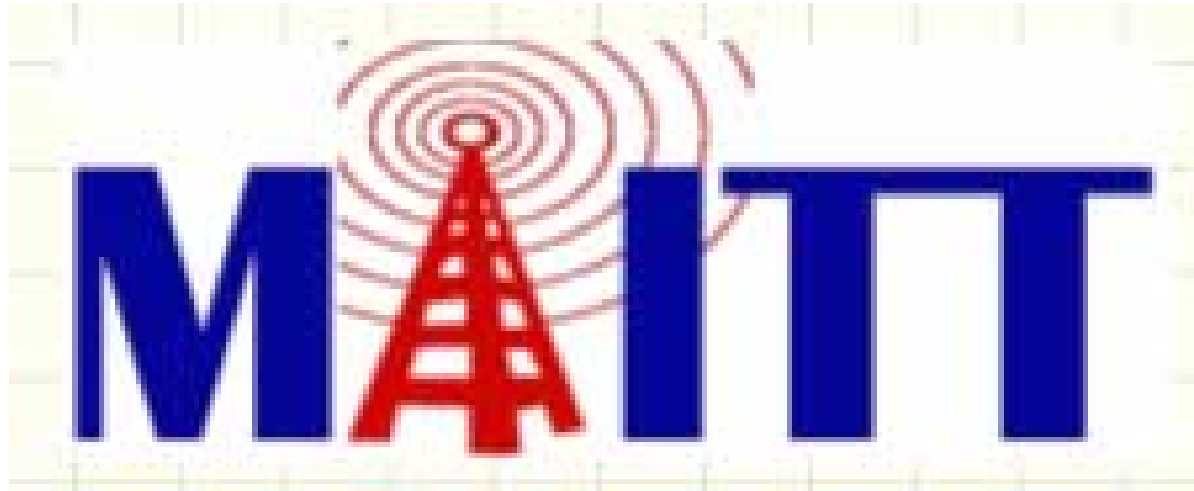


Wireless LAN Auditing Tools



Mid-Atlantic Institute for Telecommunications Technologies

Michael Qaissaunee
Mohammad Shanehsaz

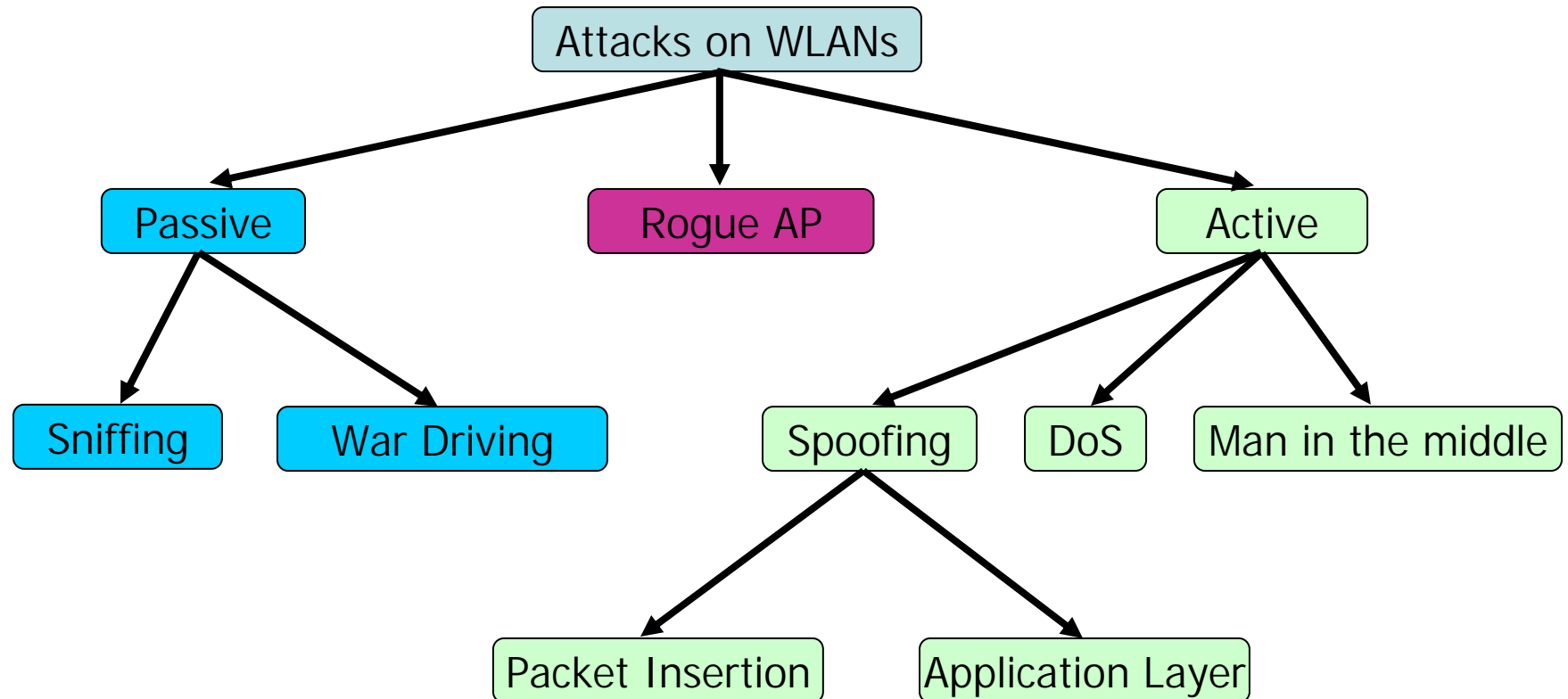


This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Attacks on WLANs



Emerging Security Solutions

- WEP Key Management
- Wireless VPNs
- TKIP
- AES
- Wireless Gateways
- 802.1X and EAP

