How To Sniff Network Traffic

Neighborhood Network Watch Home Network Awareness Program

Introduction

The communities across our beloved nation have never been at a greater risk than they are today. However, the greatest threat that we have to combat within the community is primarily invisible and typically intangible. This threat is terrorism. Since terrorists operate in cells that embed themselves within the community they often go completely unnoticed, not unlike the terrorists who carried out the September 11th attacks.

Identifying terrorists is no easy task since they become a part of the community and rely on its resources, especially for communication. Cities, towns, and suburbs all across our nation often have computer networks. These networks are located within places of business, commerce, as well as our homes. With the widespread adoption and usage of wireless networks, it has created a climate that is ripe for exploitation by terrorists. Since these networks often times are unsecured or offered as a free service to the public it allows any individual to use them, including terrorists. Even the networks that reside in our homes can be used by terrorists who maybe our own neighbors or fellow building residents.

Therefore it is imperative that these networks do not go unmonitored. That is why the Neighborhood Network Watch was established and why now the Home Network Awareness Program has been created to allows individuals like yourself to make sure that terrorists may not be using your own home network to plan the next attack on our nation or your very own community.

This document has been created so individuals like yourself and your community can become more involved with and to help the Neighborhood Network Watch carry out its mission, by learning how to packet sniff your own home network. That mission being to keep our community's networks safe from terrorists and those who may attempt to harm our community and our nation. The skills you will learn during the course of reading this document will provide you a working knowledge of the same tools that the Neighborhood Network Watch's Network Identification and Collection Divisions (NICD) use.

Operating System & Requirements

You should use a computer that has a wireless networking card. You can use a card that is either 802.11b, 802.11g or 802.11n compatible.

This can be done with a non-wireless networking card however the ability to monitor other networks in the vicinity will not be possible. You may use a desktop or a laptop, however laptops are typically preferred to their mobility.

You will also need at least 200 MBs (megabytes) of free space on your hard disk for the collection files that are generated.

Which Operating System (OS) Do You Have On Your Computer?

- Linux / Unix
- Mac Os X
- Windows 95/98/NT/2000/XP/2003/Vista


Linux / Unix / Mac Os X Requirements & Software

If you are using Linux, Mac Os X, or Unix you will not need to install anything, the application you will need to capture network data is already installed. You will need to be the administrator or have administration access on your machine.

Windows Requirements & Software

If you are using Windows you will need to install two items (refer to Appendix 1 for more info):

