

Examining Wireless Access Points and Associated Devices

Sgt. Christopher Then, CISSP, EnCE
Computer Crimes Unit
Morris County Prosecutor's Office
Morristown, NJ 07963
cthen@co.morris.nj.us

September 17, 2006

Wireless access for the home has become the preferred choice of connecting computers to the Internet. As law enforcement, we must be aware that while conducting search warrants or furthering an investigation, all associated wireless devices are located.

When an investigator can examine the active status of wireless access points, it is possible to corroborate or disprove statements based on their stored information. For example, a suspect may state that he owns one wireless laptop. It is possible, and even likely, that a technically savvy person would have one computer for legitimate use and one for criminal use. Without a proper wireless network assessment during a search warrant, crucial evidence may be left behind.

This paper will describe methods of examining a wireless access point and to determine if associated devices are present or have been present within a wireless network. The objective of this paper is to provide computer forensic examiners a resource to locate associations within a wireless network.

An association between a wireless access point and a wireless access device is simple. If the wireless device can communicate by passing network packets between the device and the access point, it is associated. In some instances, an association will occur only with wireless equipment matching MAC (Media Access Control) addresses set within the access point. This is also known as MAC filtering. The MAC address format is usually displayed as a string of 12 hexadecimal digits separated by colons, for example FF:01:02:AB:01:02. In other instances, the use of a pre-shared key (PSK) and/or the use of encryption must be applied to allow an association. Using the techniques described in this paper, an investigator can determine if encryption and/or MAC filtering is set, all without touching the access point. If active traffic is being sent between the access point and the associated device, your wireless forensic laptop can display network packet statistics. This paper will also describe methods an examiner can use to locate the associated devices and link them to wireless access points.

Before conducting any of these tests, your search warrant application should include the proper language to perform on-site examination of computer and computer-related equipment. Another word of caution – *only* test the following procedures on equipment you are permitted to do so.

During the execution of a search warrant, forensic examiners will determine the need for performing a live examination of wireless equipment, especially access points. If so, examiners should be aware of:

1. The active wireless access points physically located within the search warrant scene.
2. External wireless access points with signal coverage that overlaps the search warrant scene.
3. Which devices connect or are actively connected to associated access points.
4. The approximate range (footprint) and signal strength of the examiner's wireless network card.

The examiner's necessary hardware will be a laptop and a wireless network card that can be set to "promiscuous" or "open" mode. Most wireless cards are preset to receive only network traffic specifically addressed to them. Promiscuous mode will allow the card to receive all wireless network traffic within range. Research on different wireless cards show that PCMCIA or USB wireless cards are recommended, utilizing either the Atheros or Prism chipset. A listing of these recommended cards and drivers are found at the end of this paper. Another source of wireless cards can be found on line at: <http://forums.remote-exploit.org/showthread.php?t=2191>. The hardware equipment I utilized to conduct the following tests are; a basic Dell Latitude D820 laptop (CD/DVD drive, wired network jack, Windows™ XP Operating System), and a Proxim/Orinoco Gold 8470-WD PCMCIA wireless networking card. If possible, look for a wireless network card that has an external antenna jack. Adding an antenna to your wireless card will greatly increase your "listening radius". The use of a directional Wi-Fi antenna can direct your listening coverage to a specific direction.

The software portion consists of a set of tools created by Christophe Devine and Thomas d'Otreppe called "aircrack-ng". The aircrack-ng tool-kit can be downloaded for either Windows™ or UNIX/Linux at www.aircrack-ng.org. Currently, the aircrack-ng suite consists for five major programs: aircrack-ng, airodump-ng, aireplay-ng, airdecap-ng, and airmon-ng. Another way to use the aircrack-ng tools is to download a bootable "live-distribution CD". The live-CD utilized in this demonstration is called BackTrack and can be located at <http://www.remote-exploit.org/index.php/BackTrack>. The purpose of using BackTrack will be to use airodump-ng to determine which equipment, if any, is actively associated with a wireless access point. Airodump-ng will allow you to receive wireless packets within your listening area and will be essential for your wireless network assessment. Your forensic wireless laptop will be required to boot from the BackTrack CD. Once you have BackTrack running properly on your laptop, the first step will be to run "airdump-ng". The version of airodump-ng used in this paper is 0.5.

