Creating a Wireless Investigation Toolkit

Basic Hardware and Software Specifications

Chris Armstrong camstrong@search.org

In today's Hi-Tech world, it is common place for a law enforcement investigator to encounter a wireless network. In conjunction with **SEARCH's Advanced Responders: Search and Seizure of Networks** course, SEARCH is pleased to offer this whitepaper on hardware and software needed to put together a wireless toolkit.

SEARCH's Advanced Responders: Search and Seizure of Networks http://www.search.org/programs/hightech/courses.asp

The following handout is a compilation describing the basic hardware and software needed to help the investigator identify and recover data from a wireless network. The Training Services staff of SEARCH Group, Inc. in cooperation with law enforcement agencies around the United States, developed these specifications.

The world of wireless networking hardware is ever changing. An investigative budget must include funding to cover the investigative agencies current needs as well as funding to keep pace with the hardware and software upgrades of the future.

The products listed here are not intended to be part of an exclusive or exhaustive list, they are merely examples of what's currently available. Where prices are listed, those numbers are approximate. If you would like specific purchase recommendations or have suggestions of hardware and software to add to the list, please contact SEARCH Training Services Staff at 916/392-2550.

You will need the following tools:

Wireless Network Investigation Hardware and Software

Hardware

Laptop Computer

Wintel Laptop with PC card slot

You will need a laptop computer with a least one PC card slot to sniff for and identify wireless networks and to interrogate a suspect's router

• ORINOCO 802.11 b/g PC Gold Card – Proxim Wireless

Connector for external Range Extender Antenna http://www.proxim.com/products/cp/pc.html

Available from multiple sources

www.amazon.com or www.pcconnection.com are two examples.

Orinoco Gold b/g cards - \$66.42



ORINOCO. Classic Gold PC Card

The ORiNOCO 11b/g PC Card gives you the flexibility to connect to any 802.11b or 802.11g wireless network. Just plug the 11b/g PC Card into the Cardbus slot of your notebook computer and you have everything you need for maximum wireless productivity in an enterprise, public building or at home. The 11b/g PC Card is part of ORiNOCO's nice family of client and infrastructure products - everything you need to work anytime, anywhere and the way you want.

The Orinoco PC card in conjunction with the Yagi Antenna and Laptop will be used to sniff for and identify wireless networks

Yagi Antenna - Netgate www.Netgate.com ANT-9Y-NF 9db Yagi antenna Contact: Bill Hallett [bill@netgate.com] ~\$37.00



Pigtail Cable - Fleeman Anderson & Byrd www.fab-corp.com 5' Pig-tail Orinoco(MC) to N-Male (to connect Orinoco Gold Card to Yagi Antenna) ~\$10.99



Zap Checker - Signal Checker and Antenna - ZAP www.zapchecker.com

Model 270 with antenna depicted Controls:

> 2 Display Modes - An Analog meter and colored LED's (which are readable from a distance and at nighttime). An adjustable sensitivity knob 3 detection modes:

A switch-enabled silent vibrator ~\$320.00



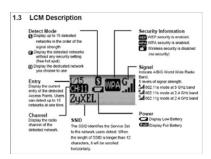
ZAP CHECKER products are ultra-sensitive instruments that detect and display Radio Frequency (RF) signals over a broad span of frequencies. They are a new generation of RF measurement tools that employ recently introduced IC technology to measure from very weak to ultra strong signals and differentiate analog from digital communications. They are ideal for wireless installations, detection of covert devices (routers, wireless hard drives, wireless cameras), and detecting and locating undesirable signal sources such as interfering transmissions, RFI, noise and leakage.

• **ZyXel** - ZyXEL Communications

www.zyxelguard.com

AG-225H WiFi Finder & USB Adapter (a handheld wireless access point detection tool) ~\$70.00





The ZyXEL AG-225H makes it easy to find a wireless hotspot when you are on the road. The dual-band tri-mode USB adapter is equipped with a high contrast LCD screen and built-in LiON battery, which allows you to scan the environment for hotspots without being attached to your notebook computer. From the graphic LCD display, users can scroll through hotspots to view information such as SSID, encryption requirements, signal strength, band used, and channels used.

• Targus Wireless WIFI Detector - Targus

Handheld WIFI receiver for 801.11b/g – detects networks

Targus Corporation

 $\underline{\text{http://targus.com/us/CategorySearch.asp?SearchedTerms=ACW20US\&Action=Go}}\\$

Model ACW2OUS

(a handheld wireless access point detection tool)

~\$60.00



The Targus WiFi Scanner makes it easy to find and connect to hot spots on the road. Lightweight and portable the ACW20US can conveniently be carried on a keychain or attached to your notebook case for easy access. Simple to operate, just push one button to activate, it will detect WiFi (802.11b/g) access points, identify the signal strength and display it on easy to read LCD. With the ability to identify each access point efficiently, you can see what is available before you turn on your notebook computer.

** NOTE: Although having both the Targus and the ZyXel are nice, you can get away with one or the other. The Targus is smaller and easier to use in a covert situation. The ZyXel comes with software giving you the ability to download and save the results of your hotspot search.

SpyFinder

Optical Camera Detector Available from multiple sources

~\$200.00



The Spy Finder reveals the presence of any camera, wired or wireless, even if the power is off.

Cat5 or 6 Ethernet Cable 6' and 10'

Available from multiple sources

~ Price varies with length

You will need the Cat5 or 6 Ethernet cable to connect your agency laptop to the suspect's router to gather router settings and DHCP lease tables. These are available from multiple sources. Cat6 Ethernet cable will allow for higher transfer rates than Cat5.



