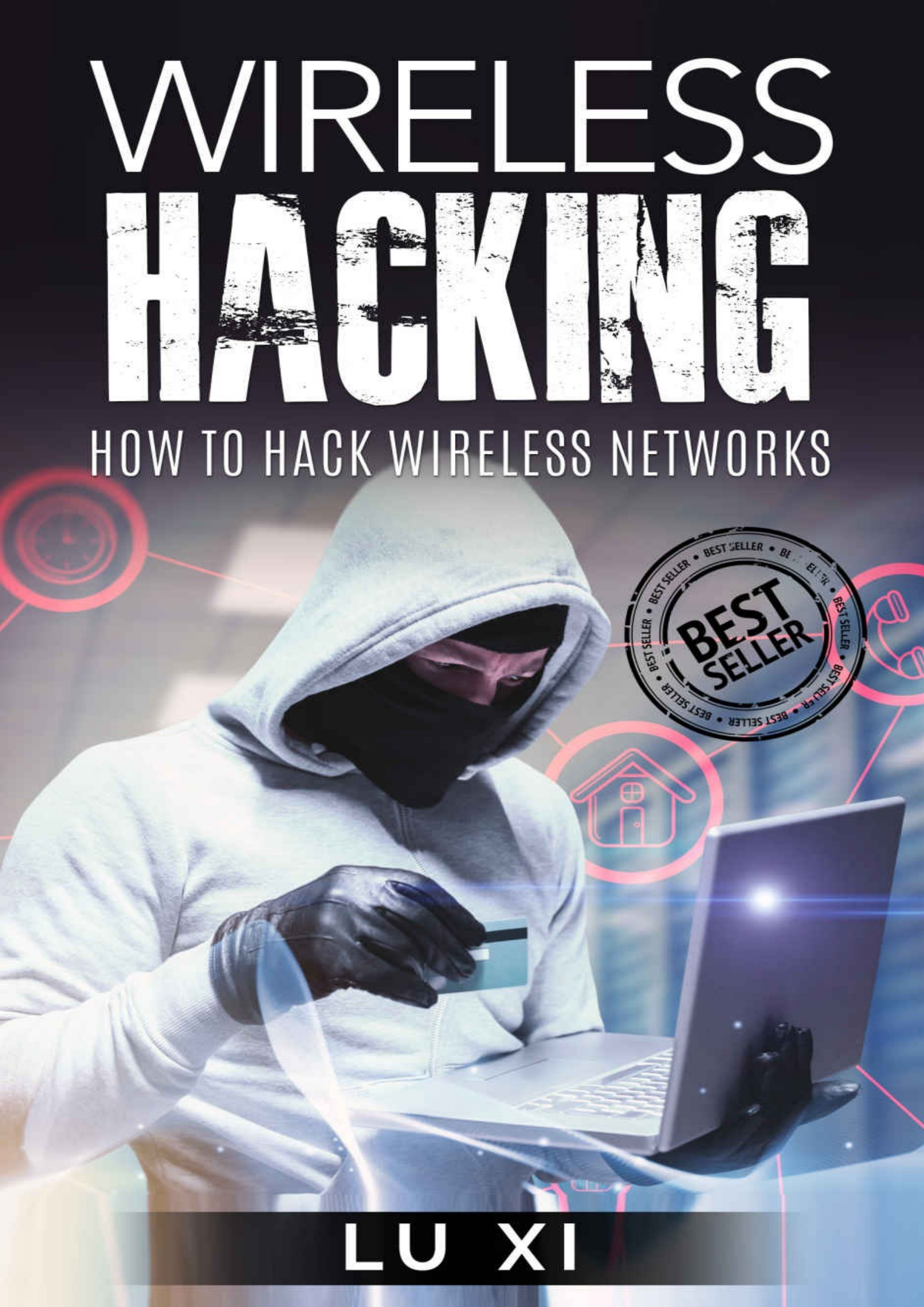
WIRELESS HACKING

HOW TO HACK WIRELESS NETWORKS



LU XI

WIRELESS HACKING

HOW TO HACK WIRELESS NETWORKS

LU XI

Lu Xi

PUBLISHED BY: Lu Xi