Once the search warrant is underway, a visual inspection of broadband modems will quickly determine if a wireless access point is physically connected. Investigators should be able to determine if a home network utilizes cable, DSL, or other method of

connecting to the Internet. Investigators should also be aware that a residence may employ more than one broadband modem or wireless access point.

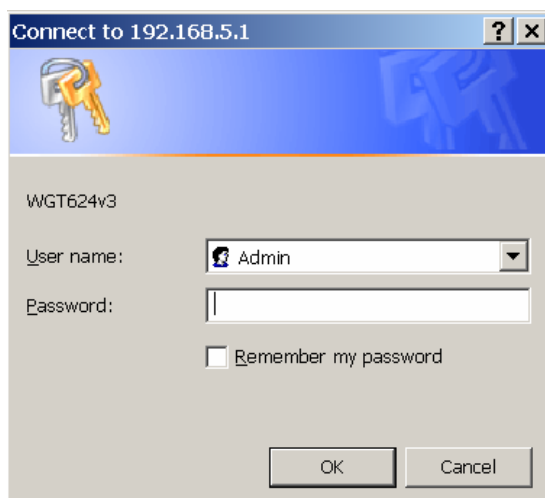
The footprint (signal coverage) of a wireless access point may be as small as a few hundred feet or as large as several city blocks. If a wireless access point is physically located, the initial goal is to determine its associated devices by directly connecting to it via a network cable.

Step 1: Direct-connect to the wireless access point

The examiner should have a standard network cable and a laptop computer with a standard network adapter. Connect the network cable between the laptop and wireless access point and determine if the laptop is assigned an IP address. If the access point and your forensic laptop has DHCP enabled, the laptop should automatically be assigned an IP address. This IP address should follow the private IP address scheme and in most cases, the wireless access point will be within the same Class C network range as your laptop, with the last octet of the access point being the number “1”. For example, if your laptop is assigned the IP address 192.168.1.100, the wireless access point will most likely be 192.168.1.1.

Another method of determining the wireless access point IP address is to run the “ipconfig” command from a Windows™ command prompt on your forensic laptop. After executing ipconfig, the results showing “default gateway” is most likely the IP address of the wireless access point.

Using an internet web-browser program, type the IP address of the wireless access point into the address bar. You may see a login window appear similar to the one shown below:



In many instances, the customer does not change the default administrator account for the wireless access point. If you look at the brand of the access point, you can attempt

to login using the default administrator credentials. A list of default credentials can be found at:

<http://www.governmentsecurity.org/articles/DefaultLoginsandPasswordsforNetworkedDevices.php>

A good, updated list of default access credentials should be part of every forensic examiners tool-kit. If you are successful in logging into the access point, you should see something similar to the following: (in this case, a Belkin 54G wireless access point is shown)

Address <http://192.168.2.1/>

BELKIN Cable/DSL Gateway Router Setup Utility Home| Help| Login

LAN Setup

- LAN Settings
- DHCP Client List
- Internet WAN**
- Connection Type
- DNS
- MAC Address
- Wireless**
- Channel and SSID
- Security
- Use as Access Point
- Wireless Bridge
- Firewall**
- Virtual Servers
- Client IP Filters
- MAC Address Filtering
- DMZ
- WAN Ping Blocking
- Security Log
- Utilities**
- Parental Control
- Restart Router
- Restore Factory Default
- Save/Backup Settings
- Restore Previous Settings

Status

You will need to log in before you can change any settings.

Version Info	
Firmware Version	4.05.03
Boot Version	2.01.09
Hardware	F5D7230-4
Serial No.	BEL1R17L

LAN Settings	
LAN/WLAN MAC	00:11:50:53:9A:23 / 00:11:50:53:9A:24
IP address	192.168.2.1
Subnet mask	255.255.255.0
DHCP Server	Enabled

Internet Settings	
WAN MAC address	00:11:50:53:9A:23
Connection Type	Dynamic
Subnet mask	255.255.255.0
Wan IP	192.168.1.47
Default gateway	192.168.1.1
DNS Address	192.168.1.1

Features	
NAT	Enabled
Firewall Settings	Disabled
SSID	belkin54g
Security	Enabled

If you are unsuccessful, the owner of the wireless access point (or another party) may have changed the default password. If the owner is not cooperative or unable to provide the password, the direct access method will not work. Under no circumstances should you attempt to hard-reset the wireless access point. A hard-reset will return the access point to factory settings and erase potential evidence.

