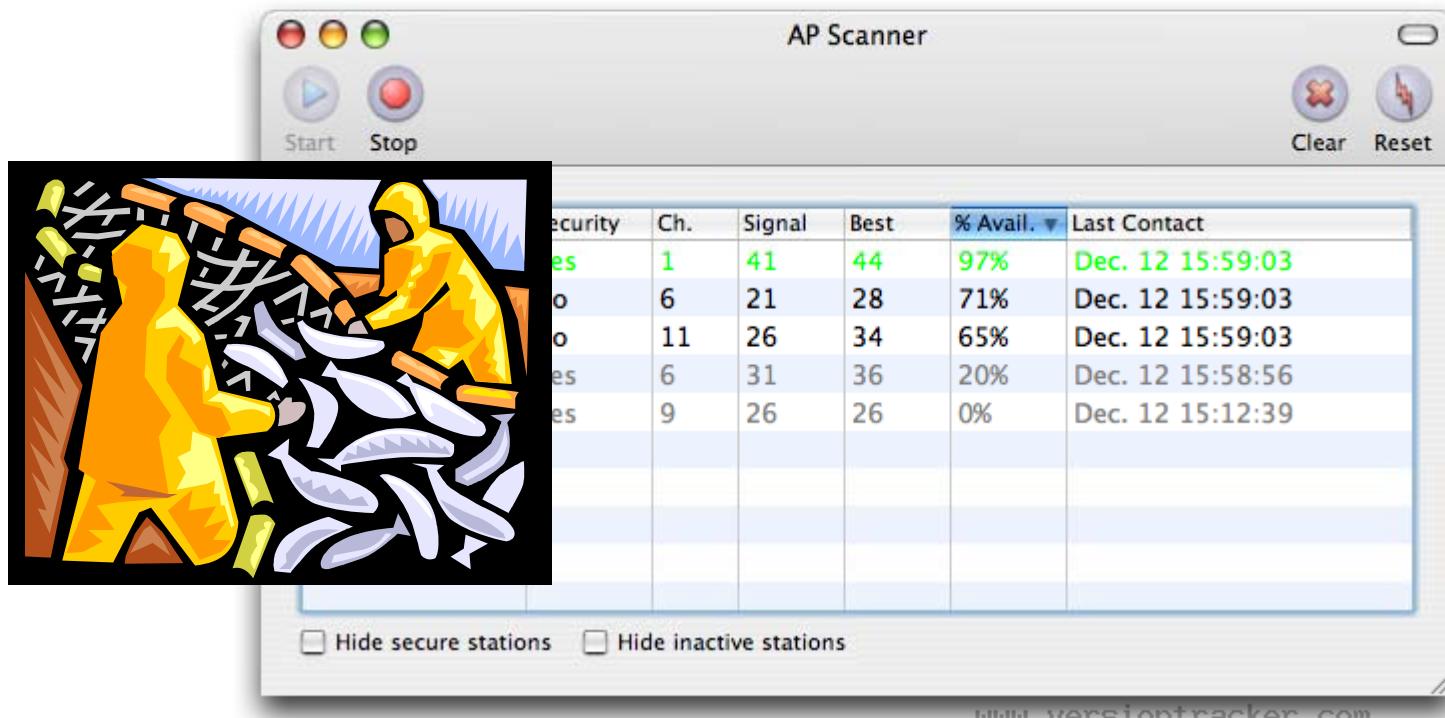
- Log all access point data to a file for post-processing
- CSV standard file suitable for import into any database or spreadsheet



Source: <http://www.bitsnbolts.com/>

# Scanning Tool: AP Scanner

AP Scanner is an application that shows a graph of the channel usage of all open wireless access points within range

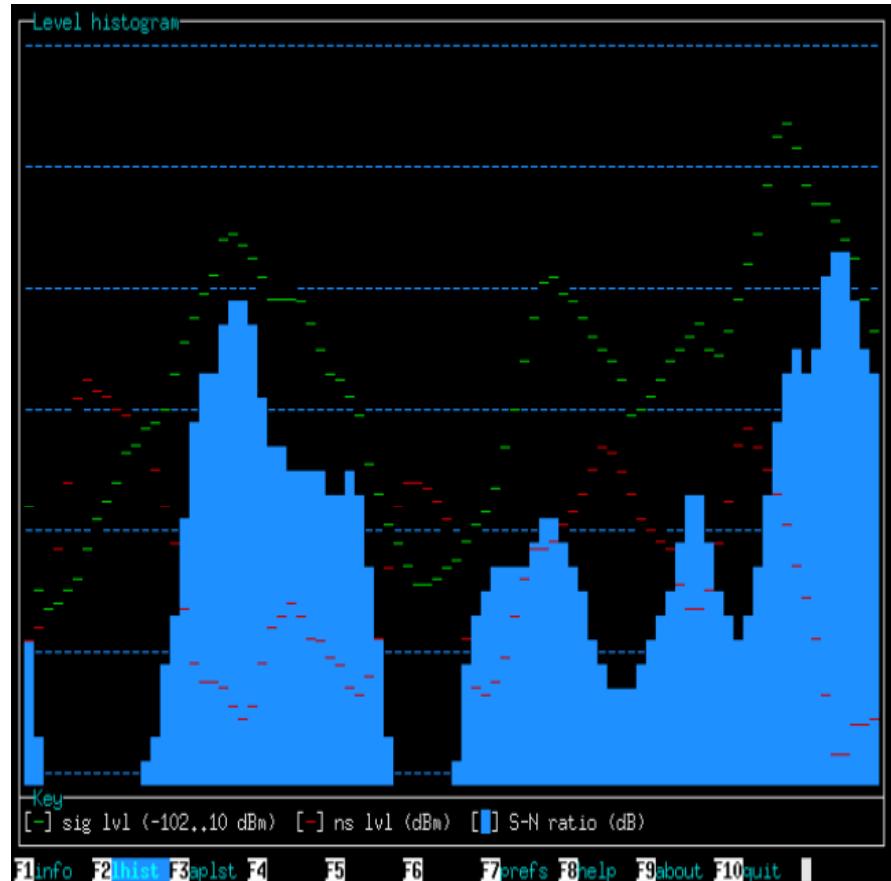


# Scanning Tool: Wavemon

Wavemon is a ncurses-based monitor for wireless devices

Wavemon allows watching of signal and noise levels, packet statistics, device configuration, and network parameters of hardware or a wireless network

It has currently only been tested with the Lucent Orinoco series of cards, although it should work (with varying features) with all devices supported by the wireless kernel extensions written by Jean Tourrilhes



Source: <http://freshmeat.net/>

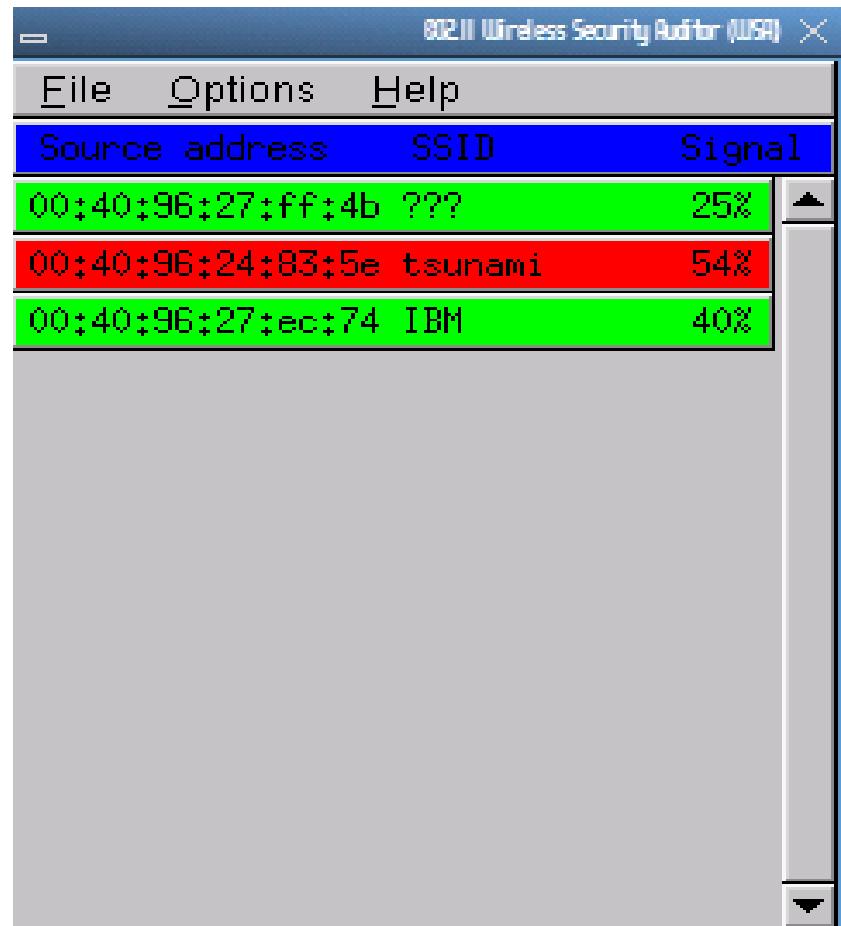
# Scanning Tool: Wireless Security Auditor (WSA)

An IBM research prototype of an 802.11

A wireless LAN security auditor,  
running on Linux or an iPAQ PDA

WSA helps network administrators by  
auditing the wireless network for  
security

Vulnerabilities in the network can be  
discovered before hackers break in the  
network



Source: <http://www.research.ibm.com/>

# Scanning Tool: AirTraf

AirTraf is a wireless sniffer that can detect and determine exactly what is being transmitted over 802.11 wireless networks

It is developed as an open source program

It tracks and identifies legitimate and rogue access points, keeps performance statistics on a by-user and by-protocol basis, measures the signal strength of network components, and more

```

AirTraf: 1.0.0 '02
Channel Scanning: listening using Cisco Aironet (eth1)

-- Activity Overview --
Total Networks: 2
Scan Mode: Complete

-- Detailed Breakdown --
CH TYPE SSID          BSSID      WEP   MGMT  CTRL  DATA  CRYPT  SIGNAL
01 AP Command Center  0006257d8777  open    136    0     9    0    0,0
08 AP WaveLAN Network 00022d28dc25  open    514    0    23    0    0,0

-- Channel APs Packets --
01 1 145
02 0 0
03 0 0
04 0 0
05 0 0
06 0 0
07 0 0
08 1 537
09 0 0
10 0 0
11 0 0
12 0 0
13 0 0
14 0 0

-- End --

-- Current Status --
Performing Initial Channel Scan...
Detected new network 'Command Center' (0006257d8777) on Channel 01.
Detected new network 'WaveLAN Network' (00022d28dc25) on Channel 08.
Initial Channel Scan Complete!
Entering Continuous Scan Mode...

Elapsed: 00:00:41

F-force new scan Up/Down/PgUp/PgDn=scroll window X=exit

```

Source: [www.elixar.com](http://www.elixar.com)

# Scanning Tool: WiFi Finder

WiFi Finder checks for 802.11b and 802.11g signals without a computer or PDA

The user interface consists of a single button and three LEDs that indicate available signal strength



Source: <http://www.kensington.com/>

Copyright © by **EC-Council**  
All Rights Reserved. Reproduction is Strictly Prohibited

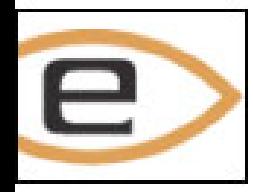
# Scanning Tool: WifiScanner

WifiScanner is designed to discover wireless node

It dumps the traffic in realtime and the sniffed channels can be changed



# WifiScanner: Screenshot



eEye Retina WiFi does not scan your eye, but it does scan the area and detects the presence of wireless devices located within a network or connected wirelessly to the network

This tool detects rogue mobile devices and transmitting laptops

eEye's Retina WiFi Scanner enables a company to ensure their customers' networks are secure





TM

# eEye Retina WiFi: Screenshot 1

The screenshot shows the 'Retina Network Security Scanner' application window. The menu bar includes File, View, Tools, and Help. The toolbar contains icons for New Scan, Open Scan, Save Scan, Print, and Help. The main interface has tabs for Discover and Report, with Discover selected. On the left, a sidebar titled 'Help and Support' lists Help Topics, eEye Web Site, Technical Support, and About Retina WiFi Scanner. The central area is divided into sections for Actions and Detected Devices.

**Actions:**

- WiFi Options:
  - Wep Key Brute forcing attack
  - Sound
  - Debug
  - Dump
- Probing interval: 1000 msec
- RSSI threshold for IP discovery: -65 msec

**Detected Devices:**

- AP MAC
- Vendor
- WEP
- Rates
- Standard
- RSSI
- Channel
- Network Type
- Mode
- Beacon Period
- ATIM Window
- DHCP
- DHCP MAC
- DNS
- Gateway
- Applied IP
- AP TP

Copyright © 2004 eEye Digital Security All right Reserved.

**eEye® Digital Security**



TM

# eEye Retina WiFi: Screenshot 2

The screenshot shows the eEye Retina Network Security Scanner application window. On the left, there's a sidebar with 'Help and Support' links: Help Topics, eEye Web Site, Technical Support, and About Retina WiFi Scanner. The main menu bar includes File, View, Tools, and Help. Below the menu is a toolbar with icons for file operations like Open, Save, Print, and Help.

A 'Discover' tab is selected in the top navigation bar. A 'Filter' dialog box is open in the center, titled 'Filter'. It contains three sections: 'Infrastructure Mode' (IBSS is unchecked, Infrastructure is checked), 'Standard' (802.11b, 802.11a, 802.11g, Other are checked), and 'WEP' (Enabled and Disabled are checked). At the bottom of the dialog are 'OK' and 'Cancel' buttons.

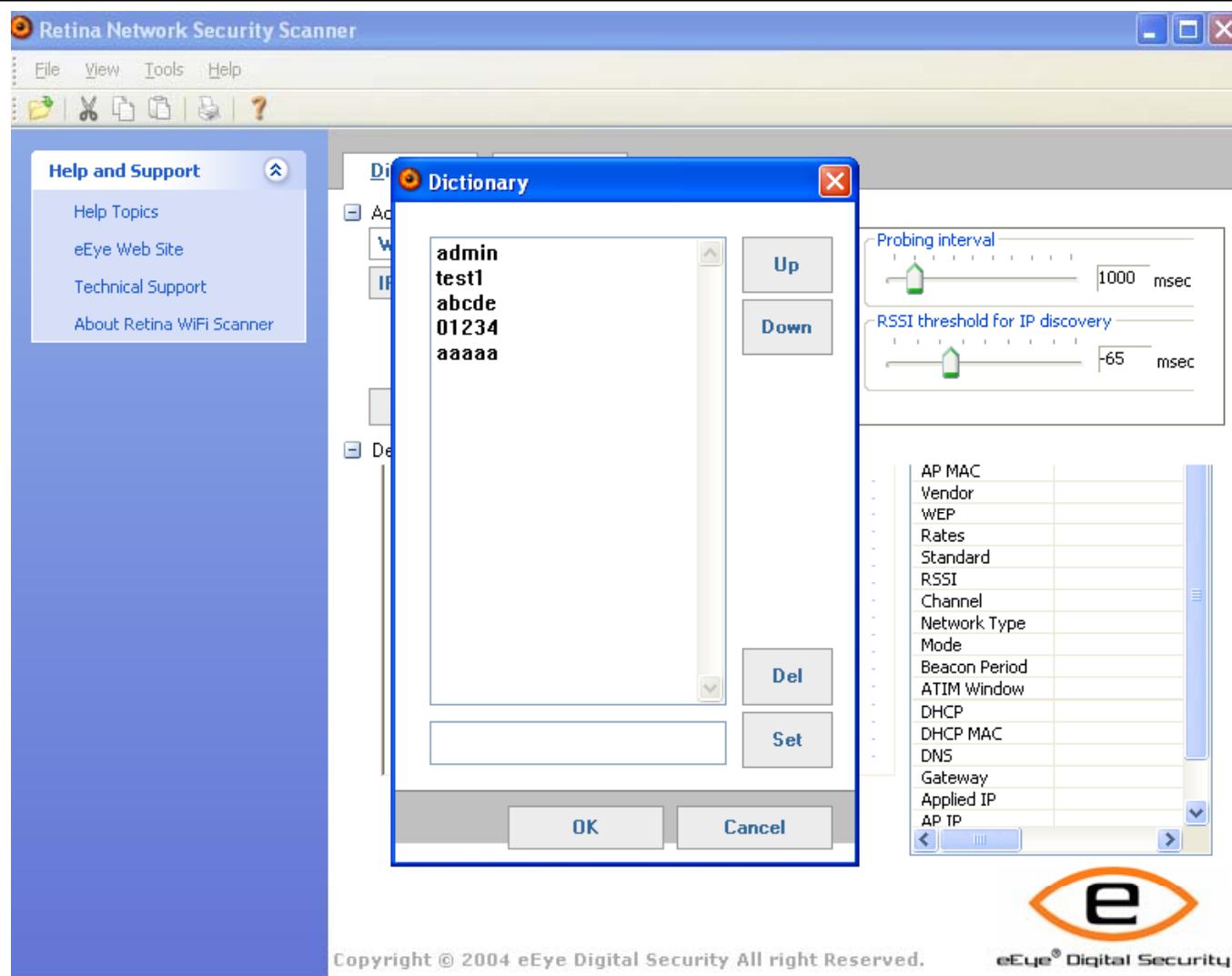
To the right of the filter dialog, there are several configuration sliders: 'Probing interval' set to 1000 msec, 'RSSI threshold for IP discovery' set to -65 msec, and a vertical list of other parameters like AP MAC, Vendor, WEP, Rates, Standard, RSSI, Channel, Network Type, Mode, Beacon Period, ATIM Window, DHCP, DHCP MAC, DNS, Gateway, Applied IP, AP TP, and a scroll bar.