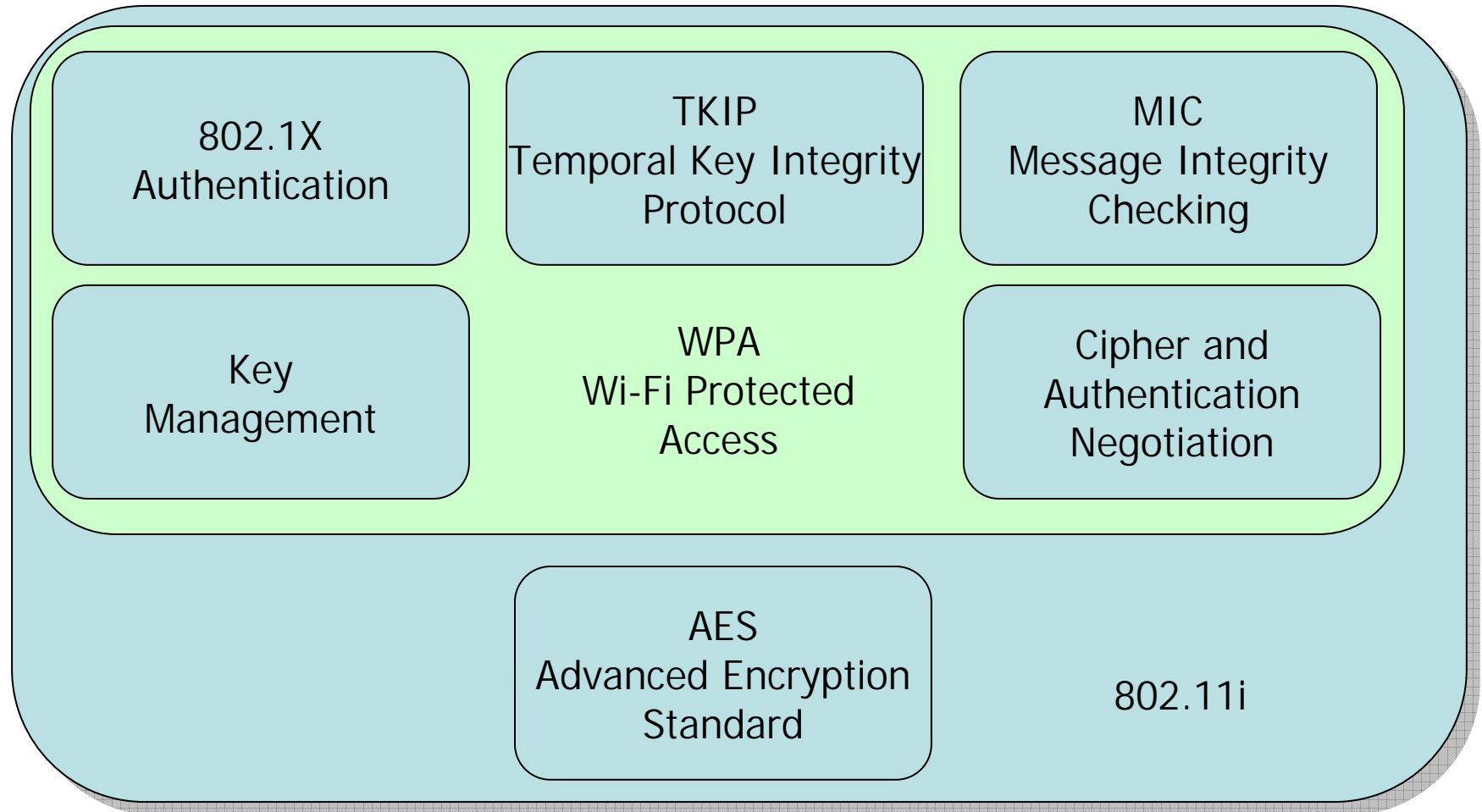


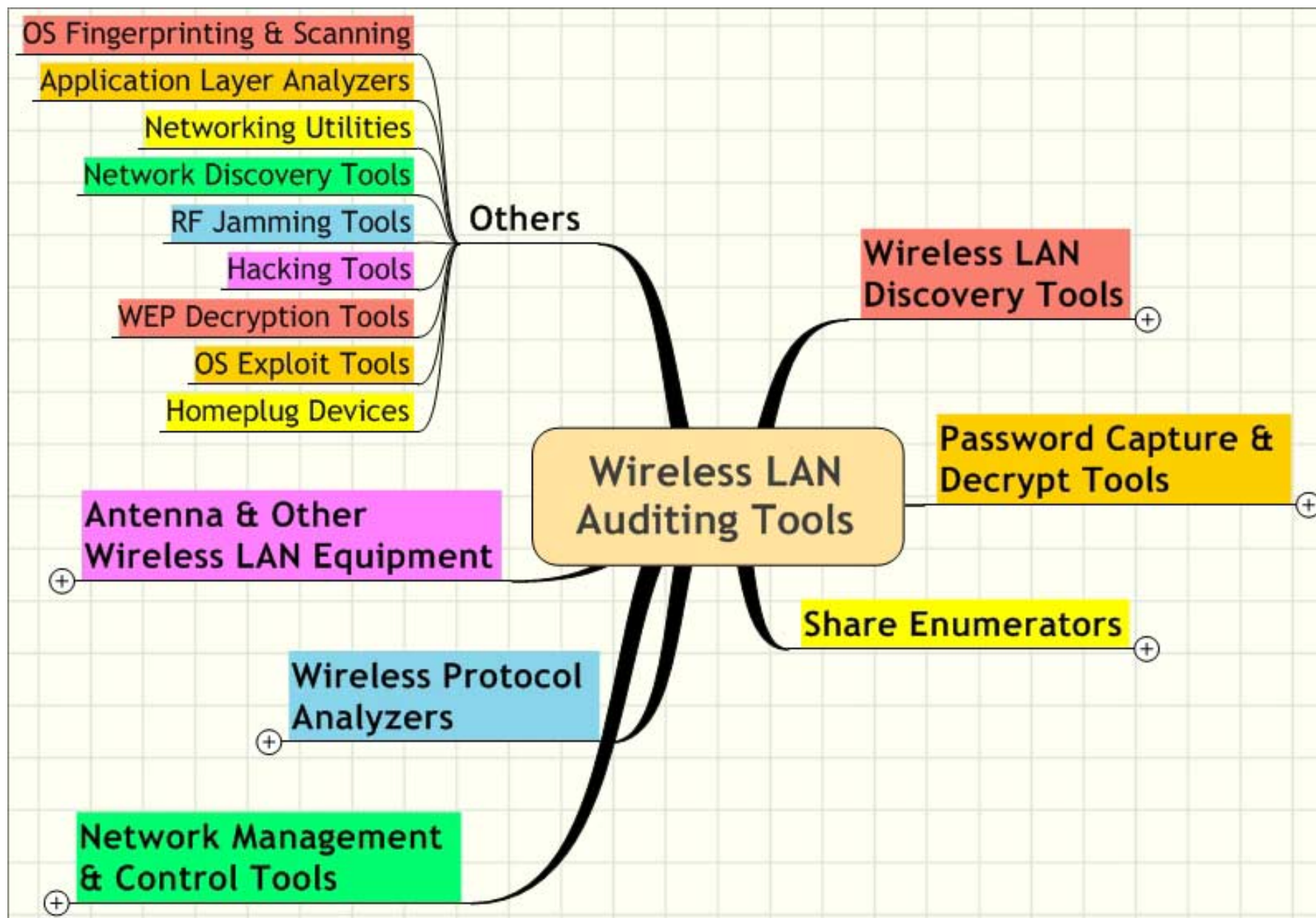
This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Emerging Security Solutions