However, if you are able to login to the access point, a wealth of information can be gathered and saved. It is important that an examiner record all security settings, access point status, network IP addresses, and especially the MAC addresses of attached equipment. The MAC address list may also provide an investigator with probable cause to continue searching for other related computer equipment. On most wireless access points, a listing of associated MAC and IP addresses can be found in a client list. Keep in

mind that the access point will not record MAC addresses of computers that have had their networking information set manually. The client list will only show associated clients that have been assigned an IP address. On this particular access point, the DHCP client list can be accessed by clicking on the “DHCP Client List” located on the upper-left column of the page. A typical list of attached client computers is shown in the next screen-capture.

Address http://192.168.2.1/lan_dhcp.html

BELKIN Cable/DSL Gateway Router Setup Utility Home | Help | Log

LAN > DHCP Client List

This page shows you the IP address, Host Name and MAC address of each computer that is connected to your network. If the computer does not have a host name specified, then the Host Name field will be blank. Pressing "Refresh" will update the list.

IP Address	Host Name	MAC Address
192.168.2.2	CMV - Lab -1	00:12:3f:2b:ec:a1
192.168.2.4	SLATE1	00:11:85:5e:01:2e

If you are assigned an IP address while physically connected to the access point, a “ping-sweep” may reveal other connected devices. Associated computers should respond to a ping request unless protected by hardware or software firewalls. An excellent piece of software, nmap, can be used to perform ping-sweeps and many other useful functions. This tool can be downloaded for free at <http://insecure.org/nmap/download.html>. This tool is also included with the BackTrack CD distribution.

In the next example, a different access point will be scanned. The IP range to be searched is 192.168.5.X. Keep in mind that there may be any number of different IP addresses and not necessarily within the same class C network. From a command prompt, execute the following:

```
nmap -sP -v 192.168.5.0/24
```

The results should show a scan of the entire Class C network from 192.168.5.0 to 192.168.5.255, complete with MAC addresses and vendor information. To find more about a specific piece of equipment, execute the command:

```
nmap -sS -A 192.168.5.1
```

The results of the nmap command “nmap -sS -A 192.168.5.1” show quite a bit of information about the access point.

```
C:\nmap>nmap -sS -A 192.168.5.1

Starting Nmap 4.11 ( http://www.insecure.org/nmap ) at 2006-08-29 21:36 Eastern
Standard Time
Interesting ports on 192.168.5.1:
Not shown: 1677 closed ports
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  Linksys WRT54G router telnetd ($veasoft firmware)
80/tcp    open  http    Linksys wireless-G WAP http config (Name DD-WRT)
443/tcp   open  ssl     OpenSSL
MAC Address: 00:13:10:32:9C:2F (Cisco-Linksys)
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux 2.4.0 - 2.5.20
Uptime 2.019 days (since Sun Aug 27 21:10:21 2006)
Service Info: Devices: router, WAP

Nmap finished: 1 IP address (1 host up) scanned in 11.188 seconds
C:\nmap>
```

To view expanded information on an entire network subset, you would use the command:

```
nmap -sS -A 192.168.5.0/24
```

The entire network subset scan may uncover additional connected equipment, as shown below. This particular laptop has a software firewall enabled, however, the MAC address and vendor information can still be recorded.

```
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
All 1680 scanned ports on 192.168.5.101 are filtered
MAC Address: 00:90:4B:D8:33:28 (GemTek Technology Co.)
Too many fingerprints match this host to give specific OS details

Nmap finished: 256 IP addresses (3 hosts up) scanned in 68.000 seconds
C:\nmap>
```

Even if you are successful in logging into the access point and “nmapping” the network, you may still want to use step two to determine the active state of connected wireless equipment.