At the bottom of the application window, it says 'Copyright © 2004 eEye Digital Security All rights Reserved.' and features the eEye Digital Security logo, which consists of a stylized 'e' inside an orange oval.



TM

# eEye Retina WiFi: Screenshot 3





TM

# Simple Wireless Scanner

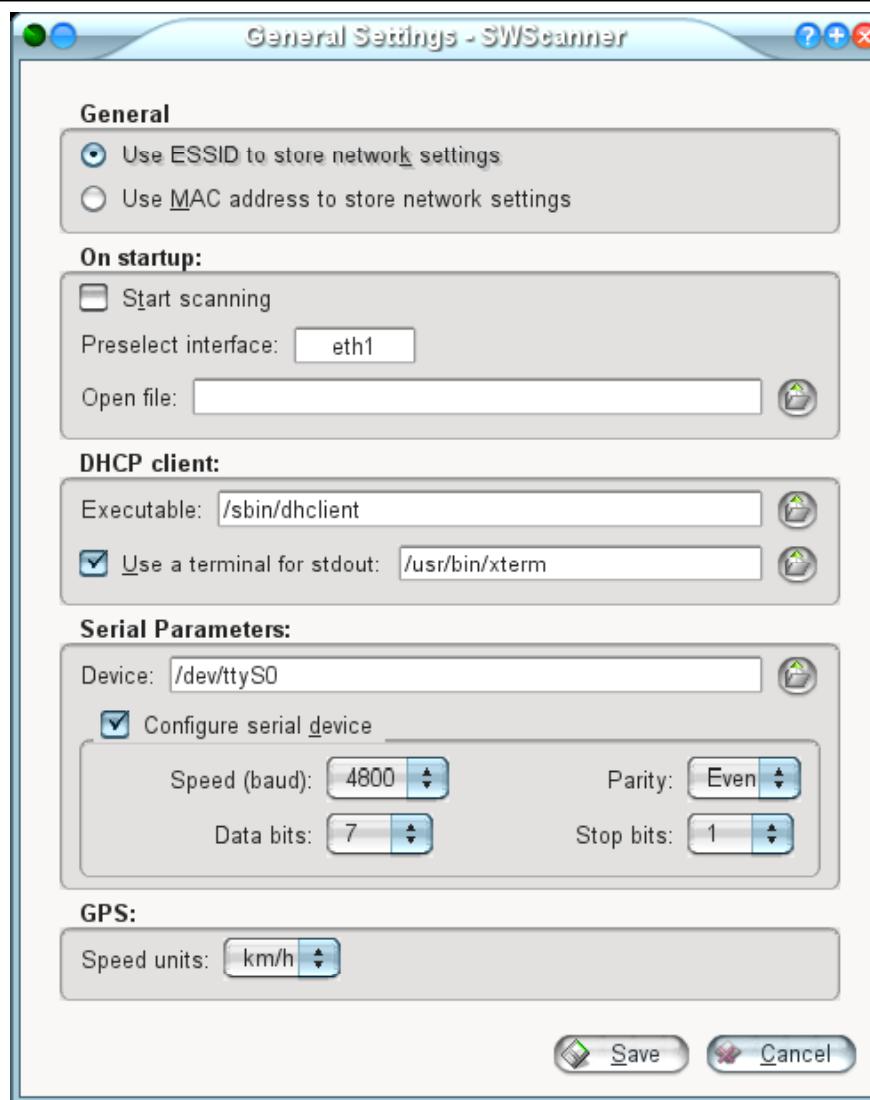
Simple Wireless Scanner (SWScanner) is an application for Linux environments designed for scanning, configuring, and managing wireless networks

SWScanner is a wardriving tool, and has a high level of compatibility with NetStumbler

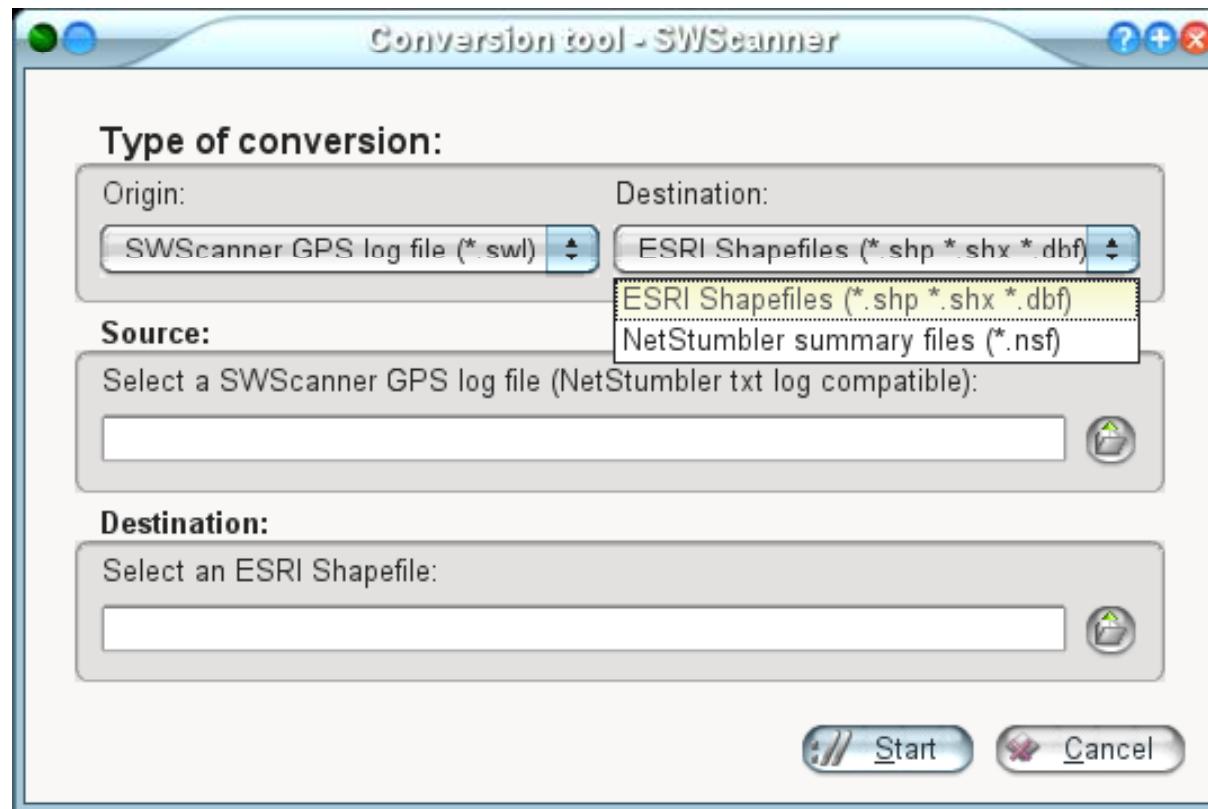
## Features:

- SWScanner uses wireless-extensions
- Has detailed and updated information of signal, noise, and other wireless network parameters of the selected interface
- Has GPS integration
- Has the possibility of storing network settings of the detected access points
- It simplifies the associating/deassociating process to an access point
- Has possibility of storing scanned data
- It simplifies wardriving
- Compatible log data between NetStumbler and SWScanner; i.e.: it is possible to open a text or summary file produced with NS. NS will also recognize log files produced by SWScanner
- Conversion of log (text or summary) files (from NS or SWScanner) to the well-known widely used ESRI Shapefile format

# Simple Wireless Scanner: Screenshot 1



# Simple Wireless Scanner: Screenshot 2





TM

# Simple Wireless Scanner: Screenshot 3

Simple Wireless Scanner - SWScanner

File Edit View Actions Tools Settings Help

Show all AccessPoints Using sound Choose interface: eth1 Scanning interval: 1 secs.

Filter /

CHANNEL

- 1
- 10
- 11
- 12
- 13
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9

ESSID

MAC

WEP

- NO
- YES

(ON)	ESSID	MAC	VENDOR	WEP	CHANNEL
WiForcada	00:12:17:DE:17:BC	CISCO-LINKSYS, LLC	NO	6	
000740DE13BF	00:07:40:A2:84:BD	MELCO INC.	YES	11	
1460064285	00:01:36:0C:31:65	CYBERTAN TECHNOLOGY, INC.	YES	5	
2A	00:0A:79:0F:44:F8	COREGA K.K.	NO	6	
3Com	00:12:A9:0A:B4:BC	3COM EUROPE LTD.	NO	11	
3Com	00:12:A9:0D:0D:C0	3COM EUROPE LTD.	NO	11	
3Com	00:12:A9:C7:B7:1C	3COM EUROPE LTD.	NO	11	
3Com	00:12:A9:C7:BB:CC	3COM EUROPE LTD.	NO	11	
3Com	00:14:7C:43:AC:36	3COM EUROPE LTD.	NO	5	
ALVAREZ	00:60:B3:D6:60:1A	Z-COM, INC.	YES	2	
ARRANZ	00:60:B3:D3:DF:8A	Z-COM, INC.	NO	9	
banservices	00:04:E2:E6:6D:D6	SMC NETWORKS, INC.	YES	11	
BARRAKA	00:0D:54:A1:D5:F5	3COM EUROPE LTD	NO	11	
belkin54g	00:11:50:8C:6A:82	BELKIN CORPORATION	NO	1	
Bodegon	00:13:49:1A:06:C2	ZYXEL COMMUNICATIONS CORPORATION NO	11		
Comtrend	00:03:C9:8C:C7:F6	TECOM CO. LTD	NO	11	

Statistics

WEP

ON	58
OFF	58

CHANNEL

1	25
2	4
3	11
4	1
5	3
6	21
7	3
8	4
9	13
10	2
11	23
12	1
13	5

AccessPoints in list: shown (116), active (1), total (116)

Status (eth1)

IP: 0.0.0.0 Netmask: 0.0.0.0 Broadcast: 0.0.0.0

Mode: Managed ESSID: WiForcada Channel: 6 WEP: NO KeyLength: -

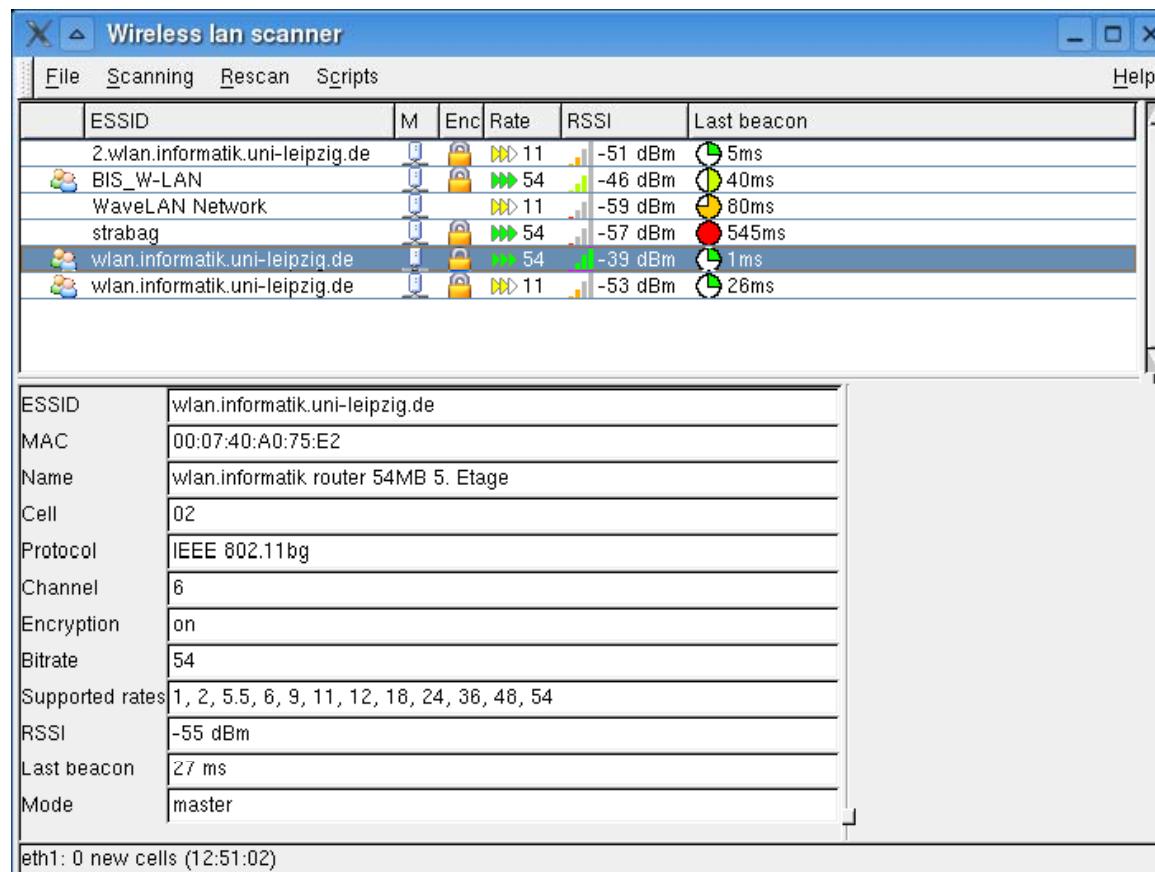
Signal: -68 Noise: -32 Link Qual: 221 AP: 00:12:17:DE:17:BC