Wireless LAN Discovery Tools

NetStumbler

- Written by Marius Milner
- You can download from www.netstumbler.com
- Free Windows-based software utility for locating and interrogating Wireless LANs using 802.11b, 802.11a and 802.11g.
- It displays MAC Address, SSID, Access Point name, Channel, Vendor, WEP on or off, Signal Strength, GPS coordinates (if GPS device is attached)

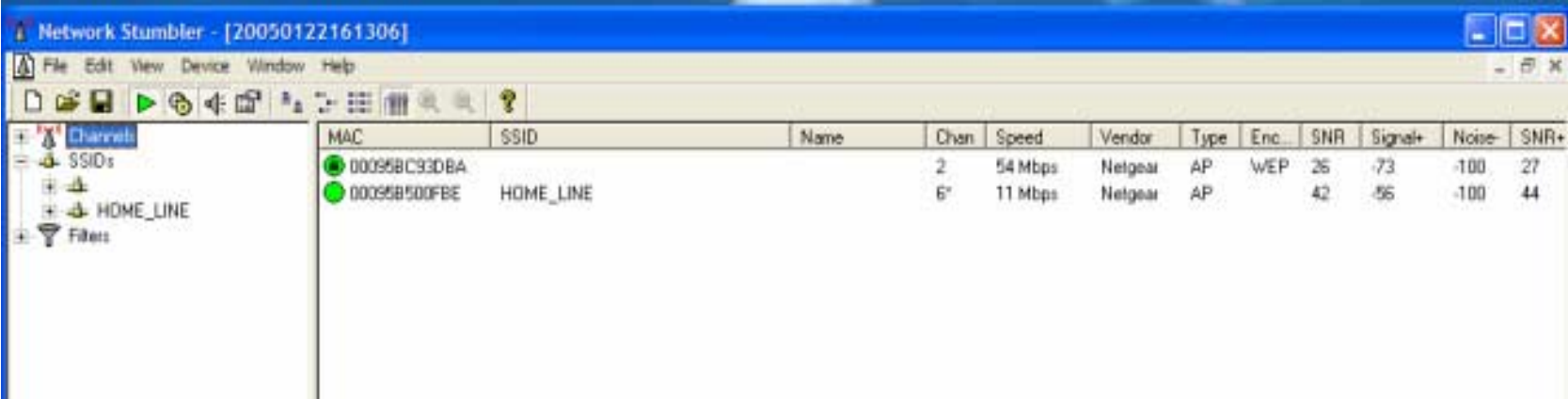


This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



NetStumbler



The screenshot shows the NetStumbler application window with the title bar 'Network Stumbler - [20050122161306]'. The interface includes a menu bar (File, Edit, View, Device, Window, Help) and a toolbar. On the left, a tree view shows 'Channels', 'SSIDs', 'HOME_LINE', and 'Filters'. The main area displays a table of detected networks.

MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc.	SNR	Signal+	Noise-	SNR+
00095BC93DBA	HOME_LINE		2	54 Mbps	Netgear	AP	WEP	26	-73	-100	27
00095B500FBE	HOME_LINE		6	11 Mbps	Netgear	AP		42	-56	-100	44

- It displays MAC Address, SSID, Access Point name, Channel, Vendor, WEP on or off, Signal Strength, GPS coordinates (if GPS device is attached)



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Wireless LAN Discovery Tools

NetStumbler

It has many uses:

- Verify that your network is set up the way you intended.
- Find locations with poor coverage in your WLAN.
- Detect other networks that may be causing interference on your network.
- Detect unauthorized "rogue" access points in your workplace.
- Help aim directional antennas for long-haul WLAN links.
- Use it recreationally for WarDriving.

Functionality

- NetStumbler sends probe request frames that cause all access points to respond with information about themselves , including the SSID.
- When using the closed network feature, Netstumbler will not see the access point, provided the access point does not respond to probe request frame using “ broadcast SSIDs “



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Wireless LAN Discovery Tools

MiniNetStumbler

- First cousin of NetStumbler
- Offer the same functionality as Netstumbler
- It is more commonly used when war walking, because it runs on the PocketPC



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Wireless LAN Discovery Tools

Kismet

- It is written by Mike Kershaw and can be downloaded from <http://www.kismetwireless.net>
- Runs on the Linux operating system
- Offers similar functionality to Netstumbler
- Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.
- Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic.