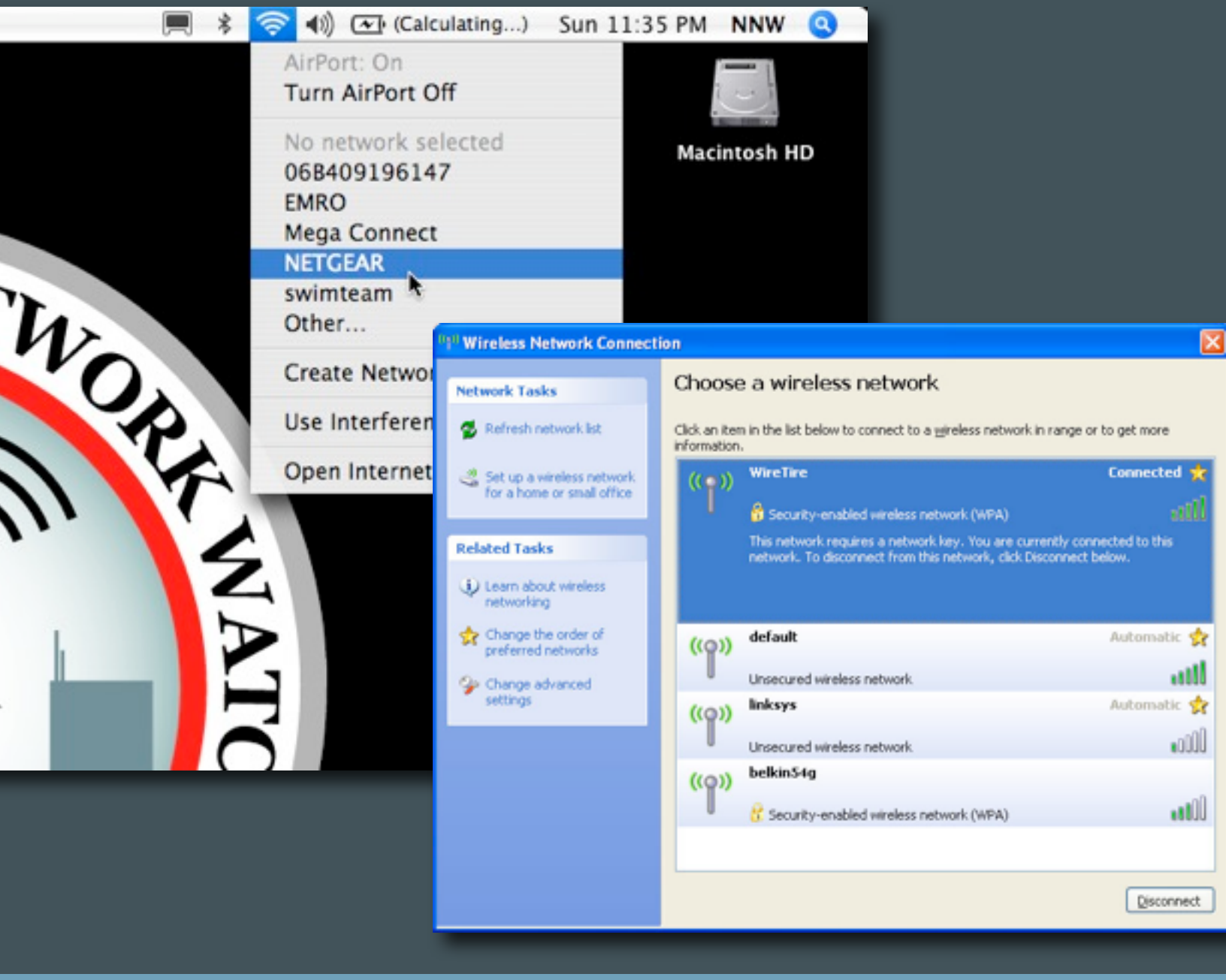
- WinCap
- WinDump

Both these items can be downloaded for free from www.wincap.org/windump/install.
You will also need administration level access on the machine you are going to be using, so make sure you have an admin account on the machine or are the admin.

Finding a Network

We recommend to start with your own home network and then eventually move onto those of your neighbors. Eventually you could begin looking at networks that are local to your community, such as cafés, local eateries, libraries, and parks.