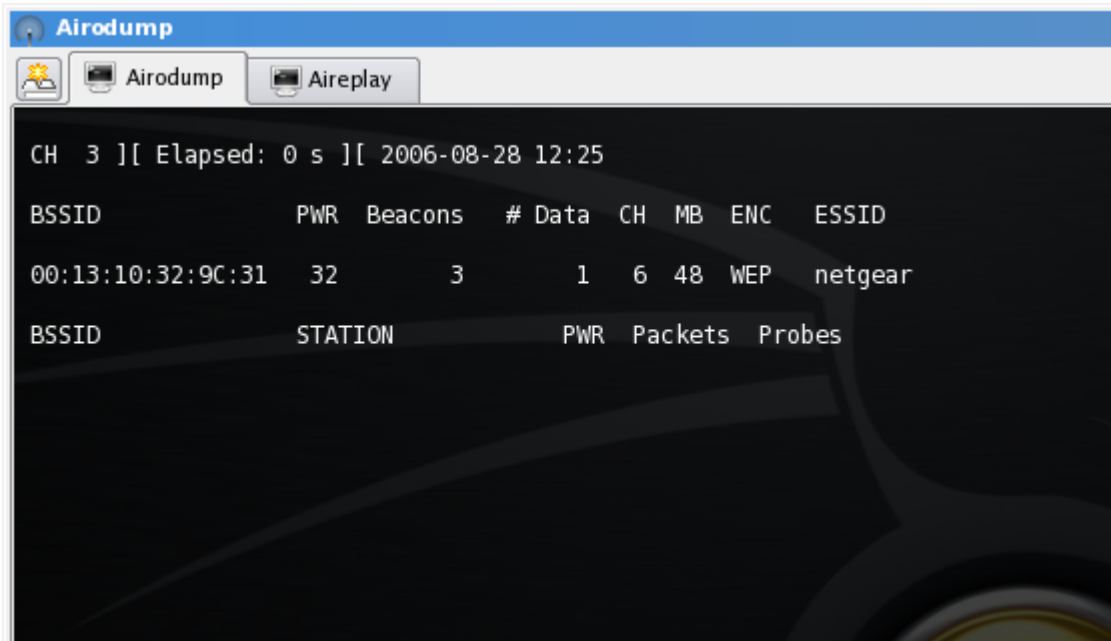
Step 2: “Sniffing” traffic between the access point and associated devices.

This method will allow the investigator to place their wireless laptop in promiscuous mode. This mode allows the radio to scan all available wireless channels and capture information within range. In the first example, I will show how BackTrack can be used to find associated wireless equipment.

Using BackTrack to find associated wireless networking equipment

This time, the goal of using BackTrack is to determine which equipment, if any, is actively associated with a wireless access point. If you have BackTrack running properly on your laptop, the first step will be to run the program “airodump-ng” (<http://www.aircrack-ng.org>).

The Airodump program can be accessed by a command prompt (type “airodump-ng” for command options) or by selecting “Aircrack suite” from the BackTrack program menu. The first run of this program will be in “scan” mode, which will check through all wireless channels while searching for access points. The screen figure below shows airodump running in scan mode.



The screenshot shows the Airodump application window with a dark background and white text. The window title is "Airodump" and it has two buttons: "Airodump" and "Aireplay". The main display area shows the following information:

```
CH 3 ][ Elapsed: 0 s ][ 2006-08-28 12:25
```

BSSID	PWR	Beacons	# Data	CH	MB	ENC	ESSID
00:13:10:32:9C:31	32	3	1	6	48	WEP	netgear