Some Features available in Kismet

- Ethereal/Tcpdump compatible data logging
- Aircnort compatible weak-iv packet logging
- Network IP range detection
- Built-in channel hopping and multiscard split channel hopping
- Hidden network SSID decloaking
- Graphical mapping of networks (gpsmap)
- Client/Server architecture allows multiple clients to view a single Kismet server simultaneously



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Some Features available in Kismet

- Manufacturer and model identification of access points and clients
- Detection of known default access point configurations
- Runtime decoding of WEP packets for known networks
- Named pipe output for integration with other tools, such as a layer3 IDS like Snort - Multiplexing of multiple simultaneous capture sources on a single Kismet instance
- Distributed remote drone sniffing
- XML output
- Over 20 supported card types



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Common Kismet's applications

- Wardriving: Mobile detection of wireless networks, logging and mapping of network location, WEP, etc.
- Site survey: Monitoring and graphing signal strength and location.
- Distributed IDS: Multiple Remote Drone sniffers distributed throughout an installation monitored by a single server, possibly combined with a layer3 IDS like Snort.
- Rogue AP Detection: Stationary or mobile sniffers to enforce site policy against rogue access points.



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Proactive Measures

The following are some of the options available for reducing the effectiveness of discovery tools:

1. **Fake Access points**

Software such as Black Alchemy's Fake AP for Linux generates thousands of counterfeit beacons, to hide wireless LAN among fake APs

2. **Advanced Security Solutions**

Solutions such as 802.1x/EAP or VPNs are more effective than MAC filters WEP, and closed system for hiding SSID

3. **Awareness**

Employee and security personnel should be educated to recognize potential problems



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Password Capture & Decrypt Tools

- Weak passwords are one of the most serious security threats in networking.
- Intruders easily guess commonly used and known passwords such as **password**, **admin**
- Two auditing tools often used by administrators and hackers alike to view clear text passwords are **winsniffer** and **ettercap**
- **L0phtcrack** (now LC4) password auditing and recovery tool used on windows OS to crack the password hashes
- **LRC** (lucent registry crack) is used to decrypt stored encrypted hash WEP key from Proxim Orinoco PC cards

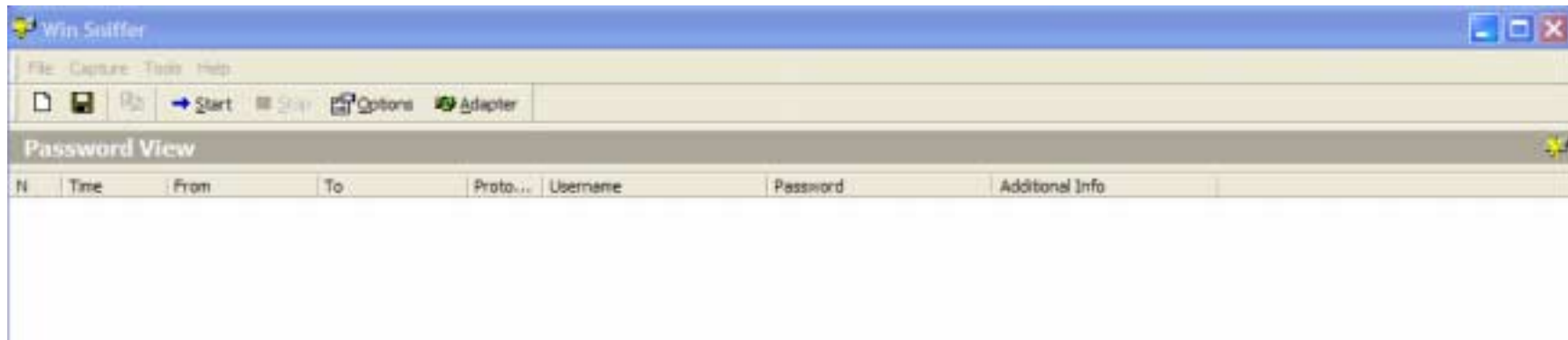


This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



WinSniffer



- You can copy it from <http://www.winsniffer.com>
- Win Sniffer allows network administrators to capture passwords of any network user.
- Win Sniffer monitors incoming and outgoing network traffic and decodes FTP, POP3, HTTP, ICQ, SMTP, Telnet, IMAP, and NNTP usernames and passwords.



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Features of WinSniffer

- It can promiscuously capture all packets from the current network segment.
- It is also able to decode FTP, POP3, HTTP, ICQ, SMTP, Telnet, IMAP, and NNTP passwords.
- Win Sniffer has one of the most intuitive packet filtering system, allowing you to look only at the desired packets.
- Win Sniffer can be left unattended for days watching your computers. All the captured data is written in log files and you don't have to worry about memory being exhausted.