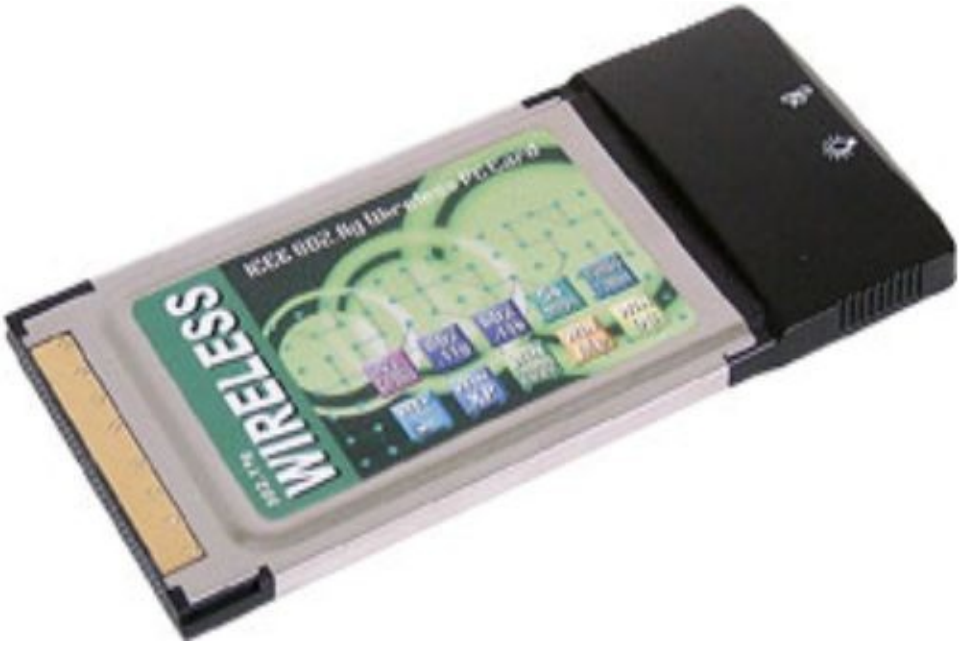
Introduction

I want to thank you and congratulate you for downloading this book!

Everything you need to know about wireless hacking is in this book.