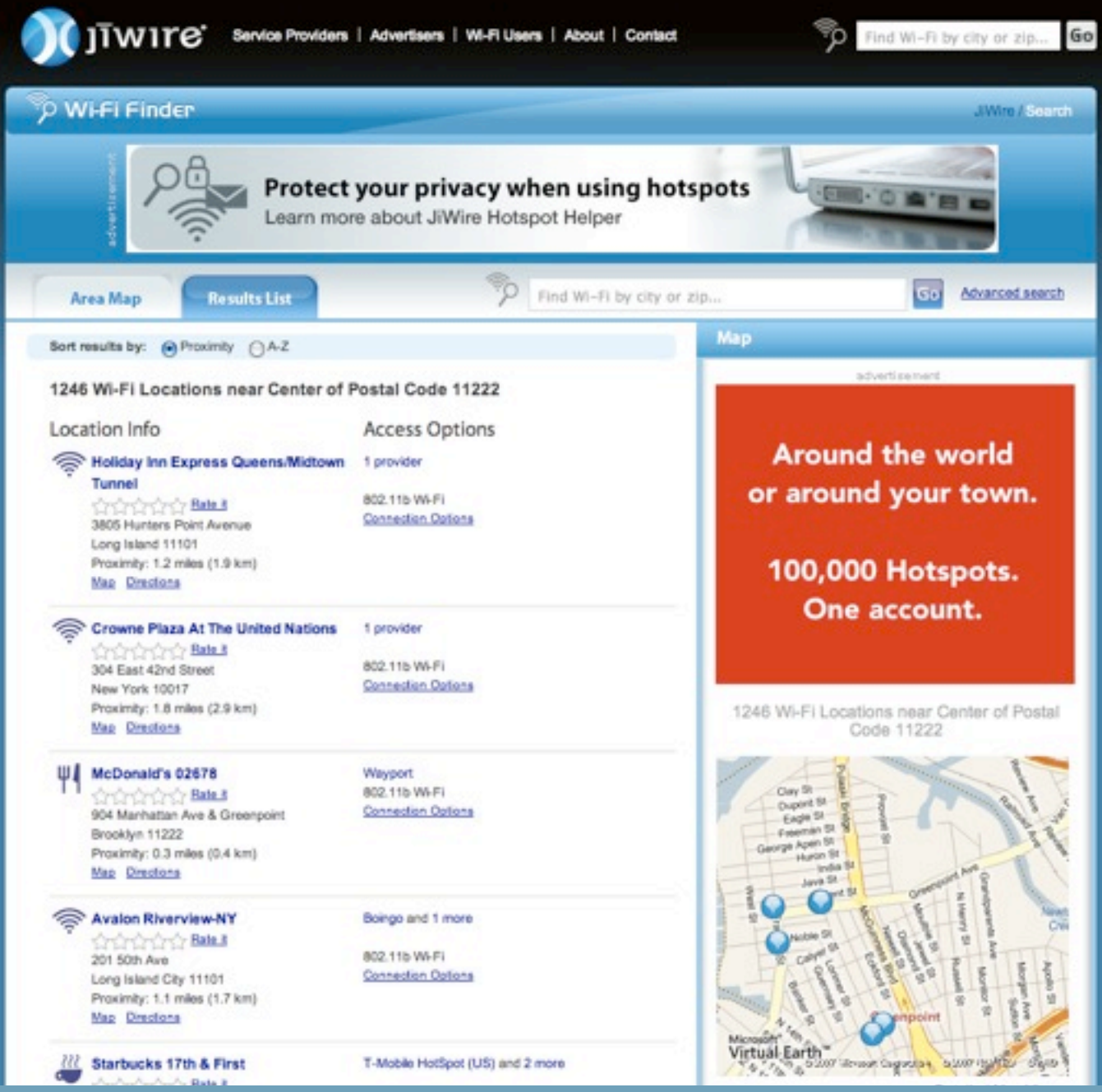
There are many ways you can find a network to monitor if you do not have one of your own or if your ready to move onto monitoring networks other than your own. On the next four pages are four ways and places to find wireless networks that maybe suitable.



Scanning Your Area

The easiest way to find a network is to simply see if there are any networks right where you are, by taking a look at the networks which are available to your wireless networking card. This could of course include the networks of your neighbors.

Of course you could also use a dedicated software package to look for these networks as well. These applications are typically referred to as WiFi Stumblers (Refer to Appendix 1).



WiFi Network Directories

You can also look up the locations of wireless networks within your area by looking for them in directories that list the locations of wireless networks. These directories are often searchable by zip code or city. Some of these directories include: Jiwire, WiFi 411, and WiFi Free Spot.

Retail and Eateries

Another option that is becoming more and more a part of the community are networks based in retail locations. These maybe the local retailer down the block or a local eatery that offers wireless internet access to their patrons. Some examples of these are local independent coffee shops, Starbucks, and Apple Stores.

City of New York
Parks & Recreation

Your City's Public Networks

City run public networks, in large to medium size cities, are another common location to find wireless networks. These maybe located in libraries and parks. For example the NYC Dept. of Parks and Recreation's free WiFi networks that are open to park goers. Check with your local public library system or park and recreation commission.