GPS

Start GPS

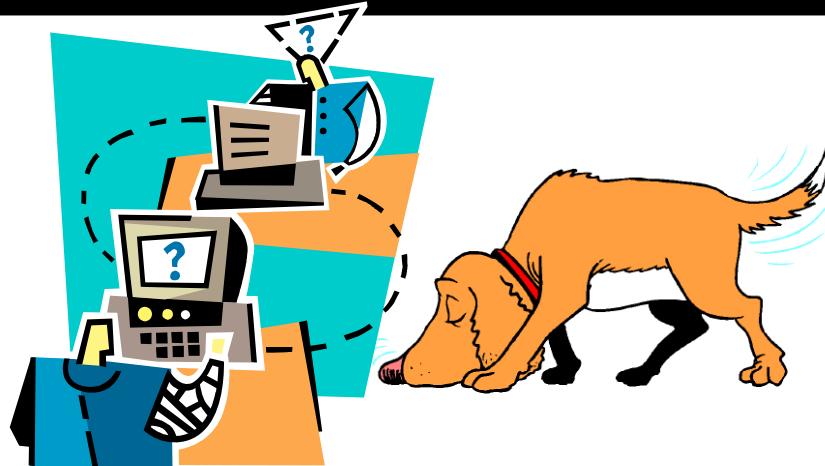
Lat(deg): 0,0000000000 Long(deg): 0,0000000000 Speed (km/h): 0 AP's 0

Lists available networks, with data like signal strength, encryption status, and connection speed



Certified Ethical Hacker

TM



# Sniffing Tools



# Sniffing Tools

- AiroPeek
- NAI Wireless Sniffer
- WireShark
- VPNmonitorl
- Aerosol
- vxSniffer
- EtherPEG
- DriftNet
- WinDump
- ssidsniff





TM

# Sniffing Tool: AiroPeek

A wireless management tool needed to deploy, secure, and troubleshoot the wireless LAN

It covers the whole wireless LAN management, including site surveys, security assessments, client troubleshooting, WLAN monitoring, remote WLAN analysis, and application layer protocol analysis

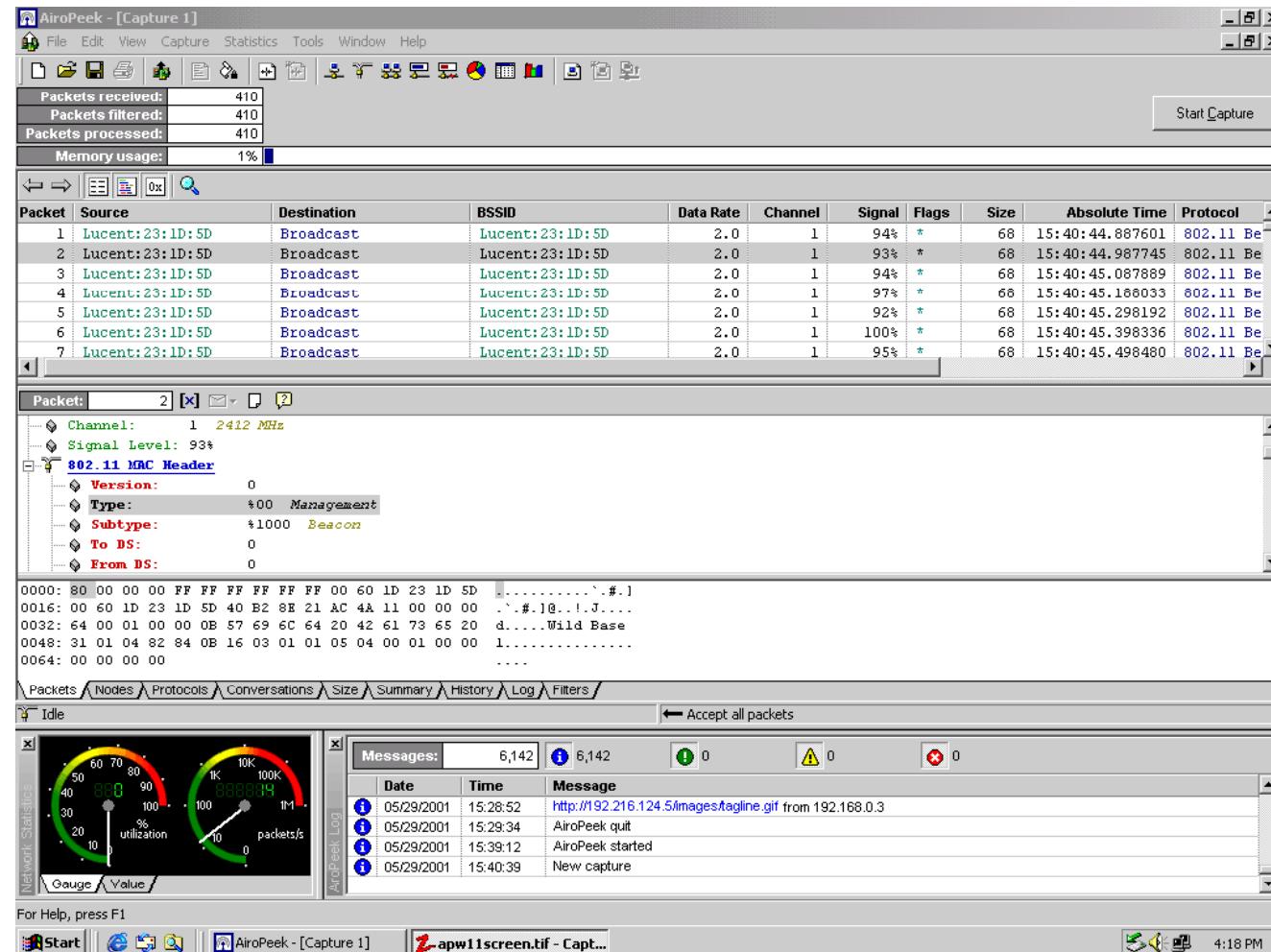
It has an enhanced analysis of VoIP

Source: <http://www.wildpackets.com/>

Copyright © by **EC-Council**  
All Rights Reserved. Reproduction is Strictly Prohibited



# AiroPeek: Screenshot

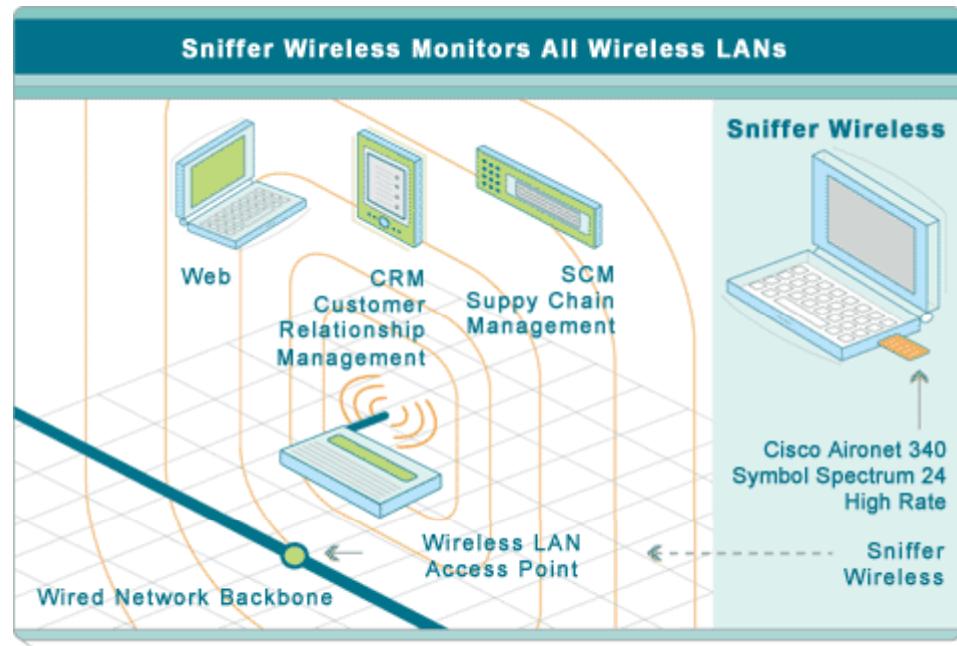


# Sniffing Tool: NAI Wireless Sniffer

NAI Wireless Sniffer is developed by Network Associates, Inc

It is used for rogue mobile unit detection

It gathers a list of all the wireless devices, whether they are access units or mobile devices, and labels them as such

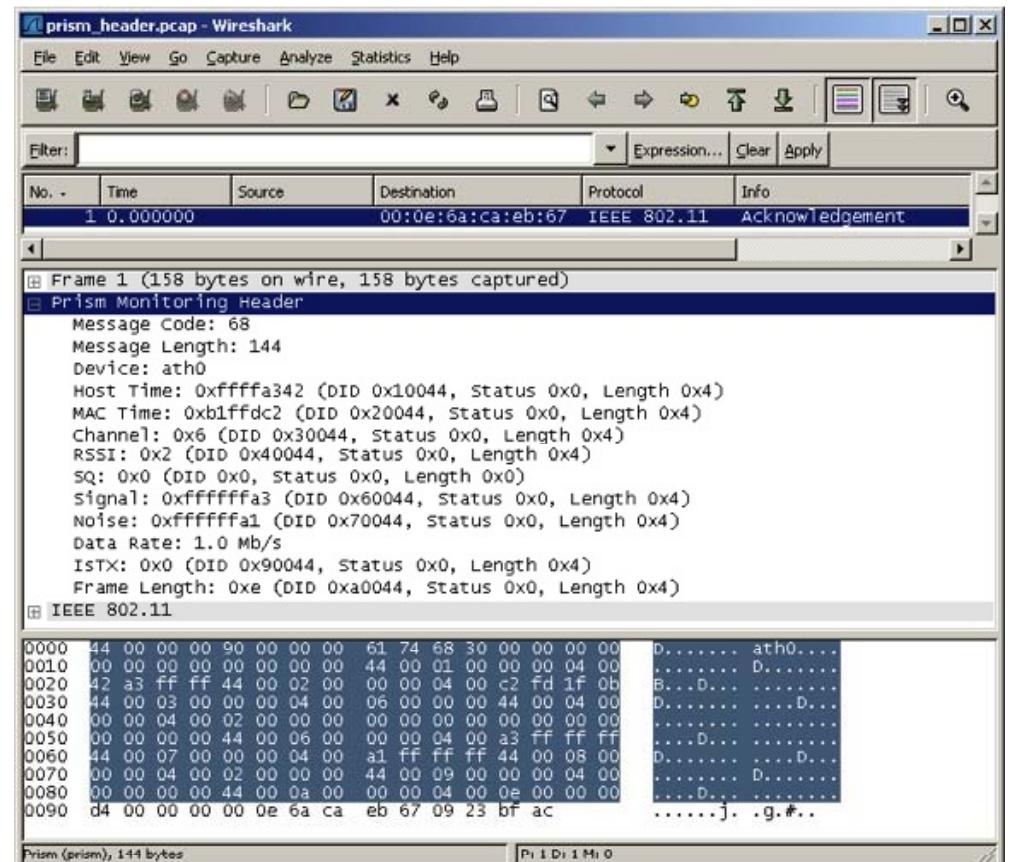


# MAC Sniffing Tool: Wireshark

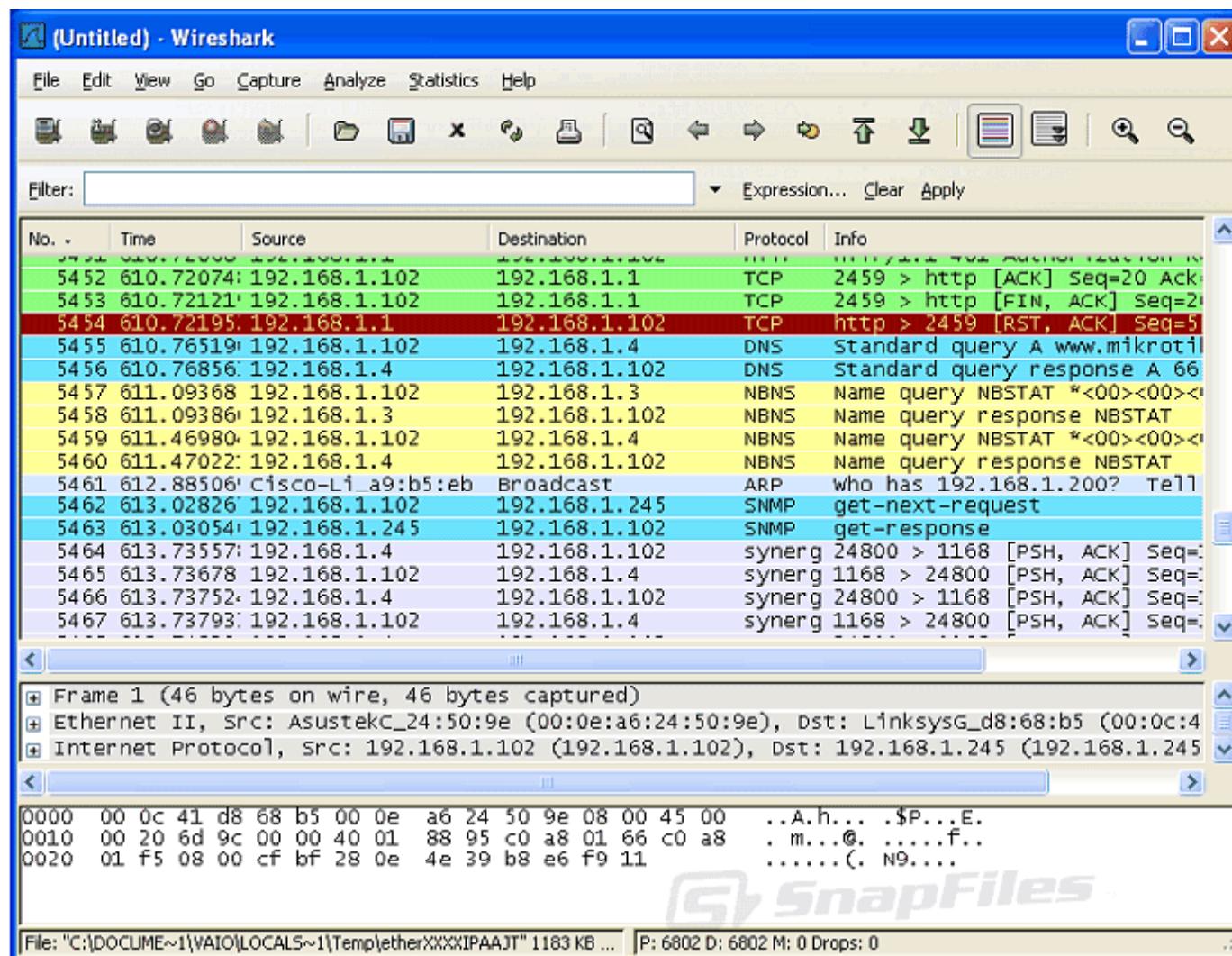
WireShark is a free network protocol analyzer for Unix and Windows

It allows examination of data from a live network or from a captured file on disk