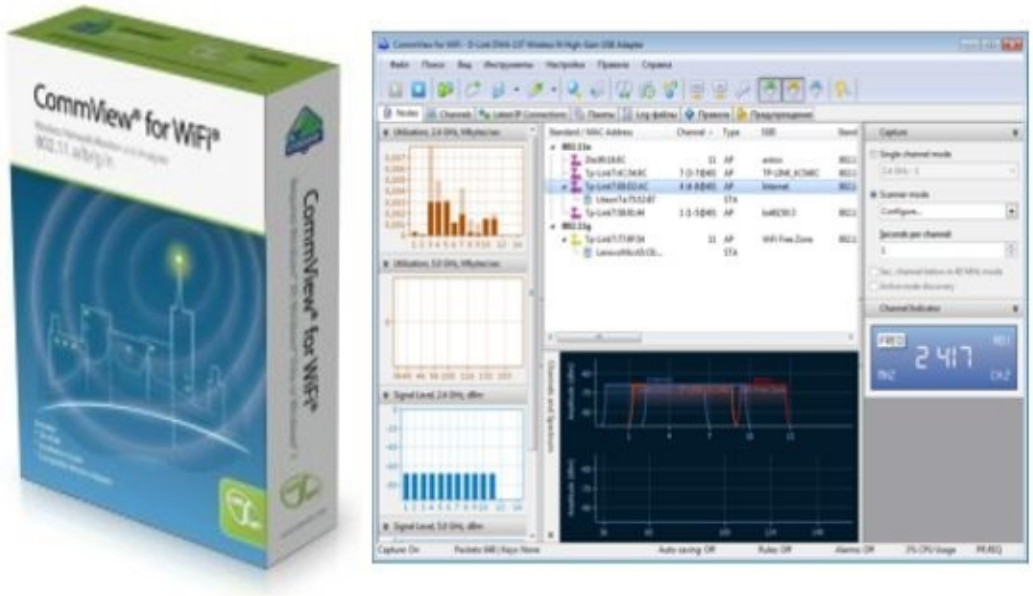
Lu Xi

Step #1: The Essential Requirement



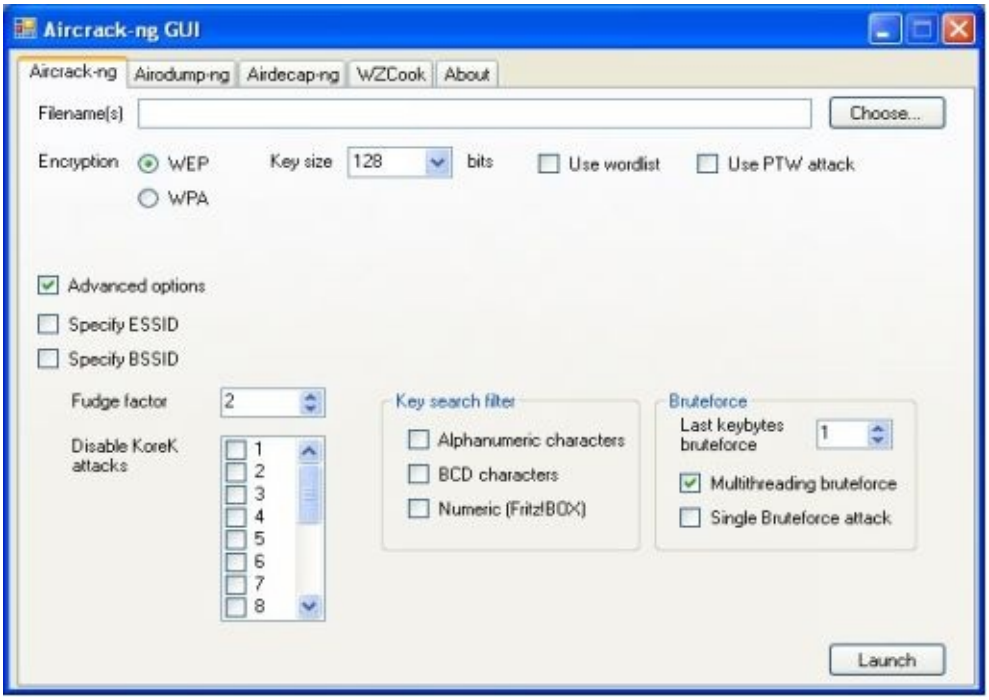
You will need to make sure that the wireless card of the computer that you will be using is compatible with the CommView software. This is necessary as its compatibility will ensure that it can monitor the network and capture the packets that travel to and from it. You can verify its compatibility by checking the list on the CommView website. If your current wireless card is not included in the list of compatible wireless cards, then you will need to purchase a compatible external wireless card adapter that you can connect to your computer, instead.