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



ettercap

- Written by Alberto Ornaghi and Macro Valleri
- It can be downloaded from <http://ettercap.sourceforge.net>
- It is one of the most powerful password capture and auditing tools ,supported by almost every OS platform, and capable of gathering data even in switched environment.
- It uses **ncurses** as a menu style user interface



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Features available in ettercap

- Character injection into an established connection
- SSH support: user can analyze username and passwords, and even the data of the SSH1 connection .
- HTTPS support: A user can sniff HTTP-SSL data even if the connection is made through a Proxy
- Remote traffic through a GRE tunnel: A user can analyze remote traffic through a GRE tunnel from a remote router



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Features available in ettercap

- PPTP broker: A user can perform man-in-the-middle attacks against PPTP tunnels
- Plug-ins support : A user can create your own plug-in using the ettercap API
- Packet filtering/dropping: A user can configure a filter that searches for a particular string in the TCP or UDP payload and replace it with a new string
- OS fingerprinting
- Kill a connection
- Passive scanning of the LAN
- Check for other poisoners on the LAN
- Bind sniffed data to a local port
- Password collector for a whole series of protocols



L0phtcrack

- LC5 is the latest version of **L0phtCrack**, the award-winning password auditing and recovery application used by windows and UNIX administrators
- LC5 reduces security risk by helping administrators to:
Identify and remediate security vulnerabilities that result from the use of weak or easily guessed passwords
Recover Windows and Unix account passwords to access user and administrator accounts whose passwords are lost or to streamline migration of users to another authentication system
Rapidly process accounts using pre-computed password tables* that contain *trillions* of passwords
There are many different ways that L0phtcrack can capture password hashes, but two in particular are file share authentication and network logons



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



LRC tool

- Proxim Orinoco PC cards store an encrypted hash of the WEP key in the windows registry.
- The Lucent Registry Crack is a simple command line utility written to decrypt these encrypted values
- LRC can be downloaded from <http://www.cqure.net>



Share Enumerators

- Share Enumerators are software programs that can scan a windows subnet for open file shares.
- A common attack is to access another computer's windows registry and redefine the properties of a file share to root directory
- Legion is a popular freeware program from Rhino 9 group that quickly scans a subnet and lists all open file shares



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Network Management & Control

- Tools available that allow for remote access and management of windows server and workstations.
- Two such applications are Hyena from www.systemtools.com and LANBrowser www.firestormsoftware.com



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Network Management & Control

- Each of these management utilities can shut down services on remote computers including:
 - Email servers
 - Firewalls
 - Virus protection
 - ftp servers
 - Web servers
 - IDS



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Wireless Protocol Analyzers

- They can capture, decode, and filter wireless packets in real-time.
- They support multiple frequency bands such as those used in 802.11b and 802.11a networks.
- They do not attempt to connect or communicate with access points or other wireless peers .



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Wireless Protocol Analyzers

- There are many vendors, such as :
Wildpackets Airoppeek
AirMagnet
Fluke WaveRunner Wireless Tester
Ethereal
Network Associate Sniffer Pro Wireless
Network Instruments Observer
Epiphany CEniffer
Tamosoft Commview



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Wireless Protocol Analyzers

- A network administrator will use a packet analyzer to spot risks such as:
 - unencrypted wireless traffic
 - rogue wireless hardware and software
 - oversized RF cells
 - misconfigured security features (such as closed system)
 - exposed Network Layer info such as ip addresses



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Proactive measures

- Layer 2 or 3 encryption prevents hackers from gathering sensitive network traffic.
- Solutions might include:

Static or Dynamic WEP

IPSec or GRE

SSH2



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Manufacturer Defaults

- The most common mistake among administrators implementing new wireless setup is NOT changing of the defaults, which are published in the user's manual.
- There are websites that list all manufacturer's default settings from user manuals and store them in one text file for hackers



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Antennas & Wireless LAN Equipment

- The tools used for auditing a wireless network include Antennas, Wireless cards, a portable computer, and specialized software.
- Antennas can be **omni** to locate WLANs or a **directional** antenna to obtain a stronger signal
- **Lucent Gold PC Card, Cisco 350 PC Card, and Symbol LA-4121 PC Card** are three most popular PC cards



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



OS Fingerprinting & Port Scanning

- Hackers must start out by finding what OS and open ports are on the network, before weaknesses can be exploited.
- LANGuard Network Security Scanner www.gfi.com can quickly fingerprint an entire network.