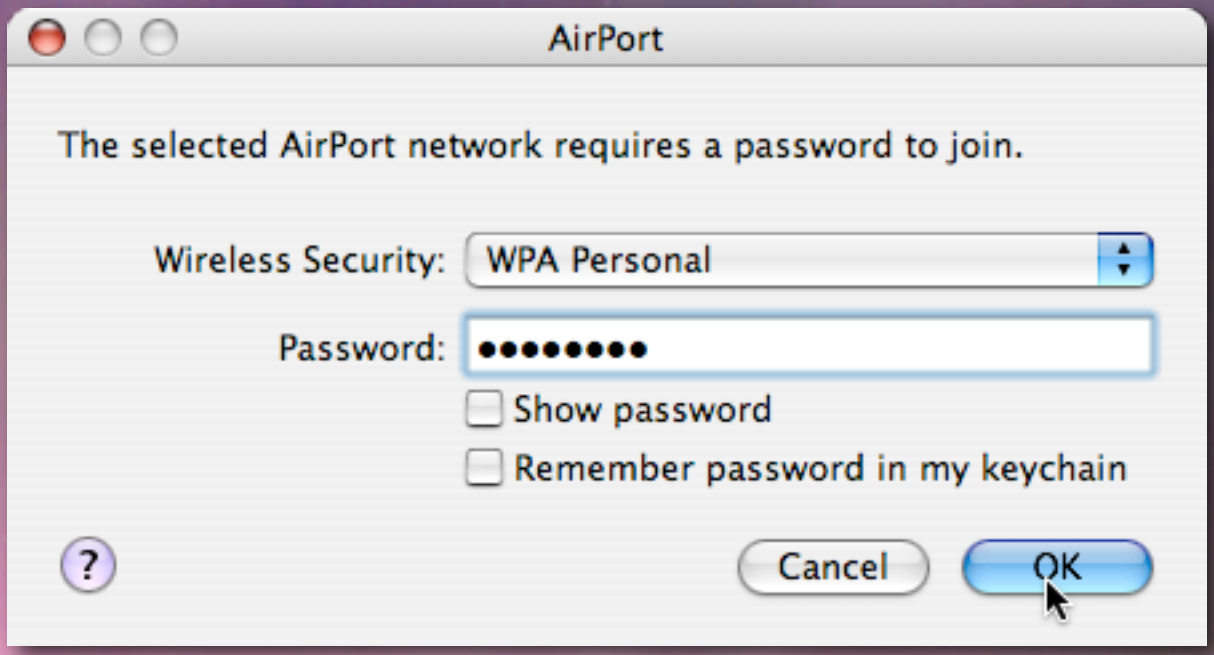
Encryption?

Networks that are encrypted will more than likely not allow you to connect to them without a password and therefore it is a smart choice to do a little bit of research before trying to profile a network. There are three main ways to obtain information about whether or not the network is encrypted and possibly the password.

(1) Check a WiFi network directory, they will often list whether a network is encrypted

(2) If it is a business it may be useful to check their website. Often times they will disclose whether or not their network uses encryption and if so it may list the password or how to obtain a password to connect.

(3) Finding out at the source, is an option as well. You have to physically go down there and scan the area the networks which will tell you if the network has encryption. You can do this with your laptop or a portable WiFi enabled device such as cell phone, portable gaming console, or MP3 player. If the network has encryption do not despair you may be able to ask a store employee for the password.