Step #2: CommView Installation



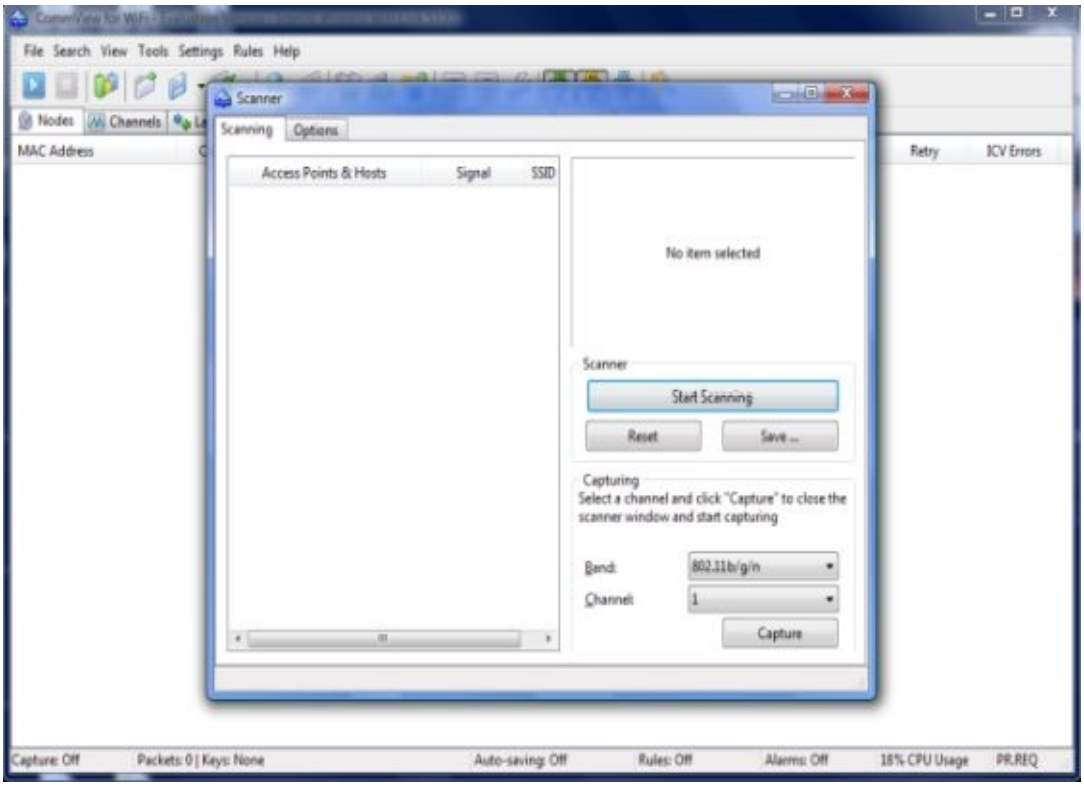
The CommView For Wifi software will be the main tool that will try to capture the packets and provide you with the information that you need with regards to the wireless network password that you are trying to crack. You should download and install the software from their website. You can just follow the onscreen instructions. It has a driver installation guide, as well, which will tell you to install the necessary drivers that you will need for this process.

Step #3: Aircrack-ng GUI



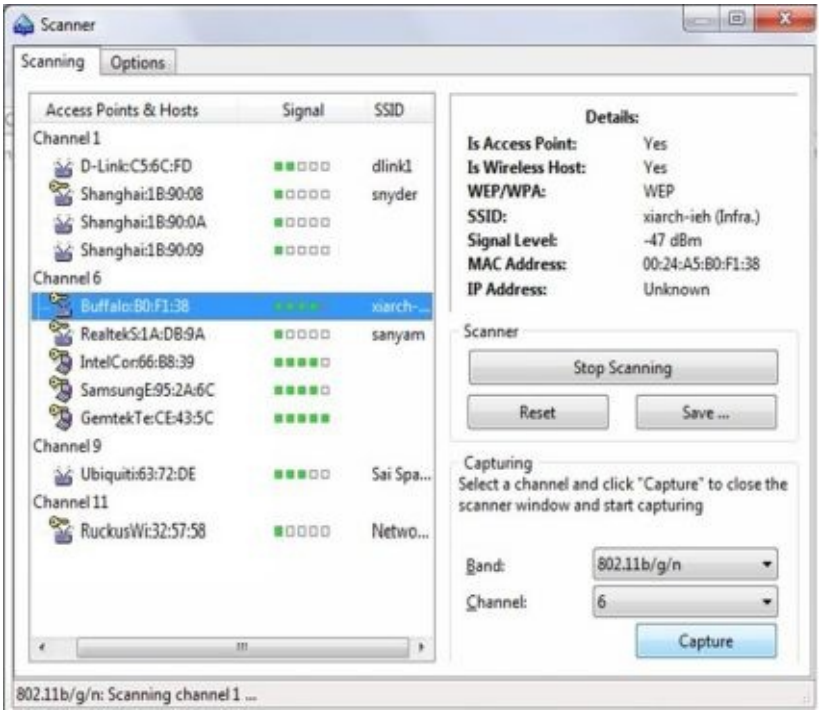
You will also need the Aircrack-ng GUI software. This is the software that does the actual cracking of the packets that were captured by the CommView software. You just have to go to their website so that you can download and install this particular software. Follow the onscreen instructions religiously to be able to successfully install the software.