• Crossover Adapter

- o Available from multiple sources
- o ~\$4.00

Need to connect two computers without using a hub or a switch. A high performance crossover adapter is an economical way to easily convert a standard patch cable into a crossover.



Software

SEARCH Toolbar

Investigators continually strive for ways to streamline and enhance their investigations. To aid investigators conducting online, cellular telephone, or wireless investigations, SEARCH has created an investigative aid called the SEARCH Investigative Toolbar.

The toolbar contains a number of drop down buttons that when clicked upon provide the investigator with pre-configured online investigative links.

You can download the SEARCH Investigative Toolbar at the following URL: http://searchinvestigative.ourtoolbar.com



 Network Stumbler v 0.4.0 – Marius Milner (Free Download) can be found on Netstumbler web site http://www.netstumbler.com

Used with laptop computer, Yagi antenna and pigtail, Network Stumbler allows you to scan for Wireless Access Points with greater detail than either the Targus or ZyXel wireless detection tools

Kismet – Mike Kershaw

(Free Download) can be found on SourceForge or, "BackTrack" Remote Exploit CD http://www.remote-exploit.org/backtrack.html

Kismet is an 802.11 wireless network detection, sniffer and intrusion detection tool. The program primarily runs under the Linux and Mac OS X. The client can also run on Windows, but it's very hard to set up and difficult to use.

Kismet is one of the many tools to be found on the "BackTrack" Remote Exploitation CD.



Network Scanner v 3.8.177 – SoftPerfect

(Free Download)

http://www.download3k.com/SoftPerfect-Network-Scanner/Download-Freenetscan.exe.html

SoftPerfect Network Scanner is a free multi-threaded IP, NetBIOS and SNMP scanner with a modern interface and several advanced features. It is intended for both system administrators and general users who are interested in computer security. The program pings computers, scans for listening TCP ports and displays which types of resources are shared on the network (including system and hidden).



SoftPerfect Network Scanner

AirSnare v 1.2.11 – Digital Matrix

(Free Download)

http://www.download.com/AirSnare/3000-2092 4-10255195.html

AirSnare is another tool to add to your Wireless Intrusion Detection Toolbox. AirSnare will alert you to unfriendly MAC addresses on your network and will also alert you to DHCP requests taking place.

• Helix v 1.9a - e-fense

(Free) can be found on e-fense web site http://www.e-fense.com/helix/

Helix is a bootable CD originally based upon Knoppix, with an emphasis on Incident Response & Computer Forensics.



 Knoppix v 5.1 – Klaus Knopper (Free) can be found on Knoppix web site http://www.knoppix.org

KNOPPIX is a bootable Live system on CD or DVD, consisting of a representative collection of GNU/Linux software, automatic hardware detection, and support for many graphics cards, sound cards, SCSI and USB devices and other peripherals. Knoppix is a great preview tools as it does not write to a Windows partition so it will not change original evidence in any way.



• Panda Anti-Rootkit v 1.06.00 – Panda Security

(Free)

http://www.antirootkit.com/software/Panda-Anti-Rootkit-Tucan.htm

Panda Anti-Rootkit is a program that uses latest generation technology to detect and remove Rootkits or Trojans Horse Viruses. Rootkits are programs designed to hide processes, files or Windows Registry entries. This type of software is used by hackers to hide their tracks or to insert threats surreptitiously on compromised computers. There are types of malware that use rootkits to hide their presence on the system.

• **Sysinternals Process Explorer** – Microsoft

(Free)

www.sysinternals.com

Whether you're an IT Pro or a developer, you'll find Sysinternals utilities to help you manage, troubleshoot and diagnose your Windows systems and applications. Process Explorer is a tool for looking under the hood to see what processes are running, what they are doing and the resources they are consuming.



Sysinternals Process Explorer

• **SNAGIT** v 9 – TechSmith

(Free Trial Version)
Purchase Price ~\$49.95

http://www.techsmith.com/download/trials.asp

Capture anything you see on the screen. Edit and combine those captures. Share them via your favorite applications. Organize and find them again later. The more you use SnagIt, the more ways you'll find to use it!



• !Quick Screen Capture v 3.0 – Etrusoft

(Free)

http://www.etrusoft.com/#!quick%20screen%20capture

!Quick Screen Capture is such a powerful screen capture and image editing utility.

• VLC Media Player v 0.8.6 – VideoLAN

(Free)

http://www.videolan.org/vlc/

VLC media player is a highly portable multimedia player for various audio and video formats (MPEG-1, MPEG-2, MPEG-4, DivX, mp3, ogg, ...) as well as DVDs, VCDs, and various streaming protocols. Additionally, VLC will play incomplete files recovered with Forensic tools.



• WirelessKeyView v 1.17 – NirSoft

(Free)

http://www.nirsoft.net/utils/wireless_key.html

WirelessKeyView recovers all wireless network keys (WEP/WPA) stored in your computer. It allows you to easily save all keys to text/html/xml file, or copy a single key to the clipboard.

• ZeroView

(Free)

http://www.techpathways.com/DesktopDefault.aspx?tabindex=8&tabid=14

"Ever worry that the system you are seizing uses whole disk encryption? Use ZeroViewTM freeware to find out." Burn ZeroView to a CD then pop it into the CD drive of the suspect machine and it will load into memory only and display the contents of Sector 0 allowing you to determine if whole disk encryption is employed on the suspect system. Once you know, then you can take the appropriate steps to capture and preserve the data you need.