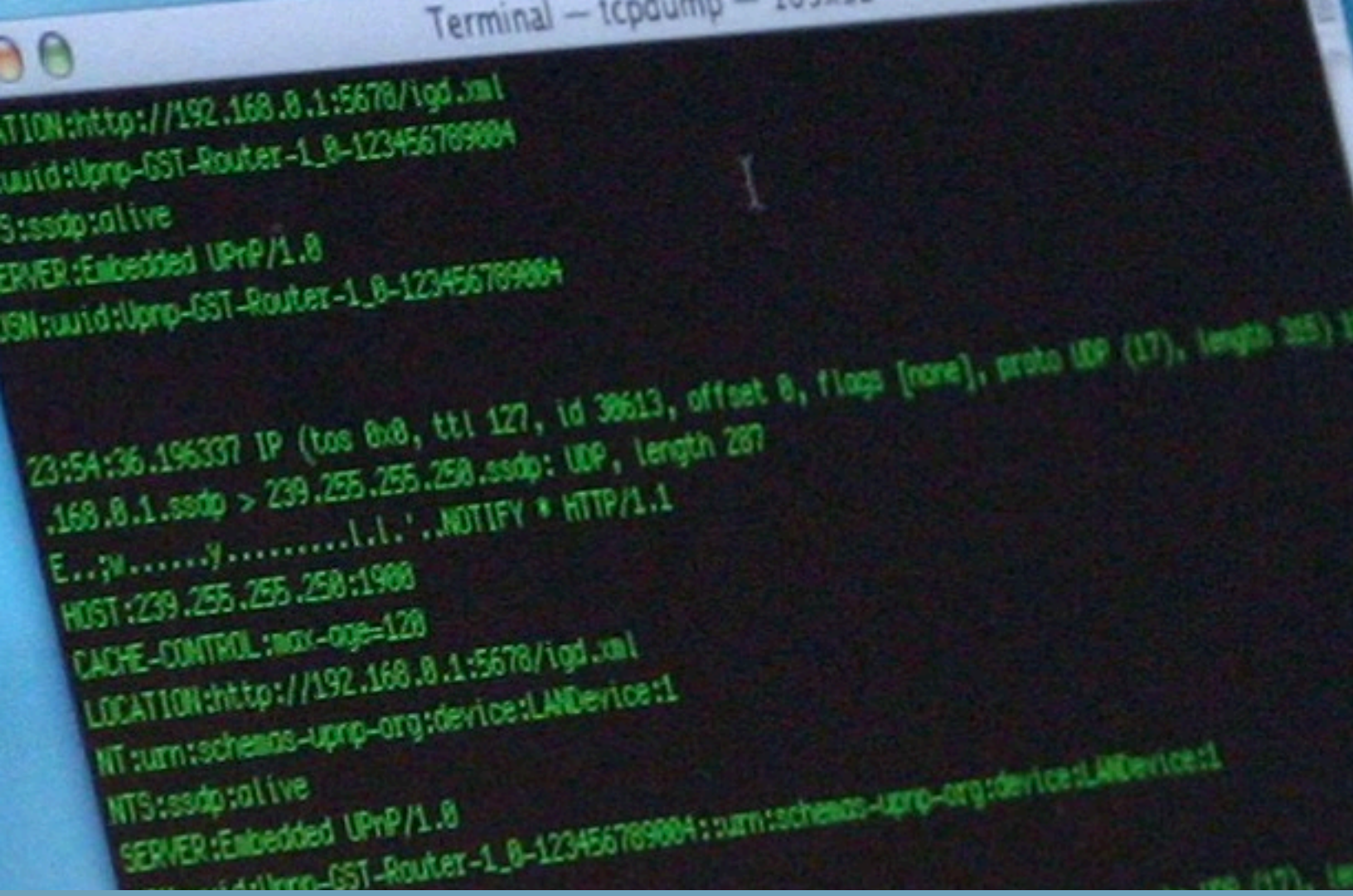
Logging On

After determining whether or not the network is using encryption or requires a password you are now ready to log on. So, go ahead and log on and get ready to start collecting network traffic.

You should be familiar with logging onto a wireless network and if not you should become comfortable with doing this prior to carrying out operations for the Home Network Awareness Program. You can easily become acquainted with the method used for logging onto a network by consulting your wireless networking cards manual or your operating system manual or technical support.