It has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session



# WireShark: Screenshot



SnapFiles

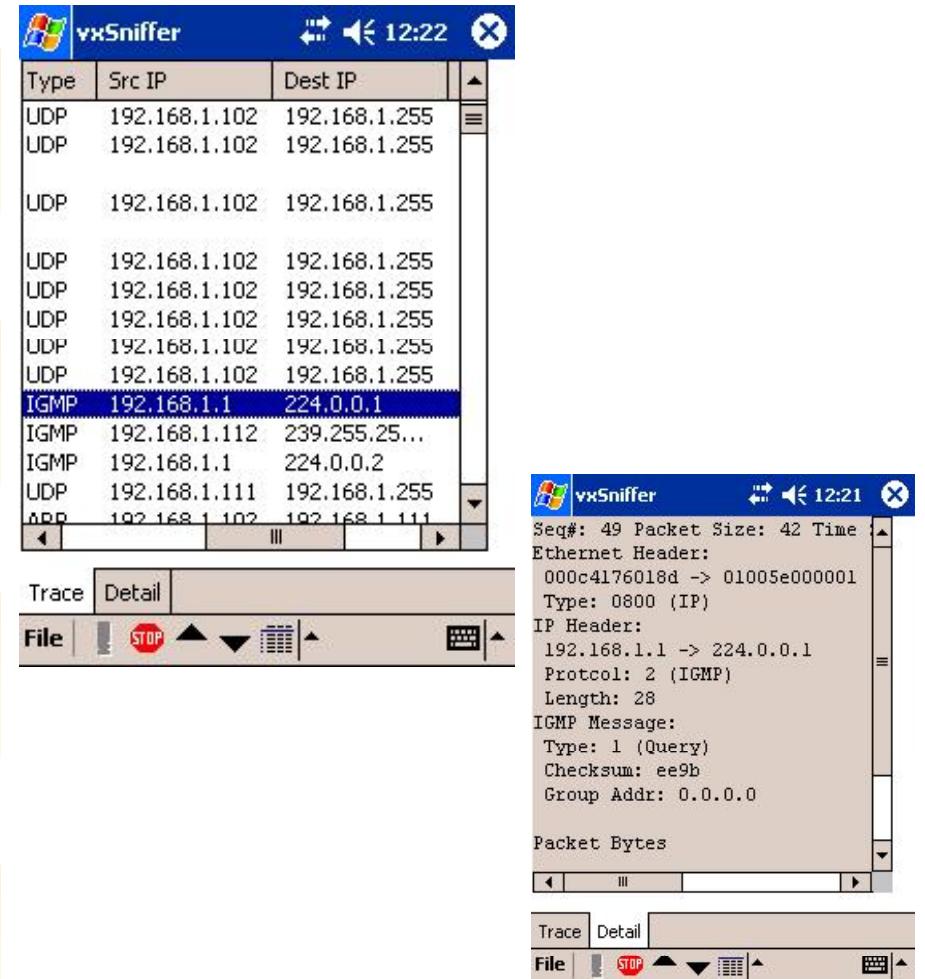
# Sniffing Tool: vxSniffer

vxSniffer is a complete network monitoring tool for Windows CE-based devices

It operates on all handheld 2000 HPCs, pocket PCs, Pocket PC 2002s, and Windows Mobile 2003s

It requires an Ethernet adapter with an NDIS-compatible driver

vxSniffer is a licensed software



Source: <http://www.cam.com/vxSniffer.html>

# Sniffing Tool: Etherpeg

Etherpeg watches the local network for traffic, reassembles out-of-order TCP streams, and scans the result for data that looks like a GIF or JPEG

It is a simple but effective hack that indiscriminately shows all image data that it can assemble

The source code is freely available and compiles easily with a simple make from the terminal window



Source: <http://www.etherpeg.org/>

# Etherpeg: Screenshot

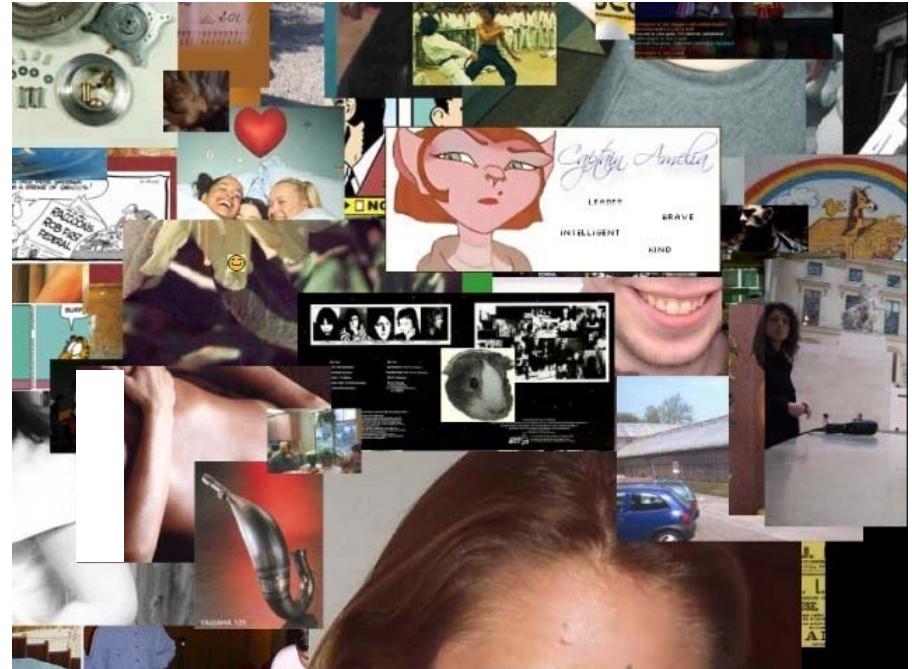


# Sniffing Tool: Drifnet

Drifnet is based on the lines of EtherPEG

It is a program that listens to network traffic and picks out images from TCP streams it observes

In the beta version, driftnet picks out MPEG audio streams from network traffic and tries to play them



# Sniffing Tool: AirMagnet

AirMagnet v1.2 is a new tool from AirMagnet

It is similar to MiniStumbler, except it has a GPS option

This tool is used not only for sniffing out wireless networks, but for the deployment and administration of WLANs in organizations

It uses many levels of graphics and animations to display real-time statistics of WLANs in the area

It not only displays the unsecured networks, but also gives a list of possible security holes and configuration problems with WLANs in the area

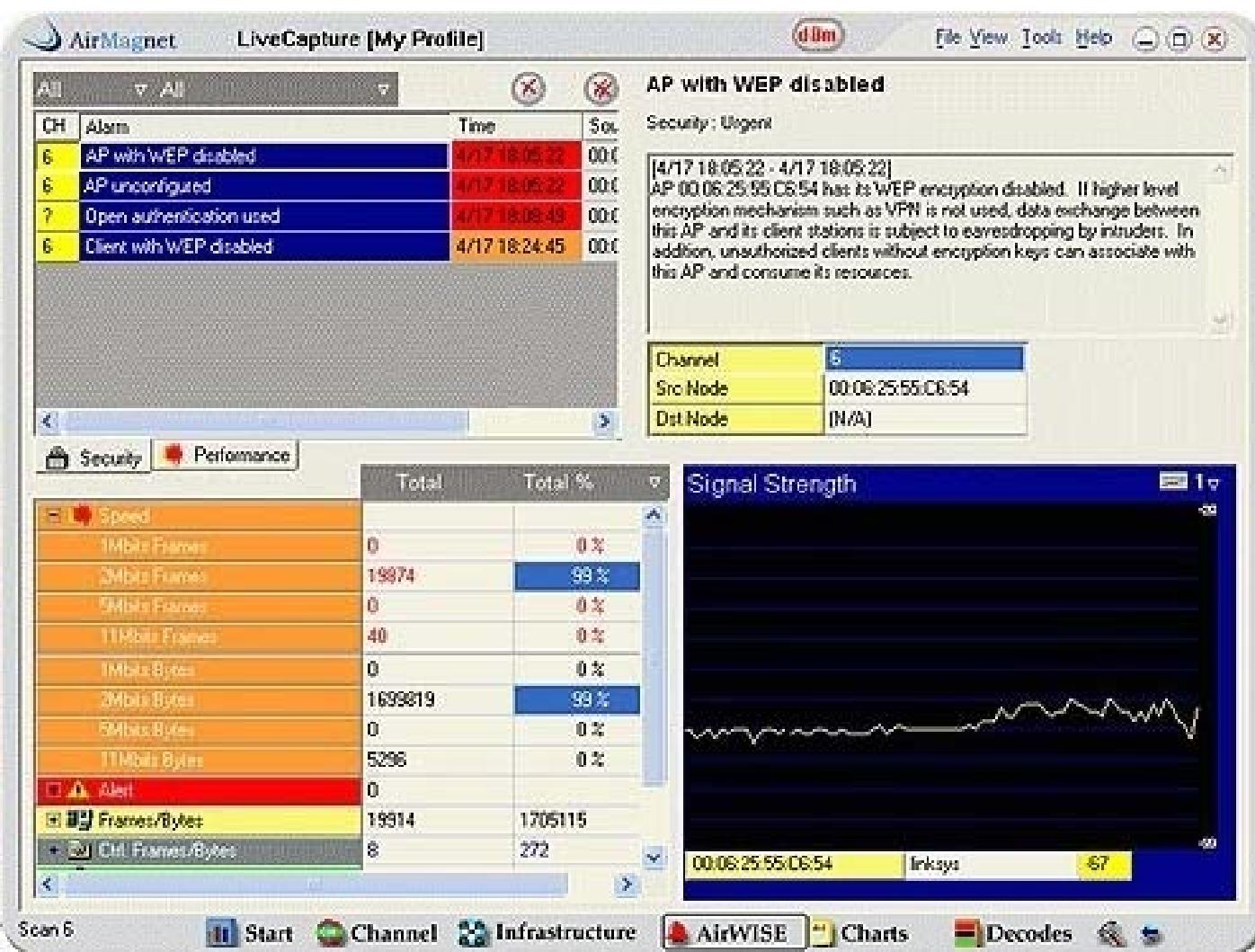


Source: <http://www.airmagnet.com>



TM

# AirMagnet: Screenshot



# Sniffing Tool: WinDump

WinDump is the porting to the Windows platform of tcpdump; the most used network sniffer/analyzer for UNIX

It is fully compatible with tcpdump and can be used to watch and diagnose network traffic according to various complex rules



```
C:\>windump -i 1 -qnt dst host 192.168.4.3 and not port 8080 and proto UDP
windump: listening on \Device\NPF_{DEB64C05-DEE8-4B4B-8783-2C3FE6BA847F}
IP 192.168.4.15.2770 > 192.168.4.3.514: udp 118
IP 192.168.4.15.2775 > 192.168.4.3.514: udp 114
IP 192.168.4.15.2776 > 192.168.4.3.514: udp 161
IP 192.168.4.15.2784 > 192.168.4.3.514: udp 114
IP 192.168.4.15.2785 > 192.168.4.3.514: udp 162
IP 192.168.4.15.2786 > 192.168.4.3.514: udp 160
IP 192.168.4.15.2788 > 192.168.4.3.514: udp 116
IP 192.168.4.15.2798 > 192.168.4.3.514: udp 114
```

# WinDump: Screenshot

The screenshot shows a Windows application window titled "WINDUMP". The window has a toolbar with various icons at the top. Below the toolbar is a menu bar with "Auto" selected. The main area of the window displays a command-line interface for the WinDump tool. The output shows the version information and usage instructions for WinDump, followed by a list of network traffic captures. The traffic list includes source and destination IP addresses, ports, sequence numbers, and timestamps.

```
E:\test>WinDump.exe -h
E:\TEST\WINDUMP.EXE version 2.02, based on TCPdump version 3.4a6
libpcap for Windows version 2.02, based on libpcap version 0.4a6
Usage: E:\TEST\WINDUMP.EXE [-adDeflnNOpPqStvx] [-B size] [-c count] [-E driver_requests]
          [-F file]
          [-i interface] [-r file] [-s snaplen]
          [-T type] [-w file] [expression]

E:\test>windump
E:\TEST\WINDUMP.EXE: listening on PPPMAC
18:18:23.779656 ip-20.dialup.dux.ru.1051 > clusterb.icq.com.80: S 71369136:71369
136<0> win 8760 <mss 536,nop,nop,sackOK> <DF>
18:18:23.794251 ip-20.dialup.dux.ru.1052 > cache.dux.ru.53: 1+ <45>
18:18:23.816884 clusterb.icq.com.80 > ip-20.dialup.dux.ru.1043: R 1877700023:187
7700023<0> win 65392 <DF>
18:18:23.844128 clusterb.icq.com.80 > ip-20.dialup.dux.ru.1044: R 2415370996:241
5370996<0> win 65392 <DF>
18:18:23.857039 clusterb.icq.com.80 > ip-20.dialup.dux.ru.1046: R 992010446:9920
10446<0> win 65392 <DF>
18:18:23.864846 clusterb.icq.com.80 > ip-20.dialup.dux.ru.1045: R 1878130955:187
8130955<0> win 65392 <DF>
18:18:23.889606 ads.web.aol.com.80 > ip-20.dialup.dux.ru.1041: R 1550904322:1550
904322<0> win 0 <DF>
18:18:24.0604
```

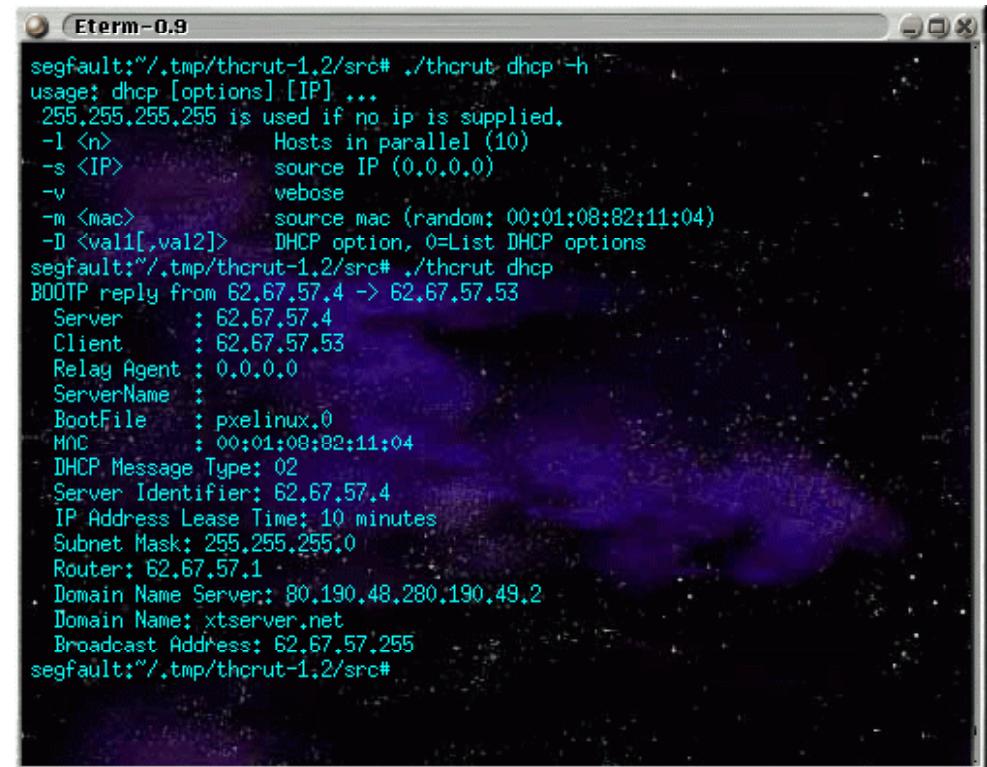


# Multiuse Tool: THC-RUT

THC-RU gathers information from local and remote networks

It offers a wide range of network discovery tools: arp lookup on an IP range, spoofed DHCP request, RARP, BOOTP, ICMP-ping, ICMP address mask request, OS fingerprints, and high-speed host discovery

THC-RUT comes with a new OS fingerprint implementation



The screenshot shows a terminal window titled "Eterm - 0.9". The command entered is "dhcpc [options] [IP] ...". The output provides usage information for the dhcpc command, including options for parallel hosts (-l <n>), source IP (-s <IP>), verbosity (-v), source mac (-m <mac>), and DHCP options (-D <val1[,val2]>). It then shows a sample interaction where a BOOTP reply is received from 62.67.57.4, followed by detailed DHCP configuration parameters such as Server, Client, Relay Agent, ServerName, BootFile, MAC, and various lease times and subnet masks.

```
segfault:"/.tmp/therut-1.2/src# ./therut dhcp -h
usage: dhcpc [options] [IP] ...
255.255.255.255 is used if no ip is supplied.
-l <n>           Hosts in parallel (10)
-s <IP>          source IP (0.0.0.0)
-v               verbose
-m <mac>         source mac (random: 00:01:08:82:11:04)
-D <val1[,val2]>  DHCP option, 0=List DHCP options
segfault:"/.tmp/therut-1.2/src# ./therut dhcp
BOOTP reply from 62.67.57.4 -> 62.67.57.53
  Server      : 62.67.57.4
  Client      : 62.67.57.53
  Relay Agent : 0.0.0.0
  ServerName  :
  BootFile   : pxelinux.0
  MAC        : 00:01:08:82:11:04
  DHCP Message Type: 02
  Server Identifier: 62.67.57.4
  IP Address Lease Time: 10 minutes
  Subnet Mask: 255.255.255.0
  Router: 62.67.57.1
  Domain Name Server: 80.190.48.280.190.49.2
  Domain Name: xtserver.net
  Broadcast Address: 62.67.57.255
segfault:"/.tmp/therut-1.2/src#
```