BSSID	STATION	PWR	Packets	Probes
-------	---------	-----	---------	--------

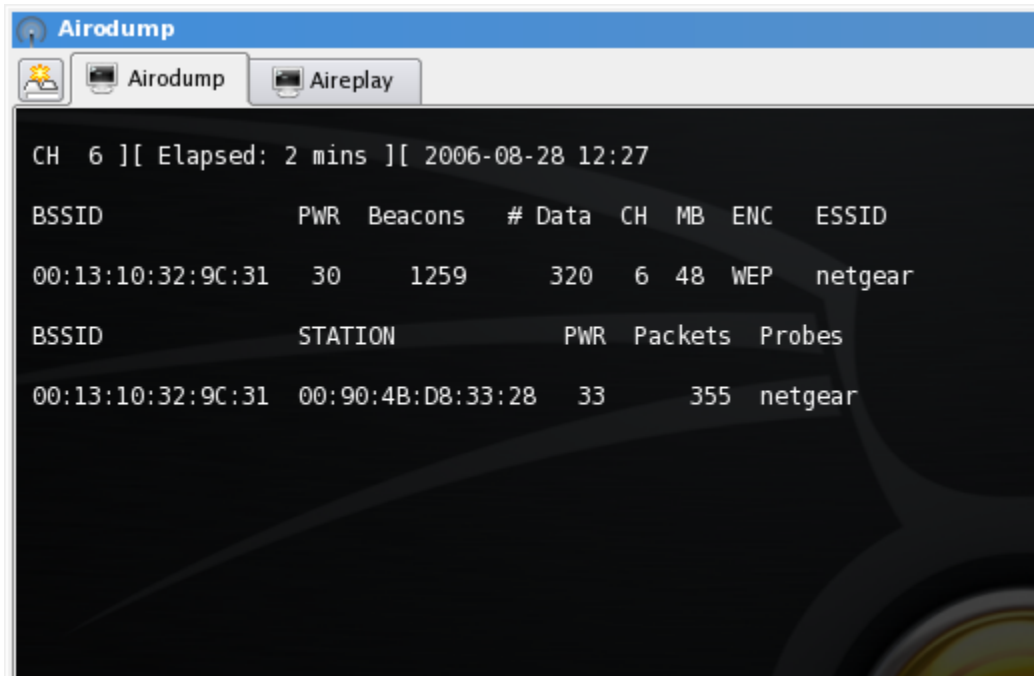
The BSSID column shows the MAC address of an access point. PWR describes the relative strength of the wireless signal as received by your location. “Beacons” show the number of beacon packets received, “# Data” show the number of packets that have the ability of being decrypted. MB describes the current rate of data transfer in megabits per-second. ENC shows the level of encryption set on the access point. You may need to

collect several data packets for the program to recognize the level of encryption. ESSID shows the broadcasted device name (also called a SSID). The columns “BSSID”, “CH” and “ESSID” are the ones we are most interested in for the initial run of airodump.

Before continuing, confirm you are viewing the correct access point. On most wireless devices, the MAC address is displayed on a label on the wireless access point. This MAC address should correspond with your scanning results, along with a strong signal reading.

If the targeted access point is displayed on your screen, make note of the channel (CH) setting. In this example, the “netgear” wireless router is operating on channel 6. Once a channel is determined, we want to concentrate on that single channel. The next time airodump is run, we will select only channel 6 to listen to traffic.

You may stop the execution of airodump by pressing “Ctrl-C” or clicking the window-close button. Restart airodump, except in this instance, you would add the switch “-c 6” to designate that you only want to listen to channel 6. You should see something similar to the screen shown below.



Using the web-site www.coffer.com/mac_find, you can enter a MAC address and determine the vendor information. In this example, I search the MAC address of the listed BSSID using the link http://www.coffer.com/mac_find/?string=001310329C31 (notice the MAC address is at the end of the link) and notice that this MAC address is associated with a Cisco/Linksys product, not Netgear. It is easy to change the ESSID to something else. It is also possible to change the MAC address within networking

equipment. Investigators need to be aware that software settings make it very easy to disguise equipment.

The example shows that within two minutes, an associated device has appeared. This device has the MAC address of 00:90:4B:D8:33:28 and is actively communicating with the “netgear” access point. It is important to mention that the examiner should concentrate on the “Packets” column in the association list. The “Beacons” column does not reflect data passing between the access point and associated equipment. The number in the associated list “Packets” column will increase with network activity. A search on that particular MAC address reveals that the vendor is Gemtek Technology, not particularly helpful since it does not reveal the make and type of the related computer equipment (in this case, a Gateway laptop). Since we can see that the access point has WEP encryption set, we can conclude that the connection of the device to the access point was made by someone having knowledge of the WEP key or pass-phrase. It should be noted that if airodump cannot determine the state of encryption on the access point, the ENC portion will display “WEP?”. Airodump requires several packets to make a determination of the type of encryption being used.