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



OS Fingerprinting & Port Scanning

- These programs generate reports on:
 - Service packs installed on machines
 - Missing security patches
 - Network shares
 - Open ports
 - Services in use
 - Users and groups
 - Strength of passwords
 - known vulnerabilities and where to find the exploit



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Application Layer Analyzers

- decodes and reconstructs network traffic - such as emails, instant messages, Web-browsing sessions and more - in its original format.
- In other words, you can actually see the web pages viewed by a suspicious employee or follow the trail of a hacker through your network, to quickly determine whether company security has been compromised.
- IRIS from <http://www.extralan.co.uk/products/Diagnostic-Tools> is an example
- Iris even delivers a complete audit trail, giving you the evidence you need to take appropriate action against those committing malicious or non-compliant acts.



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Networking Utilities

- Most intrusion attempts start with a scan of the network.
- Networking utilities such as WS_Ping ProPack www.ipswitch.com or NetscanTools Professional www.netscantools.com can perform ping sweeps for ip addresses, port scans, and computer name resolution.

next more detailed probes can be accomplished with tools such as LANGuard



Networking Discovery Tools

- Management software package, such as What's Up Gold www.ipswitch.com
SNMPc www.castlerock.com
Solarwinds www.solarwinds.net
Have network node discovery tools that uses SNMP to map their way through an enterprise, and discover network devices automatically to create logical views of your network



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



RF Jamming Tools

- RF jamming tools allow auditors to force users to roam and to introduce interference to examine the stability of certain technology such as FHSS in a noisy environment
- Intruders use them for DOS and hijacking
- Example YDI.com's PSG-1 is used to test antennas, cables, connectors for wireless devices becomes a jamming device, when gets connected to high gain antenna.



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Hijacking Tools

- A hacker can jam the signal of a valid AP, forcing the client to associate with the access point software running on the hacker's laptop.
- The following are some of the programs available for this purpose:
- ZoomAir AP (Windows) <http://www.zoom.com>
- Cqure AP (Linux) www.cqure.net
- Orinoco Client Utility (Base Station mode)



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



WEP Decryption Tools

- A significant amount of data (apx 5-10 million packets) is required to decrypt the keys
- Popular WEP crackers include:
AirSnort <http://airsnort.shmoo.com>
WEPcrack <http://sourceforge.net/projects/wepcrack>
They run in UNIX based environments.
use physical security and security solutions stronger than static WEP keys to prevent such an occurrence



Operating System Exploit Tools

- Security scanner tools, such as LANGuard, can point out operating system exploit opportunities.
- One exploit in particular for windows is the default setting for the windows registry to accept remote connections in wireless environment.
- Proactive measures to install OS updates.



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Homeplug Devices

- These are new devices that use a building's electrical wiring for data transmission.
- Administrators should sweep on regular bases, and IDS should be used when possible.



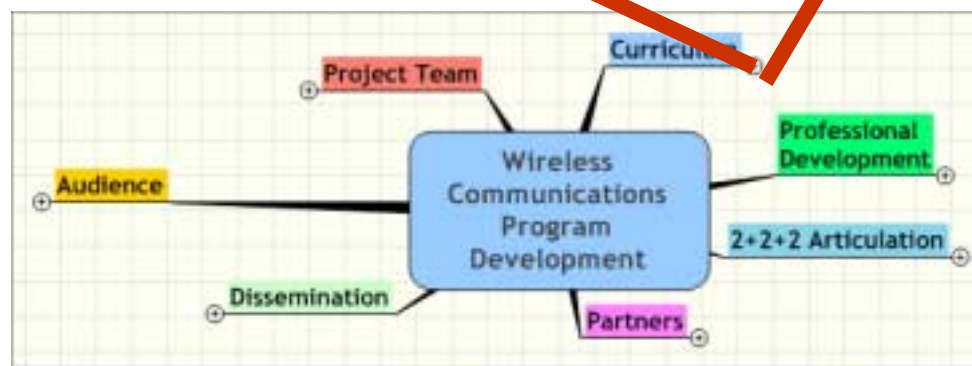
This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



- Market Relevant
- Modular
- Competency Based
- Work Based Learning Units
- Integration of "Soft Skills"
 - Teamwork
 - Problem Solving
 - Leadership
 - Communications
 - Life Long Learning

- Well Articulated with BS Degree Programs
- Industry Driven
- Integrate "Best Practices"
- Industry Skill Standards
- Industry Certifications



2 Year AAS Wireless Communications (Proposed)

<u>Semester 1</u>		<u>Semester 2</u>	
Writing	3	Speech	3
Introduction to Wireless	3	Introduction to Security	3
Fund. of Telecommunications	3	Wireless LANs	3
Introduction to Networking TCP/IP	3	ELEC 105 or ELEC 106	3-4
Humanities/Social Science	3	Humanities/Social Science	3
	15		15-16