Source: <http://www.thc.org/thc-rut/>

# Tool: WinPcap

WinPcap is a free public system for direct network access under Windows

Most networking applications access the network through widely used system primitives, such as sockets

This approach allows easy transfer of data on a network, because the OS copes with low-level details (protocol handling, flow reassembly, and so on) and provides an interface similar to the one used to read and write on a file

WinPcap can be used by different kind of tools for network analysis, troubleshooting, security, and monitoring



Source: <http://winpcap.mirror.WireShark.com/>

Copyright © by **EC-Council**  
All Rights Reserved. Reproduction is Strictly Prohibited

# Tool: AirPcap

AirPcap enables troubleshooting tools like Wireshark (formerly WireShark) and WinDump to provide information about the wireless protocols and radio signals

It is the first open, affordable, and easy to deploy WLAN (802.11b/g) packet capture solution for the Windows platform

It comes as a USB 2.0 adapter, and it has been fully integrated with WinPcap and Wireshark

It enables you to capture and analyze:

- 802.11b/g wireless traffic
- Control frames
- Management frames
- Power information

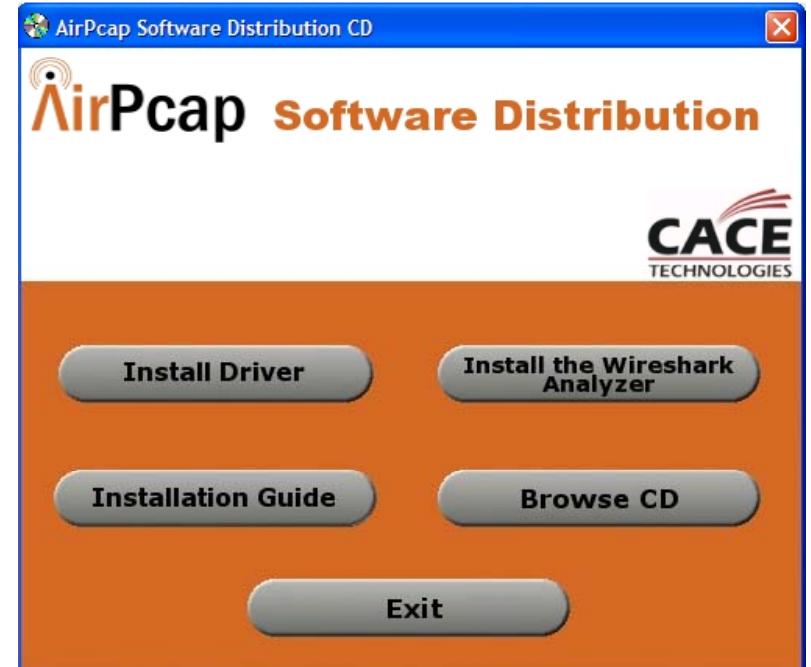


Source: <http://www.cacetech.com/>

# Tool: AirPcap

## Features:

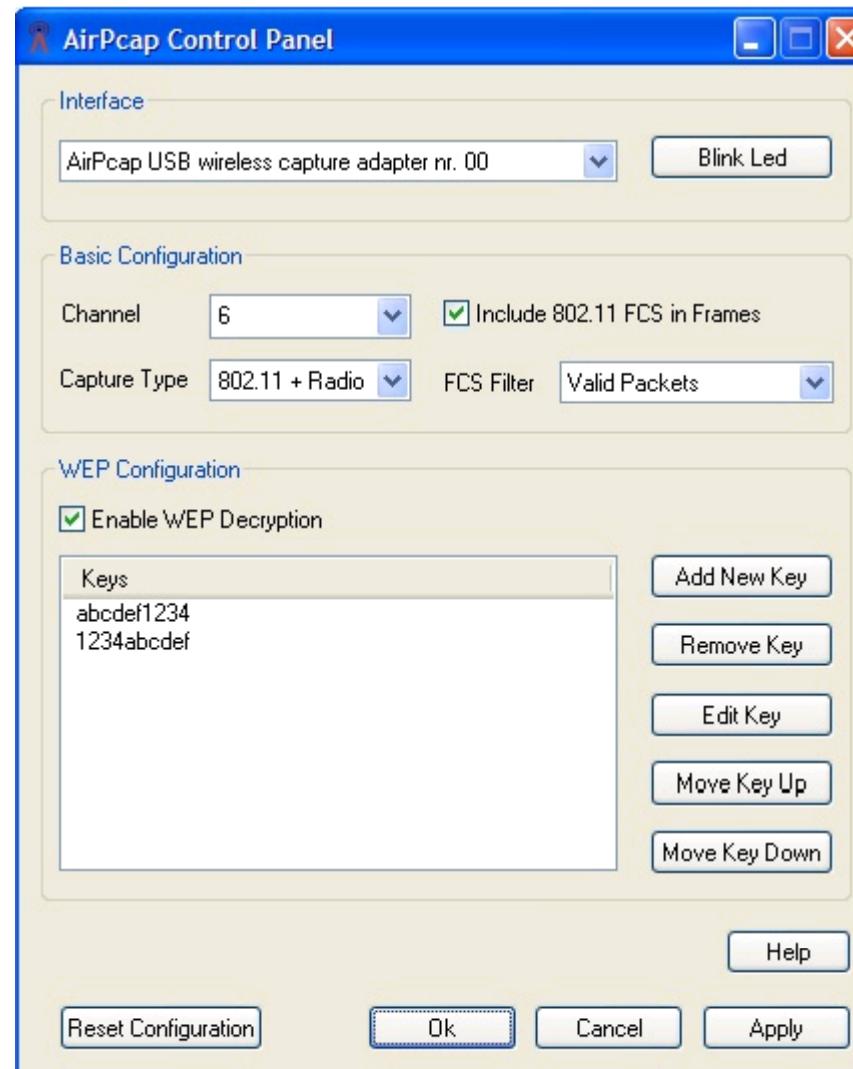
- Complete visibility on your wireless networks
- Portable and versatile
- Easy to set up
- Easy to use
- The performance you need
- Ready to power your application