During a computer-related search warrant, one of the first and most important steps is to not allow anyone access to electronic devices. So, unless the computer equipment is actively communicating with the access point, how can you determine if there are additional devices? Sending a de-authentication packet using the program “aireplay” may force active wireless equipment to reconnect to the default wireless access point, revealing them to our forensic laptop.

Aireplay is an additional wireless assessment tool found within the aircrack portion of the BackTrack folder. This program has the ability to inject specially crafted data packets into the wireless stream. In this example, we will use aireplay’s ability to fool the connected equipment into thinking the access point is malfunctioning. Once the equipment is de-authenticated, the wireless devices should attempt to re-connect to that access point. Investigators should be aware that many newer wireless devices reject de-authentication packets. You must keep the airodump program running while sending the de-authentication packets. If the wireless devices are active, you may see them appear as they attempt to reconnect to the network. In this example, we’ll send de-authentication packets using aireplay.

Aireplay utilizes a specific command to send de-authentication packets. According to the user instructions found at <http://www.aircrack-ng.org>, utilize the command

```
aireplay-ng --deauth 5 -a {MAC of AP} {interface}
```

where the MAC after the “-a” is the MAC address of the access point and the “interface” will be the type of your wireless network card. The process of injecting data packets is difficult. Currently, only a handful of wireless network cards are capable of de-authenticating other devices, and this function currently only works in the UNIX/Linux version of aireplay.

An easier method of forcing associated wireless equipment to reconnect is by simply unplugging the access point and plugging it back in. When plugging the access point back in, make sure that the reset button is NOT pressed. Again, make sure that airodump is running when you power on the access point. Also, do not allow too much time to elapse before reattaching the power. Wireless devices may cease attempting to connect to a previously functioning access point. Three to five seconds of inactivity should suffice.

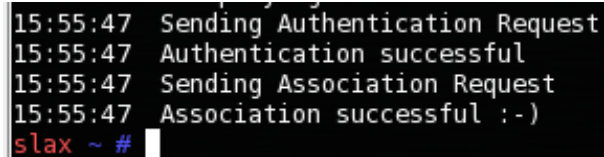
Aireplay-ng can also be utilized to determine if MAC filtering is being utilized on the target access point. If your card supports packet injection, you can attempt a forced association. However, if MAC filtering is active, you will be denied the association. For this procedure, you will need BackTrack or similar UNIX/Linux system. Within BackTrack, open a terminal window. From the command prompt, type:

```
aireplay-ng -fakeauth 0 -e {target ESSID} -a {MAC address of AP} -h {MAC address of your forensic laptop's wireless card}
```

An example command would look like:

```
aireplay-ng -fakeauth 0 -e belkin54g -a 00:11:50:53:9A:24 -h 00:20:A6:52:23:30
```

Once the command is executed, you will see a message telling you if authentication and association were successful.



```
15:55:47 Sending Authentication Request
15:55:47 Authentication successful
15:55:47 Sending Association Request
15:55:47 Association successful :- )
slax ~ #
```