Step #4: Running CommView



After successfully downloading and installing the CommView software, you have to run the program. Once you have opened the program, click on the Play button located at the top left of the page. This is the one with the blue arrow icon and the first button that you will see. This way, you will be able to see the “Scanner” dialog box.

Step #5: Scanning Networks



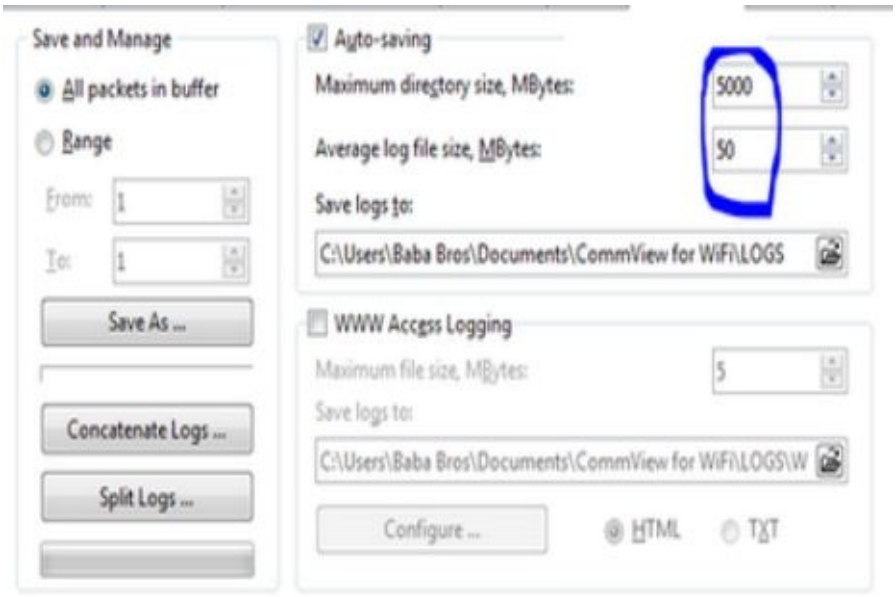
On the Scanner dialog box, click on the “Start Scanning” button. Doing so will instruct the software to start scanning the area for different wireless networks that it can find. You just have to wait for a few moments while it does the scanning process. At the end, you will

find a lot of wireless networks along with several details, such as the security type as well as signal, appearing on the screen.

Step #6: Targeting A Wireless Network

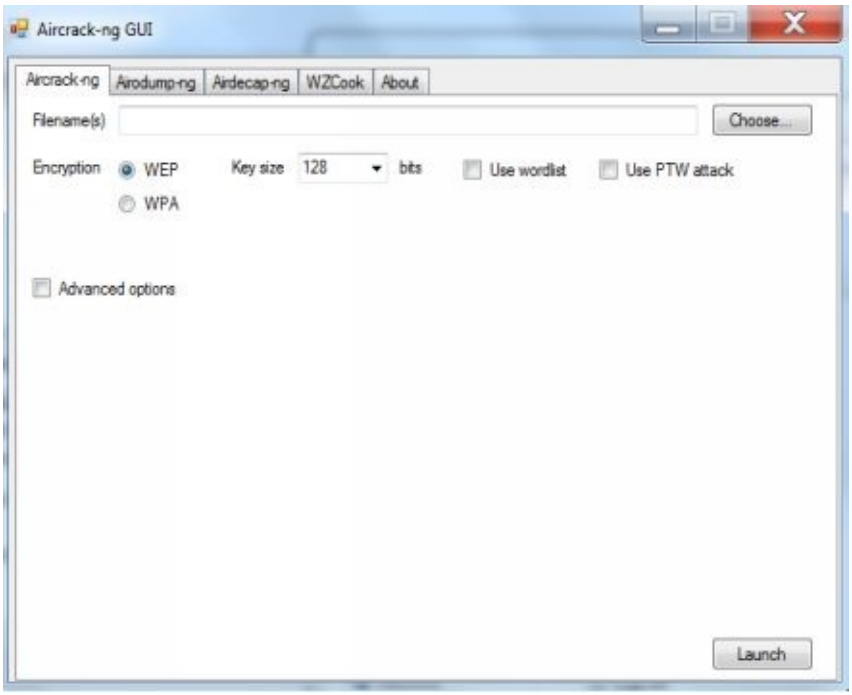
The next thing to do is to choose a wireless network that you will target and hack. Also, choose a network that is WEP-protected, meaning it only has WEP right beside the network name and not WPA. You should choose a network with the highest signal yet lowest decibel or dB. Once you have identified the perfect target, you should click on the “Capture” button. During this process, you need to make sure that the Packets column will reach 100,000 before you can proceed to the next step.