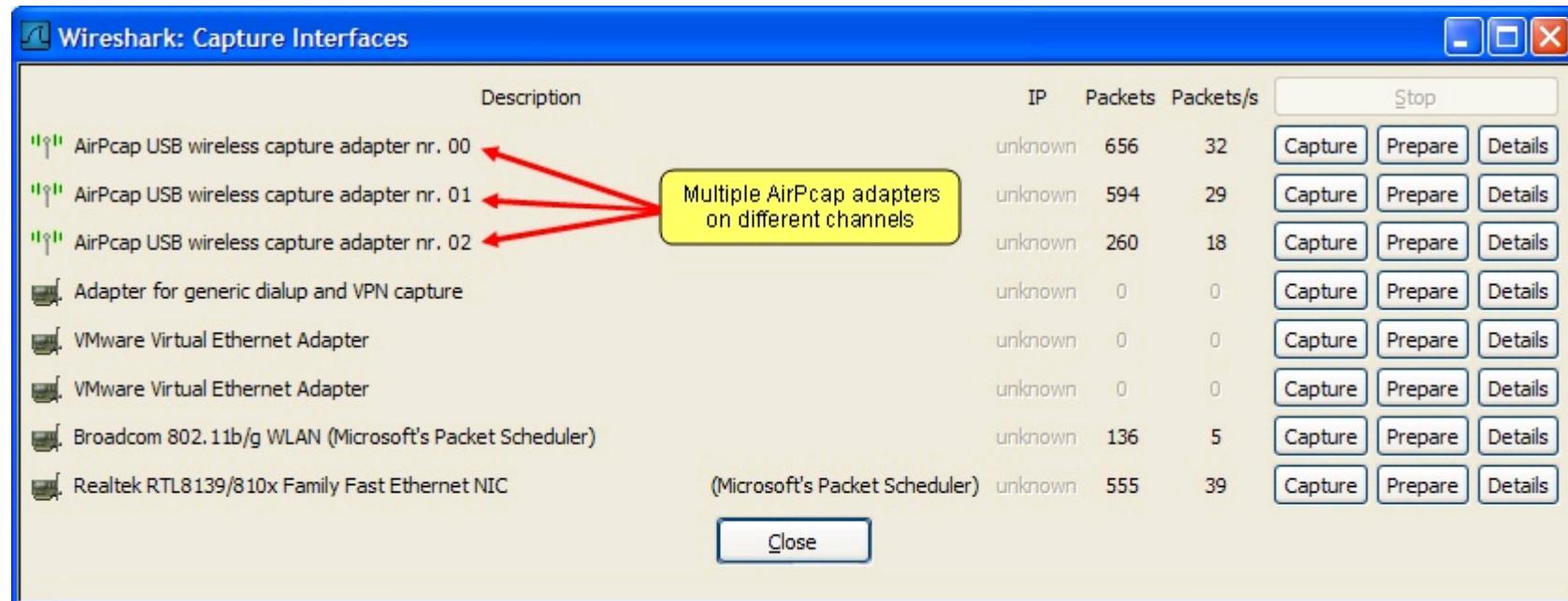


TM

# AirPcap: Screenshot 1

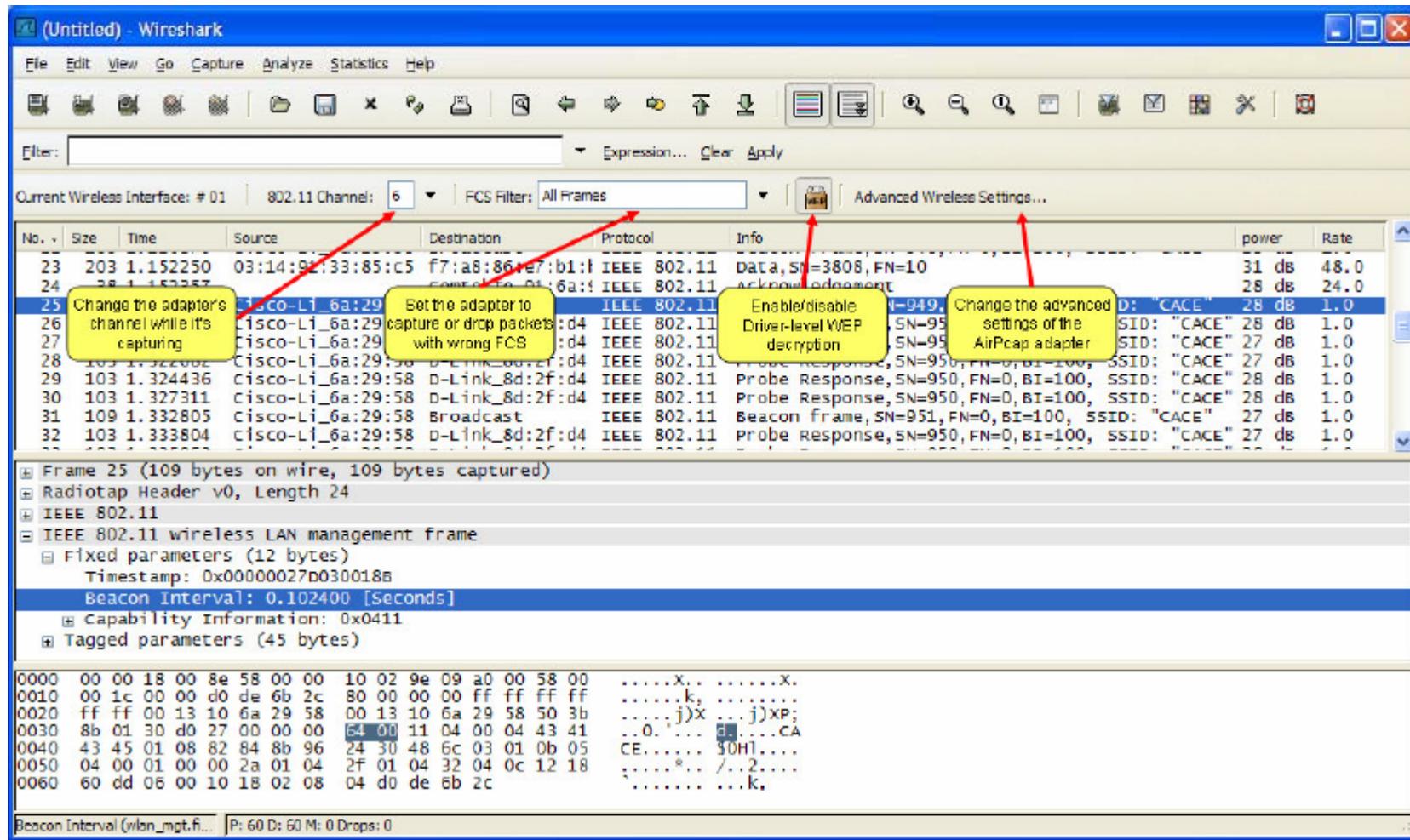


# AirPcap: Screenshot 2

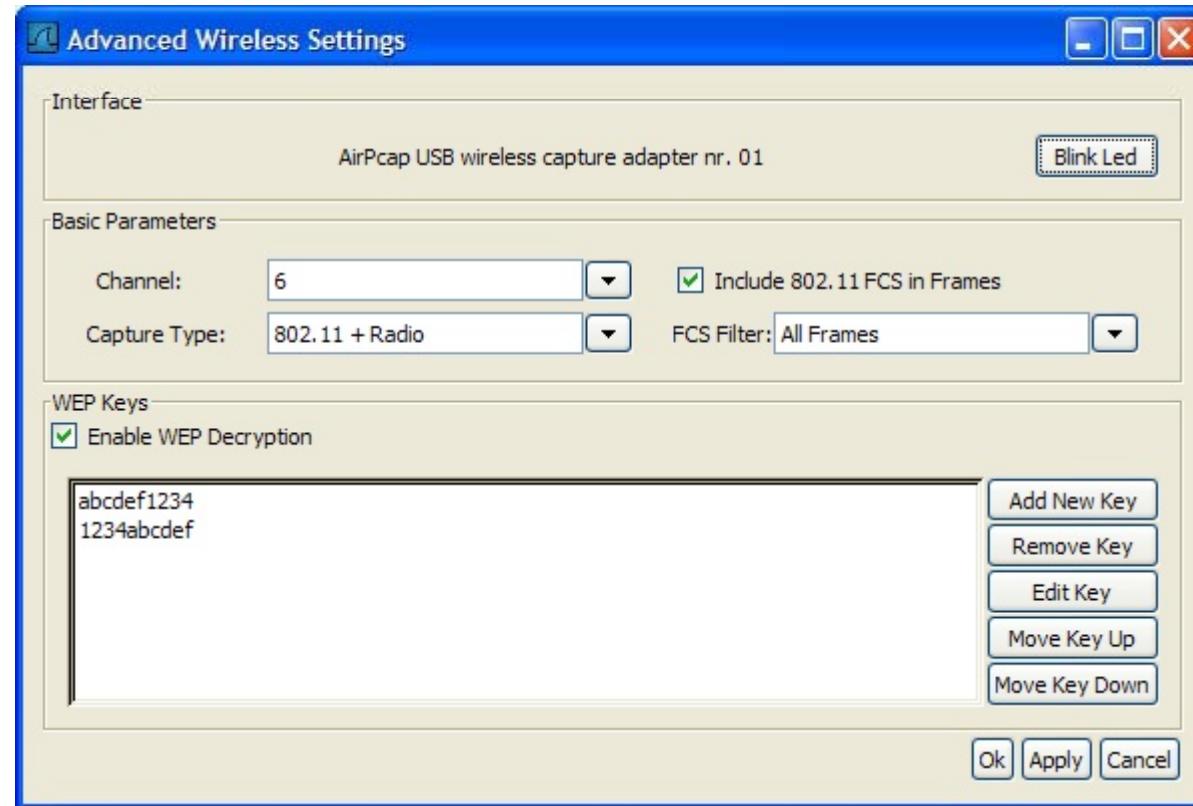


Multiple AirPcap Adapters in Wireshark

# AirPcap: Screenshot 3



# AirPcap: Screenshot 4



# AirPcap: Example Program from the Developer's Pack

```
c:\ C:\WINDOWS\system32\cmd.exe
Channel frequency: 2452 MHz
Channel number: 9
Channel type: 802.11b, 2Ghz spectrum
Signal Quality: 28
antenna n. 0
Signal Strength: 71dB
Frame Check Sequence: 0xa0c2e5fc

00000000 : 40 00 00 00 ff ff ff ff ff ff 00 90 4b 45 36 62 0.....KE6b
00000010 : ff ff ff ff ff ff a0 06 00 00 01 08 02 04 0b 16 .....
00000020 : 24 30 48 6c 32 04 0c 12 18 60 dd 09 00 10 18 02 $0H12....;
00000030 : 00 10 00 00 00 a0 c2 e5 fc .....;

Packet length - captured portion: 81, 81
Rate: 1.0 Mb/s
Channel frequency: 2452 MHz
Channel number: 9
Channel type: 802.11b, 2Ghz spectrum
Signal Quality: 92
antenna n. 0
Signal Strength: 73dB
Frame Check Sequence: 0xb04f9b12

00000000 : 40 00 00 00 ff ff ff ff ff ff 00 90 4b 45 36 62 0.....KE6b
00000010 : ff ff ff ff ff ff b0 06 00 00 01 08 02 04 0b 16 .....
00000020 : 24 30 48 6c 32 04 0c 12 18 60 dd 09 00 10 18 02 $0H12....;
00000030 : 00 10 00 00 00 b0 4f 9b 12 .....0..;

Packet length - captured portion: 81, 81
Rate: 1.0 Mb/s
Channel frequency: 2452 MHz
Channel number: 9
Channel type: 802.11b, 2Ghz spectrum
Signal Quality: 100
antenna n. 0
Signal Strength: 72dB
Frame Check Sequence: 0x3e671f4

00000000 : 40 00 00 00 ff ff ff ff ff ff 00 90 4b 45 36 62 0.....KE6b
00000010 : ff ff ff ff ff ff c0 06 00 00 01 08 02 04 0b 16 .....
00000020 : 24 30 48 6c 32 04 0c 12 18 60 dd 09 00 10 18 02 $0H12....;
00000030 : 00 10 00 00 00 03 e6 71 f4 .....q.
```



TM

# Microsoft Network Monitor

Wireless (802.11) capturing and monitor mode on Vista – with supported hardware, (Native WIFI)

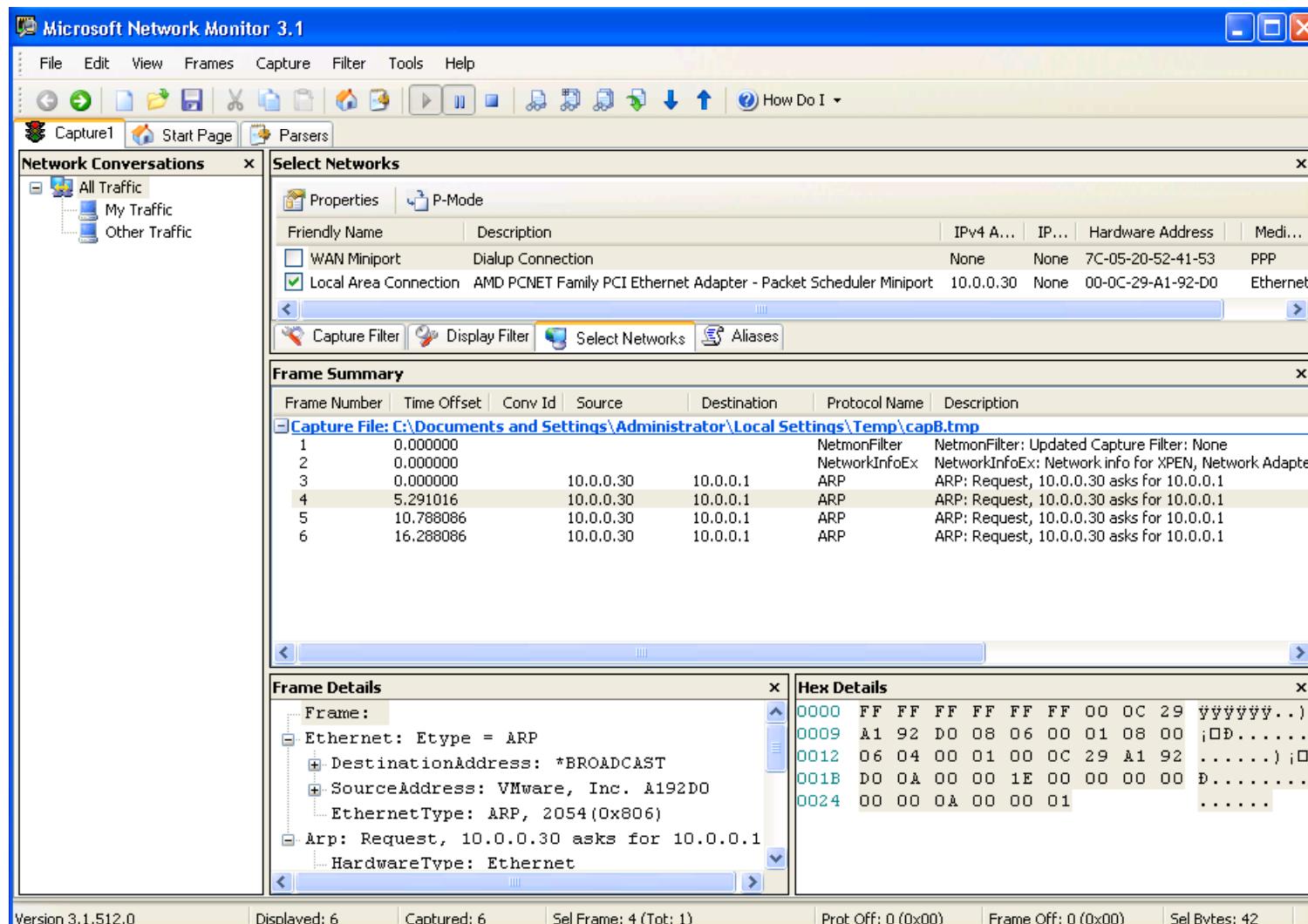
It troubleshoots wireless connections

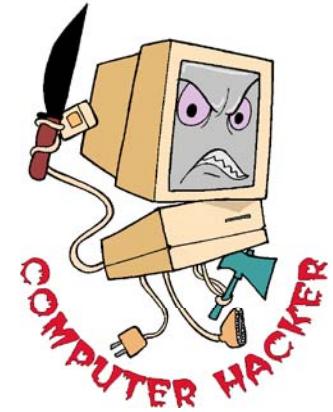
It can trace wireless management packets

It scans all channels or a subset of the ones your wireless NIC supports

RAS tracing support on Vista

# Microsoft Network Monitor: Screenshot





# Hacking Wireless Networks

# Steps for Hacking Wireless Networks

Step 1: Find networks to attack



Step 2: Choose the network to attack



Step 3: Analyze the network



Step 4: Crack the WEP key



Step 5: Sniff the network



# Step 1: Find Networks to Attack

An attacker would first use NetStumbler to drive around and map out active wireless networks

Using Netstumbler, the attacker locates a strong signal on the target WLAN

Netstumbler not only has the ability to monitor all active networks in the area, but it also integrates with a GPS to map APs



## Step 2: Choose the Network to Attack

At this point, the attacker has chosen his target

NetStumbler or Kismet can tell him whether or not the network is encrypted



# Step 3: Analyzing the Network

## Example:

- WLAN has no broadcasted SSID
- NetStubmler tells you that SSID is ZXECOUNCIL
- Multiple access points are present
- Open authentication method
- WLAN is encrypted with 40bit WEP
- WLAN is not using 802.1X



# Step 4: Cracking the WEP Key

Attacker sets NIC drivers to monitor mode



It begins by capturing packets with Airodump

Airodump quickly lists the available network with SSID and starts capturing packets



After a few hours of Airodump session, launch Aircrack to start cracking!

WEP key for ZXECOUNCIL is now revealed!

# Step 5: Sniffing the Network

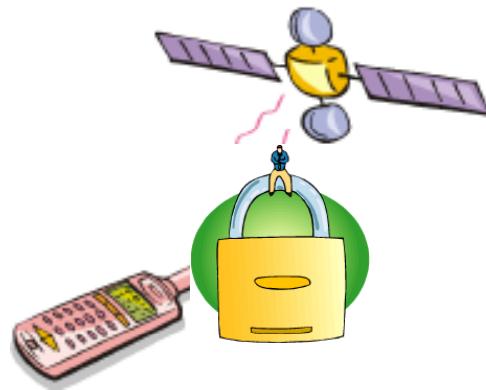
Once the WEP key is cracked and the NIC is configured appropriately, the attacker is assigned an IP and can access the WLAN



Attacker begins listening to traffic with Wireshark

Look for plaintext protocols (in this case, FTP, POP, and Telnet)



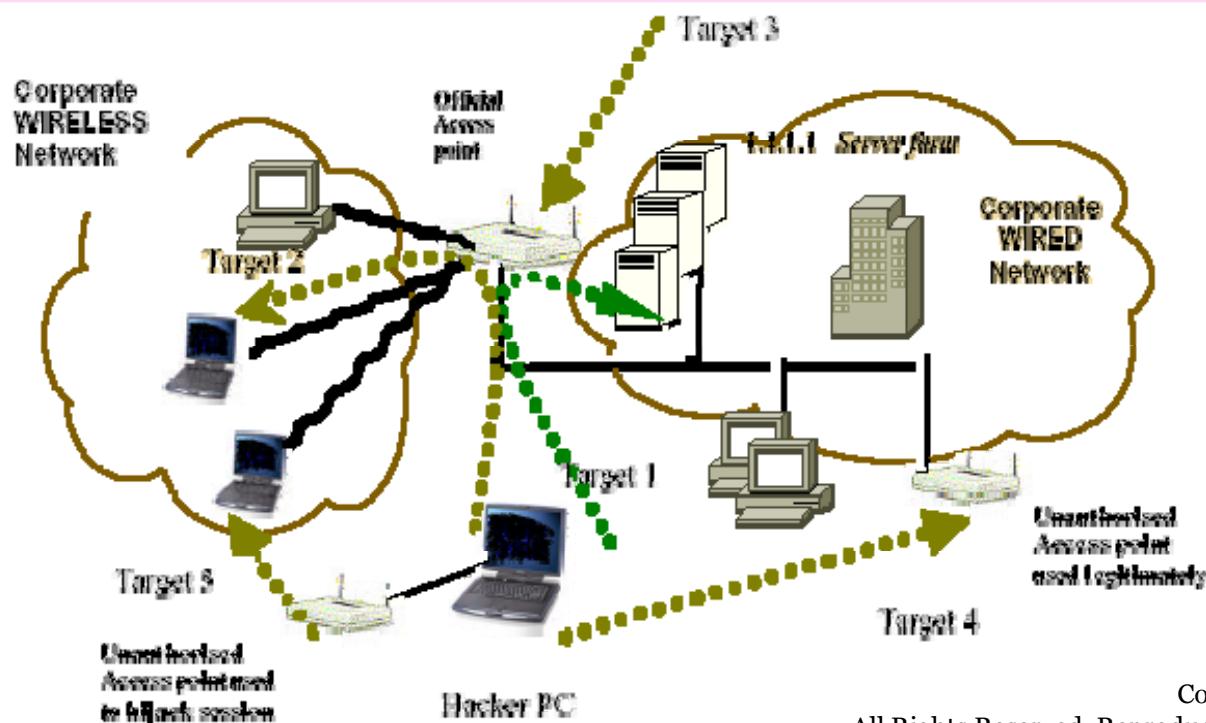


# Wireless Security

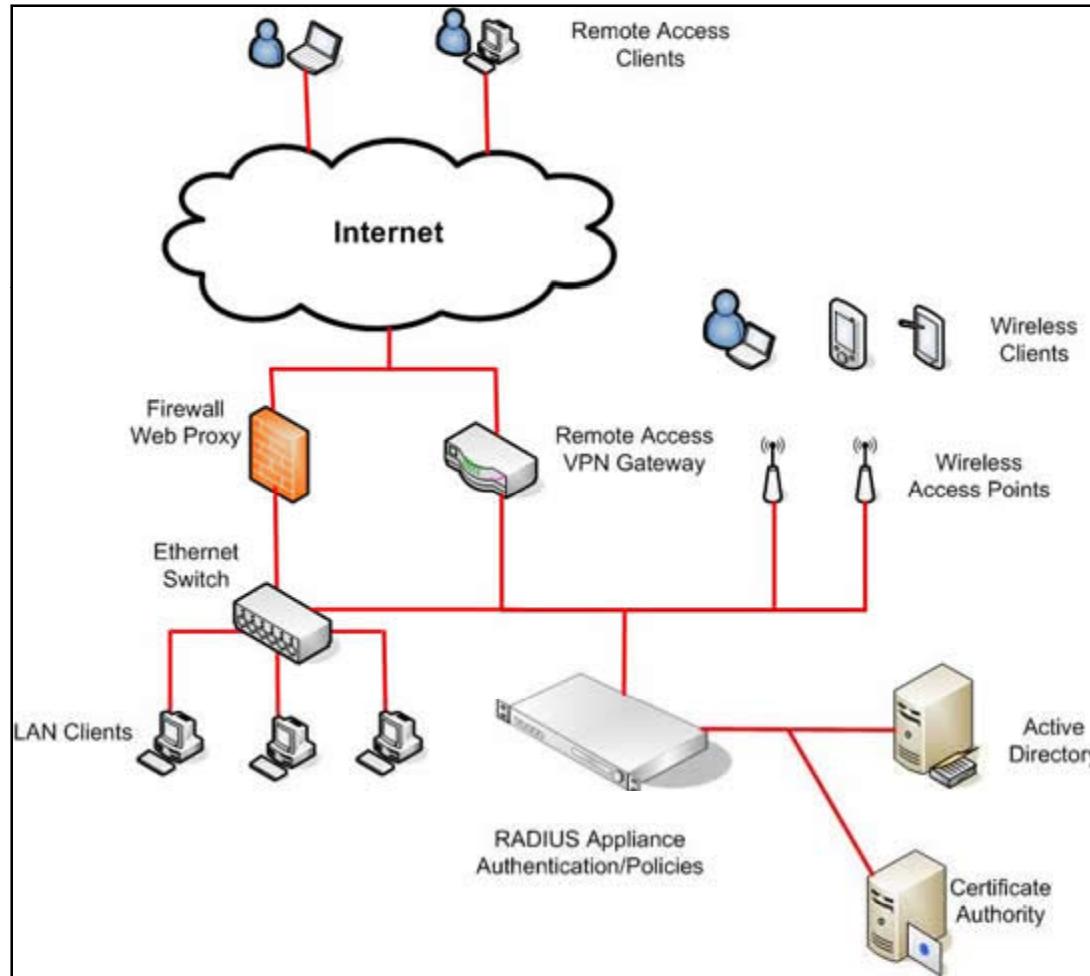
# WIDZ: Wireless Intrusion Detection System

WIDZ is a proof of concept IDS system for 802.11 that guards APs and monitors locally for potentially malevolent activity

It detects scans, association floods, and bogus/rogue APs. It can easily be integrated with SNORT or RealSecure