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



2 Year AAS Wireless Communications (Proposed)

<u>Semester 3</u>		<u>Semester 4</u>	
Cellular / Broadband Technologies	3	Capstone Course	3
Network Operating Systems	3	Advanced Topics in Wireless	3
Applied Wireless Security	3	Advanced Security	3
Math/Science/Technology*	3	Tech Elective	3-4
Free Gen Ed	3	Free Gen Ed	3
	15		15-16

*** MATH 263 Applied Calculus required for transfer students**



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



1-Year Security Certificate (Proposed)

<u>Semester 1</u>		<u>Semester 2</u>	
Writing	3	Speech	3
Introduction to Wireless	3	Applied Wireless Security	3
Introduction to Security	3	Disaster Recovery	3
Introduction to Networking TCP/IP	3	Forensics	3
Network Operating Systems	3	Advanced Security	3
	15		15



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



1-Year Wireless Certificate (Proposed)

<u>Semester 1</u>		<u>Semester 2</u>	
Writing	3	Speech	3
Introduction to Wireless	3	Applied Wireless Security	3
Introduction to Security	3	Wireless LANs	3
Introduction to Networking TCP/IP	3	Cellular/Broadband Technologies	3
Network Operating Systems	3	Advanced Topics in Wireless	3
	15		15



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Key Takeaways!

Opportunities

- 1.9 billion mobile connections by 2008 (Ovum 2003)
- 1.25 million subscribers per week sign up in China every week (Vision Gain, 2003)
- 100 million Java enabled handsets in 2003, growing to 878M by 2007 (Arc, 2002)
- 64 million US homes on broadband by end of 2003 (strategy Analytics Global, 2003)
- Data usage growing from 16% of ARPU to 49% in 2006 (Yankee, 2002)
- Steady adoption of VoIP: 66% growth of IP PBX systems in 2003 (IDC, 2003)



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Key Takeaways!

Opportunities

- The number of mobile connections in North America grew to more than 196.3 million in the fourth quarter of 2004. This was a 14.2 percent increase compared with one year ago. Net additions in the quarter in the U.S. were the highest recorded to date, reaching 7.4 million. (Gartner, 8 April 2005)
- 1Q05 Telecommunications services and equipment revenue grew to \$1.41 trillion in 2004 and will be \$1.78 trillion in 2009. Revenue for the terminal market achieved significant growth of 23 percent in 2004 compared with 2003. (Gartner, 28 March 2005)

"convergence of the computer, telephone and wireless markets is taking place. The future of medical organizations, automotive companies, computer equipment manufacturers and software design companies, utility companies, among others, is becoming dependent upon wireless device integration."- 1999 *GWEC White Paper*



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Key Takeaways!

Where Every Company is Going



Network Computing

Wireless/IT/Connectivity

Attack Cost and Complexity
Accelerate Service Deployment
Unleash Mobility with Security

- Academic institutions need to make **Wireless/IT/Connectivity** a key focus for the future of the US economic development
- Community colleges, universities, and high schools will need to work more closely to ensure a sufficient number of experts in the workforce
- That is what we are beginning to do through **Partnerships and Collaboration**

How do you predict the future? That's easy. How do you ***create the future?*** That's hard. -Robert X. Cringely



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Thank You!

**Michael Qaissaunee,
MAITT Principal Investigator/Director
NCTT Co-Principal Investigator, Open Content
(mqaissaunee@brookdalecc.edu)
Brookdale Community College
765 Newman Springs Road
Lincroft, NJ 07738
732-224-2879**

**Mohammad Shanehsaz,
MAITT Co-Principal Investigator/ Asst Director
(mshanehsaz@brookdalecc.edu)
Brookdale Community College
765 Newman Springs Road
Lincroft, NJ 07738
732-224-2827**

This work is supported by the
National Science Foundation under
Grant Number DUE 0302909



Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.



Resources used

- www.netstumbler.com
- CWSP from Mc Graw Hill
- <http://www.kismetwireless.net>
- <http://www.dachb0den.com/projects/bsd-airtools.html>
- <http://www.winsniffer.com>
- <http://www.extralan.co.uk/products/Diagnostic-Tools>
- <http://ettercap.sourceforge.net>



This work is supported by the
National Science Foundation under
Grant Number DUE 0302909

Any opinions, findings and conclusions or recommendations
expressed in this material are those of the author(s) and do not
necessarily reflect those of the National Science Foundation.