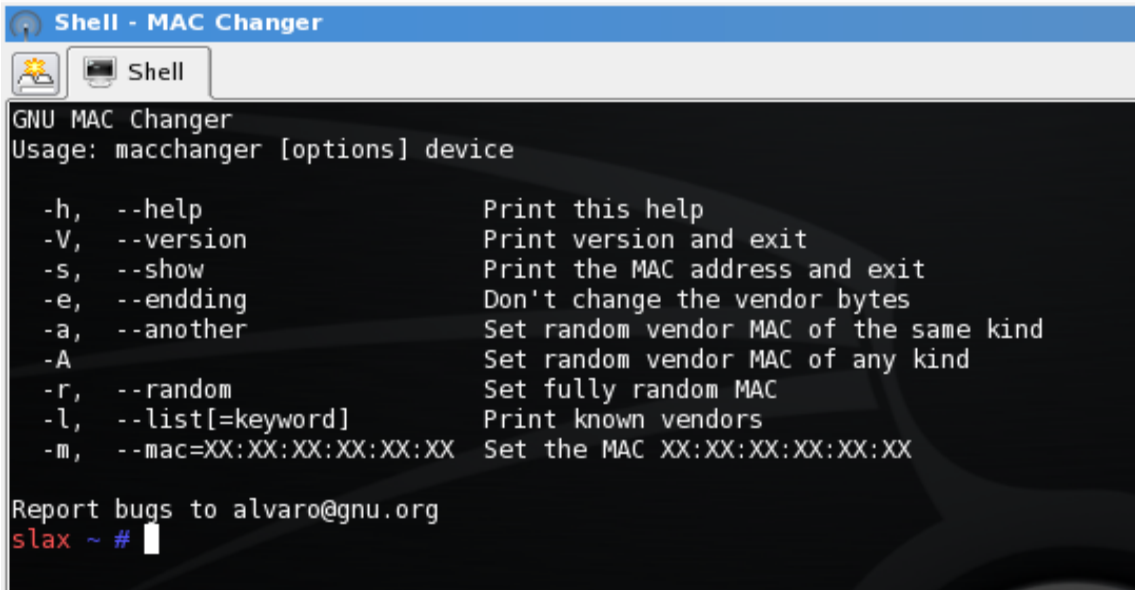
If the attempt was not successful, do not assume that MAC filtering is in place. If, while using airodump-ng, you see an associated MAC address, you may attempt to re-associate by spoofing your MAC address. Within the BackTrack program, select “BackTrack”, “Wireless Tools”, “Miscellaneous”, “MAC Changer”. Before changing the MAC, your wireless network card cannot be active. Close airodump-ng or any other program that utilizes the network card before continuing. You may need to force the card to shutdown by typing:

```
ifconfig {interface} down
```

The method is simple – type in the following command:

```
macchanger -m {MAC of currently associated device} {interface}
```

Below shows a list of available options for “macchanger”

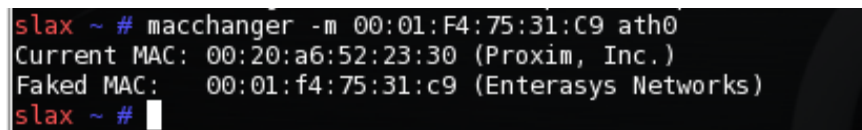


```
Shell - MAC Changer
GNU MAC Changer
Usage: macchanger [options] device

-h, --help          Print this help
-V, --version       Print version and exit
-s, --show          Print the MAC address and exit
-e, --ending        Don't change the vendor bytes
-a, --another       Set random vendor MAC of the same kind
-A                 Set random vendor MAC of any kind
-r, --random        Set fully random MAC
-l, --list[=keyword] Print known vendors
-m, --mac=XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX

Report bugs to alvaro@gnu.org
slax ~ #
```

Once complete, you will have set your wireless card with a newly spoofed MAC address. The display should show your previous and new MAC address and vendor settings.



```
slax ~ # macchanger -m 00:01:F4:75:31:C9 ath0
Current MAC: 00:20:a6:52:23:30 (Proxim, Inc.)
Faked MAC: 00:01:f4:75:31:c9 (Enterasys Networks)
slax ~ #
```

Make sure that you re-activate your network card by typing:

```
ifconfig {interface} up
```

Now you can attempt an authentication and association to the access point using our spoofed MAC. If you see the “success” message, MAC filtering is indeed active on the access point. If MAC filtering is turned off and encryption is turned on, you will not be successful using this method of authentication.

Wireless devices have become a major issue for computer-related investigations. Because wireless devices have become cheaper and faster, investigators will undoubtedly contact them during search warrants. Investigators may also incorporate a wireless network “sweep” before a search warrant is executed. Discovering an open, non-encrypted access point within your target location will change the dynamic of the search warrant. Discovering an access point with many active wireless clients will also change the dynamics of conducting your search. Hopefully this method will assist you to locate associated wireless devices.

Appendix A: Recommended PCMCIA network cards for use with the “aircrack-ng” suite

Make	Model	Interface	Chipset
Netgear	WG111	USB	PrismGT
Netgear	WG511T	PCMCIA	Atheros
Netgear	WAG511	PCMCIA	Atheros
Proxim	8470-WD	PCMCIA	Atheros
Ubiquiti	SRC	PCMCIA	Atheros