# Radius: Used as Additional Layer in Security



## MAC Address Filtering

- MAC Address Filtering method uses a list of MAC addresses of client wireless network interface cards that are allowed to associate with the access point



## SSID (NetworkID)

- The first attempt to secure a wireless network was the use of Network ID (SSID)
- When a wireless client wants to associate with an access point, the SSID is transmitted during the process
- The SSID is a seven-digit alphanumeric ID that is hard coded into the access point and the client device



## Firewalls

- Using a firewall to secure a wireless network is probably the only way to prevent unauthorized access

Wireless networks that use infrared beams to transport data from one point to another are secure

# Securing Wireless Networks (cont'd)

Change the default SSID names, such as NETGEAR

Add passwords to all devices on the wireless network

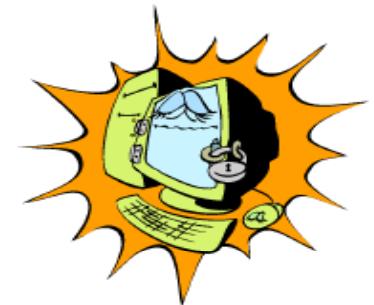
Disable broadcasting on network access points

Do not give the network a name that identifies your company, like EC-Council-NYC

Move wireless access points away from windows

Disable DHCP and use manual IP addresses

Do not allow remote management of access points



# Securing Wireless Networks (cont'd)

Use the built-in encryption at the access point

Disable the features you do not use such as printing and music support in the AP

Upgrade your firmware regularly

Put a firewall between the wireless network and other company computers on the network

Encrypt data at the application protocol, for example, SSL

Change all default settings for access points:

- Such as the IP address

Regularly test wireless network security

Include VPN in your wireless security solutions



# Wireless Network Security Checklist

- ✓ Ensure that all unused ports are closed
  - ✓ Any open ports must be justified
  - ✓ “Pessimistic” network view
- ✓ Enforce the rule of least access
- ✓ Ensure SSIDs are changed regularly
- ✓ Ensure insurance and authentication standards are created and enforced
- ✓ Use strong encryption
  - ✓ SHA-1 (Secure Hashing Algorithm)
- ✓ Initiate encryption at user and end at server that is behind the firewall, outside the DMZ
- ✓ Treat WLANs as untrusted networks that must operate inside the DMZ





# Wireless Network Security Checklist (cont'd)

- ✓ Access trusted network via VPN and two-factor authentication
- ✓ Increase application security:
  - ✓ Possibly through use of an enterprise application system
  - ✓ Minimally through increased encryption
- ✓ Do not allow ad hoc WLANS
- ✓ Embrace and employ the 802.11i IEEE security standard
  - ✓ Native per user access control
  - ✓ Native strong authentication (tokens, smartcards, and certificates)
  - ✓ Native strong encryption

# WLAN Security: Passphrase

A passphrase is a sequence of words or other text used to control access to a computer system, program, or data



It is similar to a password in usage, but is generally longer for added security

Passphrases are often used to control both access to, and operation of, cryptographic programs and systems

Passphrases are particularly applicable to systems that use the passphrase as an encryption key

# Don'ts in Wireless Security



- Do not breach your own firewall
- Do not reject Media Access Control
- Do not reject WEP
- Do not permit unauthorized access point
- Do not permit Ad-hoc Laptop communication





# Wireless Security Tools

# WLAN Diagnostic Tool: CommView for WiFi PPC

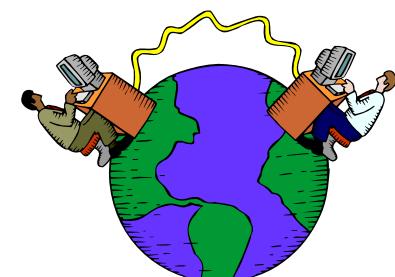
CommView for WiFi PPC is a special lightweight edition of CommView for WiFi that runs on Pocket PC handheld computers

It is a WLAN diagnostic solution designed for express wireless site surveys, as well as capturing and analyzing network packets on wireless 802.11b/g networks

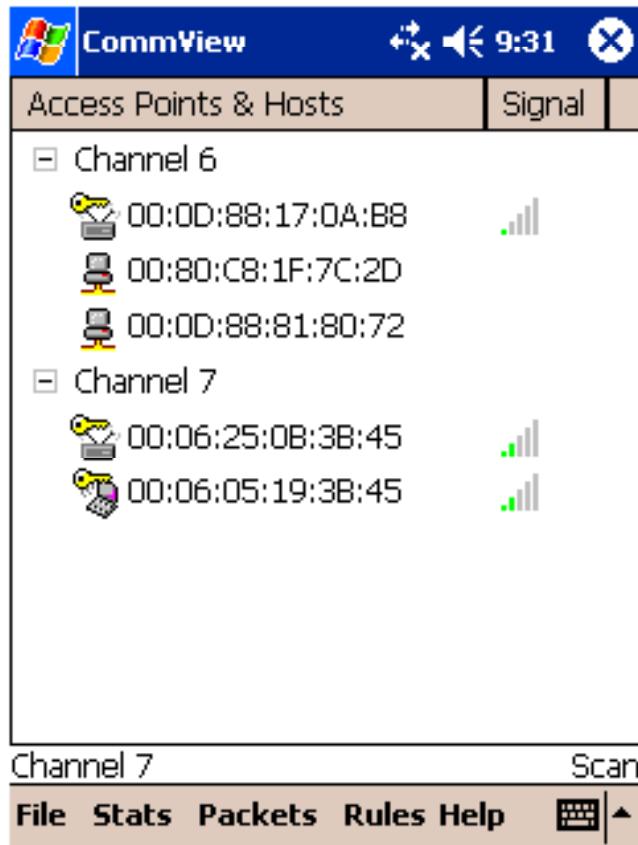
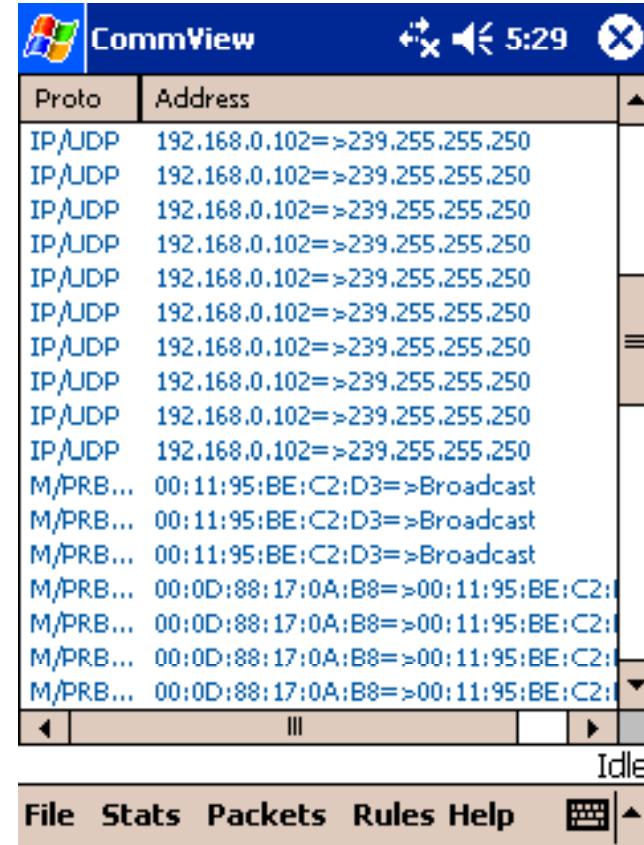
It gathers information from the wireless adapter and decodes the analyzed data

With CommView for WiFi PPC, you can:

- Scan the air for WiFi signals
- Select channels for monitoring
- Detect access points and wireless stations
- Capture packets
- Measure signal strength
- View the list of network connections
- Examine and filter individual packets



# CommView for WiFi PPC: Screenshots

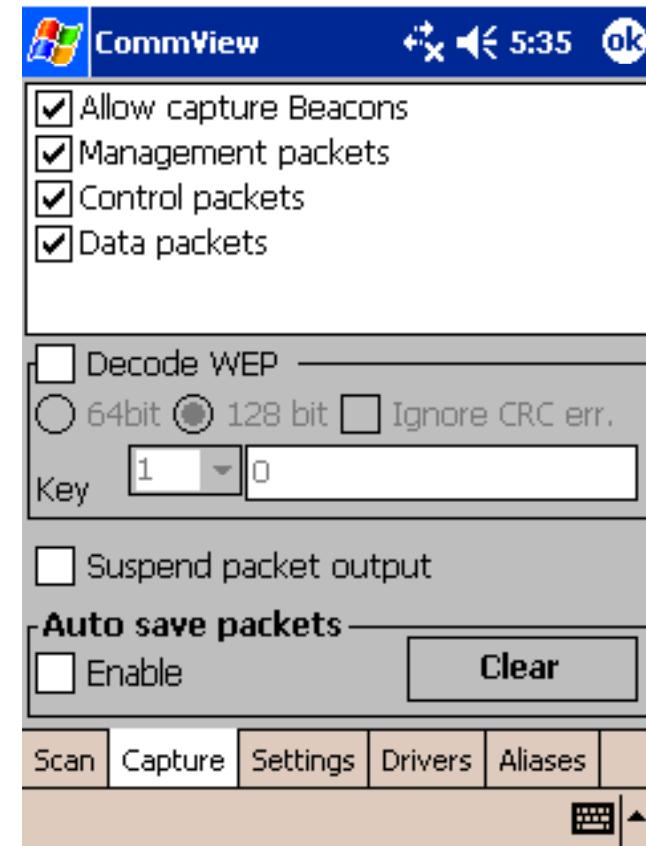
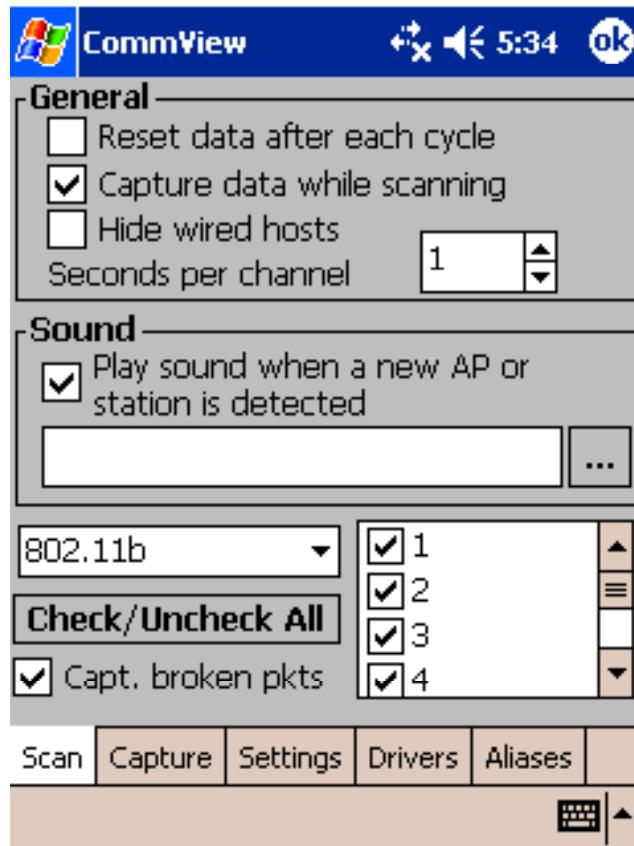



The screenshot shows the CommView interface for WiFi PPC displaying a list of network traffic entries. The table has columns for "Proto" and "Address".

Proto	Address
IP/UDP	192.168.0.102=>239.255.255.250
M/PRB...	00:11:95:BE:C2:D3=>Broadcast
M/PRB...	00:11:95:BE:C2:D3=>Broadcast
M/PRB...	00:11:95:BE:C2:D3=>Broadcast
M/PRB...	00:0D:88:17:0A:B8=>00:11:95:BE:C2:D3

The status bar at the bottom shows "Idle".

# CommView for WiFi PPC: Screenshots



# WLAN Diagnostic Tool: AirMagnet Handheld Analyzer

Handheld Analyzer is a convenient and inexpensive way to solve serious problems in the enterprise wireless LAN

It is used for troubleshooting of 802.11 b LANs

## Features:

- Automatically detects vulnerabilities
- Locks down security policies
- Performs live, interactive network tests
- Tracks down rogues and devices
- Detailed packet and frame analysis
- Accesses the AirWISE® expert
- GPS support
- Flexible mobile form factor





TM

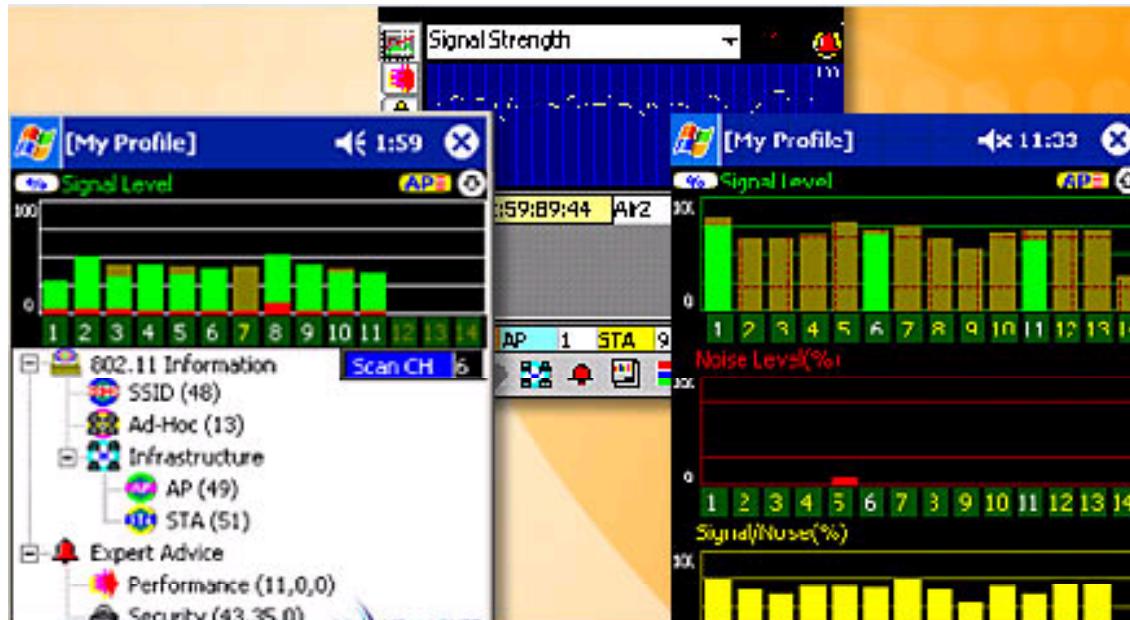
# AirMagnet Handheld Analyzer: Screenshot 1