Step #7: The Logs



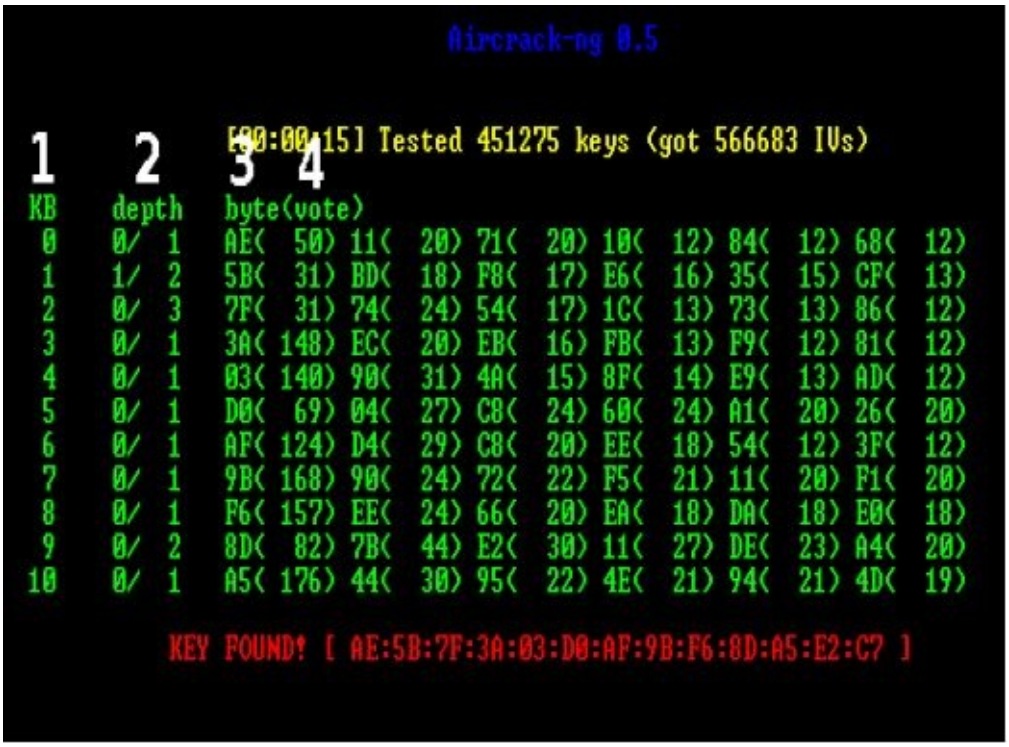
After capturing the required amount of packets, go the Logging tab and select all the saved logs. Open the log file and export the file to any destination that you want. It is advisable to choose a destination path that you can easily access. Make sure that the format is in tcpdump. The file should have a .cap extension when you look for it in the destination folder. Do not close the CommView software at any point in time during this process.

Step #8: Cracking with Aircrack-ng GUI



After getting all the logs, you should then run the Aircrack-ng GUI software. This way, you can start cracking the password for the wireless network. You have to choose WEP and open the file that has a .cap extension. This is the file that you should have saved in the previous step. Then, click on Launch and type the index number or your target wireless network on the command prompt.

Step #9: Hercules



Lastly, you should wait for a few while. If the software has successfully cracked the password, it will show you the wireless network key on the screen. The wireless network key will then be the one that you need to use in order to access your target wireless network. A different step will be necessary, though, if you will need to crack a WPA password.

Conclusion

Thank you again for downloading this book! I hope you learned a lot!

Finally, if you enjoyed this book, then I'd like to ask you for a favor, would you be kind enough to leave a review for this book on Amazon? It'd be greatly appreciated!

Thank you and good luck