TM

# AirMagnet Handheld Analyzer: Screenshot 2

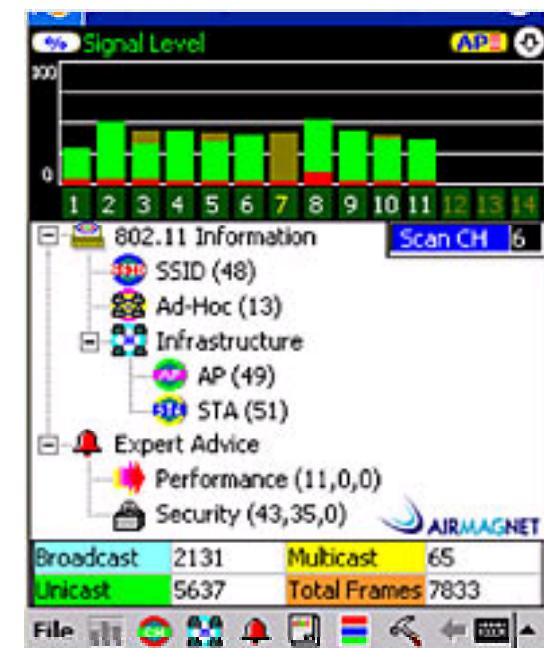
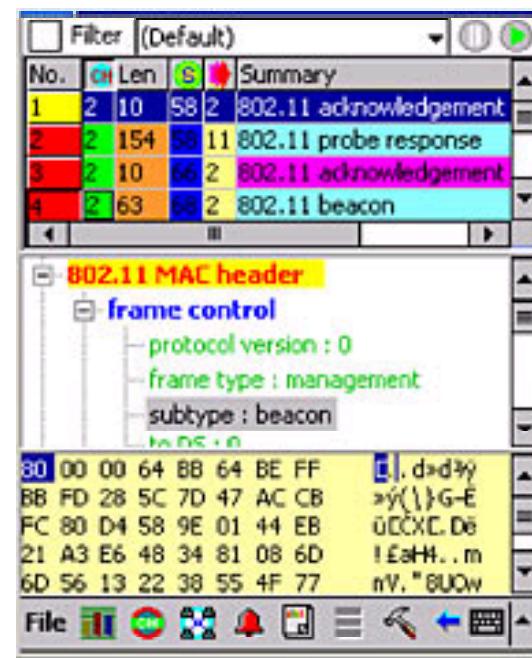
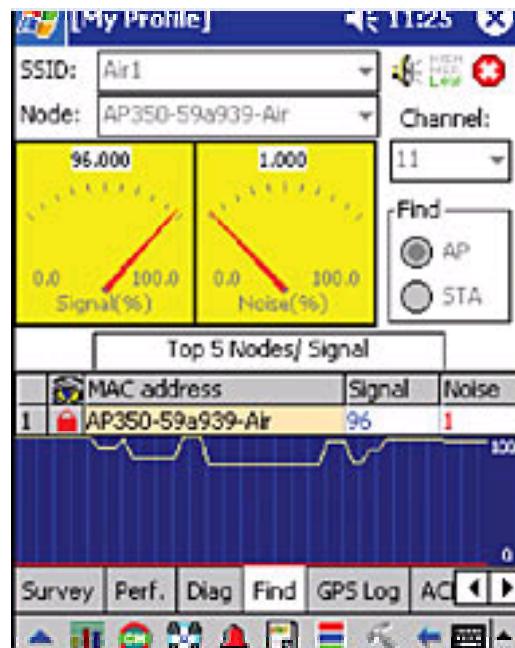


STA:	Agere:2E:57:08	Diagnose	Print	Help
AP:	Aironet:29:4F:46 -airpocket	Diagnose	Print	Help
STA Connection Diagnosis				Status
Beacon received	Yes(1)			
Probe request sent	Yes(5)			
Probe response received	Yes(1)			
Auth. request sent	Yes(1)			
Auth. challenge received				
Auth. challenge response received				
Auth. final response received	Yes(1)			
Association request sent	Yes(1)			
Association response received	Yes(1)			
Data Tx: IP ARP	Yes(61)			
Data Rx: IP ARP	Yes(30)			
Click here to view the diagnostics				Done!
<a href="#">Survey</a> <a href="#">Perf.</a> <a href="#">Diag</a> <a href="#">Find</a> <a href="#">Ping</a> <a href="#">Trace</a> <a href="#">Help</a>				
<a href="#">File</a> <a href="#">Edit</a> <a href="#">Search</a> <a href="#">Print</a> <a href="#">Help</a>				



TM

# AirMagnet Handheld Analyzer: Screenshot 3





TM

# Auditing Tool: BSD-Airtools

BSD-Airtools is a package that provides a complete toolset for wireless 802.11b auditing

It contains a bsd-based WEPCracking application, called dweputils, as well as kernel patches for NetBSD, OpenBSD, and FreeBSD

It also contains a curses-based AP detection application similar to NetStumbler (dstumbler) that can be used to detect wireless access points and connected nodes, view signal to noise graphs, and interactively scroll through scanned APs and view statistics for each

It also includes other tools to provide a complete toolset for making use of all 14 of the prism2 debug modes as well as do basic analysis of the hardware-based link-layer protocols provided by prism2's monitor debug mode

Source: <http://www.dachboden.com/>



TM

# AirDefense Guard



AirDefense Guard is an 802.11a/b/g wireless LAN intrusion detection and security solution that identifies security risks and attacks, provides real-time network audits, and monitors the health of the wireless LAN

It detects all rogue WLANs

It secures a wireless LAN by recognizing and responding to intruders and attacks as they happen

It performs real-time network audits to inventory all hardware, tracks all wireless LAN activity, and enforces WLAN policies for security and management

It monitors the health of the network to identify and respond to hardware failures, network interferences, and performance degradation

Source: [www.AirDefense.com](http://www.AirDefense.com)



TM

# AirDefense Guard: Screenshot

**You are currently protected by AirDefense Personal.**

AirDefense will alert you to impending dangers in your wireless network environment or security risks in your system

Last Scan Performed: 09:36 30.03.2006  
Total Number of scans: 1

**Your Wireless Threat Information**

**Current threat level:**  
**What this means:**  
Your computer is well configured. It has minimal wireless security risks. It will be very hard for intruders to hack it.

**Guarded** **Low**

**Wireless Threats Status**

	Critical	Major	Minor	Ignore	Total
Today	0	0	0	0	0
Yesterday	0	0	0	0	0
All	0	0	0	0	0

AirDefense

Wireless Stations

Access Points

Remote Sensor

Wireless Stations

Access Points

Remote Sensor

Cloud

Server Appliance

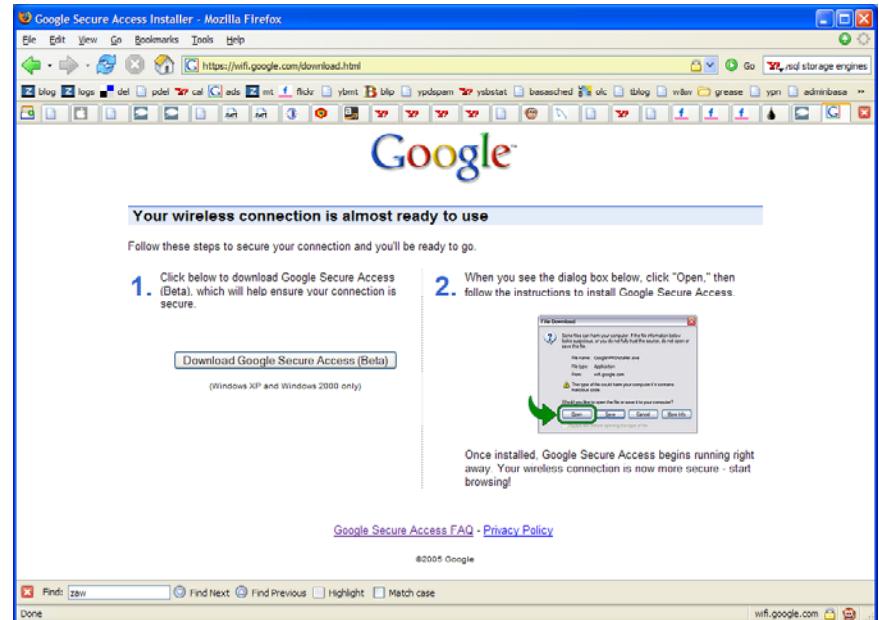
# Google Secure Access



Google Secure Access is a downloadable client application that allows users to establish a more secure WiFi connection

It connects to Google's VPN ("Virtual Private Network")

It encrypts your Internet traffic and sends it through Google's servers to the Internet. The data that is received will then be encrypted and sent back through Google's servers to your computer



# Tool: RogueScanner

RogueScanner is a network security tool for automatically discovering rogue wireless access points by scanning a wired network

It can also be used for network asset discovery

It can find all network connected devices like printers, routers, web cameras, and PCs

IP Address	MAC Address	Vendor	Model	Score	Class	Feedback
192.168.1.1	00:E0:FC:07:65:D0	Not classified yet				
192.168.1.231	00:05:5D:2F:19:E3	Not classified yet				
192.168.1.31	00:11:2F:7B:A7:C8	Not classified yet				
192.168.1.3	00:02:55:07:8A:AB	Not classified yet				
192.168.1.4	00:40:95:C0:05:47	Not classified yet				
192.168.1.39	00:60:E0:80:34:08	Not classified yet				
192.168.1.240	00:05:5D:2F:19:F8	Not classified yet				
192.168.1.76	00:0C:6E:6A:D1:43	Not classified yet				
192.168.1.230	00:02:55:07:3C:30	Not classified yet				
192.168.1.253	00:02:55:07:22:52	Not classified yet				
192.168.1.23	00:02:55:07:B1:AD	Not classified yet				
192.168.1.184	00:10:5A:9C:39:1F	Not classified yet				
192.168.1.230	00:0C:6E:7A:F2:49	Not classified yet				
192.168.1.8	00:40:95:30:86:7C	Not classified yet				
192.168.1.9	00:04:60:01:78:31	Not classified yet				
192.168.1.10	00:0E:53:03:FF:34	Not classified yet				
192.168.1.11	00:0E:53:04:06:24	Not classified yet				
192.168.1.13	00:0B:AC:EA:75:C0	Not classified yet				
192.168.1.14	00:E0:4C:B0:62:EA	Not classified yet				
192.168.1.15	00:04:75:FC:33:75	Not classified yet				
192.168.1.17	00:40:95:30:06:70	Not classified yet				
192.168.1.22	00:05:5D:35:A8:09	Not classified yet				
192.168.1.27	00:40:95:30:82:68	Not classified yet				
192.168.1.32	00:05:5D:35:B0:74	Not classified yet				
192.168.1.33	00:06:5B:15:94:26	Not classified yet				
192.168.1.34	00:0D:07:0E:A5:6E	Not classified yet				
192.168.1.35	00:50:FC:64:66:9C	Not classified yet				
192.168.1.36	00:50:FC:64:66:49	Not classified yet				
192.168.1.195	00:E0:4C:EC:A1:C9	Not classified yet				
192.168.1.182	00:E0:4C:EC:B9:BB	Not classified yet				
192.168.1.41	00:06:5B:15:AC:D1	Not classified yet				
192.168.1.42	00:0C:6E:6A:D1:0D	Not classified yet				
192.168.1.44	00:E0:4C:EE:04:56	Not classified yet				



# What Happened Next?

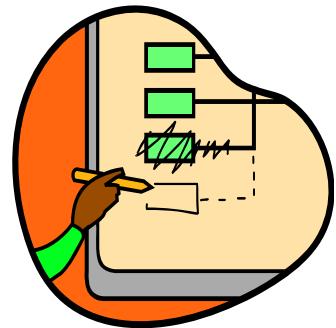
Jason Springfield, an ethical hacker, was called in to investigate the incident. Jason performed the following tests:

- He scanned the network and traced it
- He checked for SSID broadcasted and secured it by assigning unique alpha numeric values
- He traced rogue access points by using tools, such as, NetStumbler and MiniStumbler
- He deployed WEP to provide confidentiality of data on WLAN
- He employed WSA for auditing the network and traced the vulnerabilities



Jason suggested them to take following precautions:

- Use MAC address filtering, SSID, and firewalls for wireless networks
- Use infrared beams to transport data





# Summary

A wireless network enables a mobile user to connect to a LAN through a wireless (radio) connection

Wired Equivalent Privacy (WEP) is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN

It is vulnerable because of relatively short IVs and keys that remain static

Even if WEP is enabled, an attacker can easily sniff MAC addresses as they appear in the clear format. Spoofing MAC addresses is also easy

Wireless networks are vulnerable to DoS attacks

Wireless network security can adopt a suitable strategy of MAC address filtering, firewalling, or a combination of protocol-based measures

TM



Certified Ethical Hacker

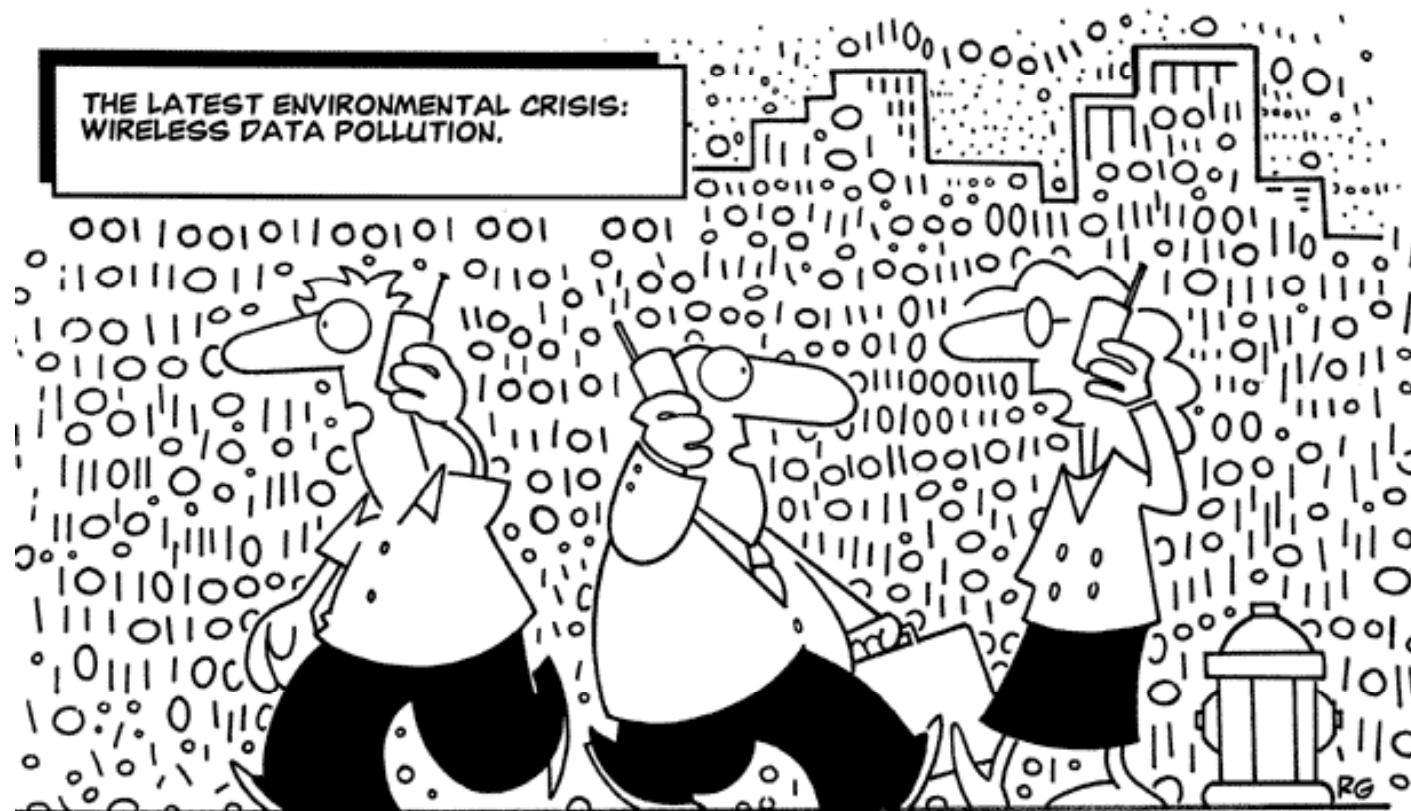


© 2003 Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)

**"This phone won't disturb anyone at the movies.  
It has a ringer that sounds like people eating popcorn!"**



TM



Copyright 2004 by Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)

Certified Ethical Hacker

TM

© 2000 Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**“It’s an internet-ready, tri-mode, LCD color, MP3 compatible, digital wireless communicator. We make them extra big so people will notice how cool you are.”**



TM

Copyright 2003 by Randy Glasbergen.  
[www.glasbergen.com](http://www.glasbergen.com)



**"Watch where you're going, Larry — you walked  
right through my wireless data stream!"**