Remember to keep a log or journal of all the networks you collect from. This log should include the following:

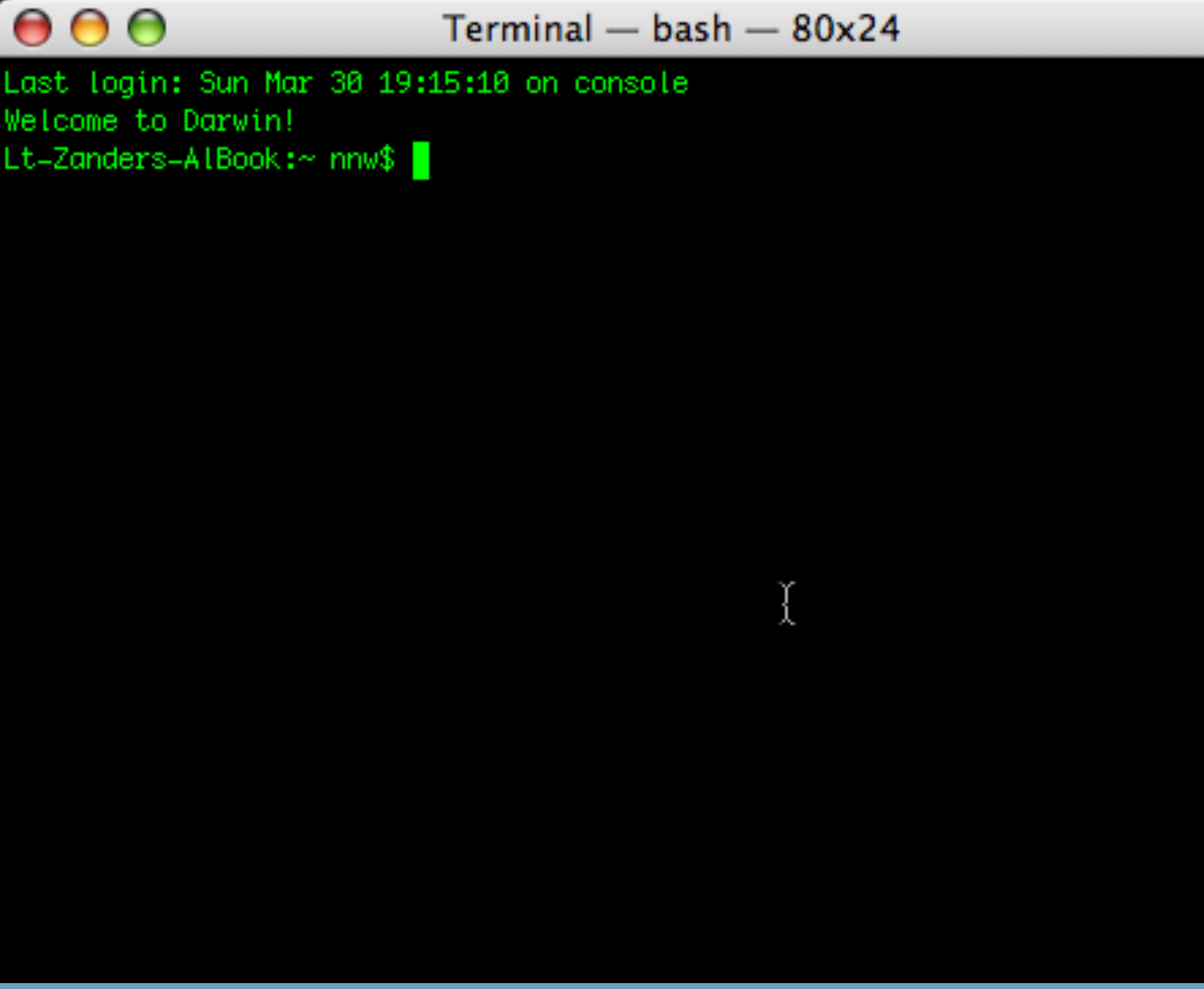
- Name of the network, also known as the SSID
- Location of the network, preferably with the address if it is known or accessible
- Time that the collection took place, which should include the start and end times
- Names of the files that were generated during the course of capturing traffic from the given network



Collecting Network Traffic Or “Sniffing”

The method you will employee for capturing data from a network is commonly known as “packet sniffing.” Every email, instant message, or website your browse is broken up into small packages that contain the data that is being sent and received, these are called packets. A “packet sniffer” allows your networking card to listen to all the packets that are being transmitted across a given network from any computers using this network, along with allowing you to see their contents and store them. Employing a packet sniffer to capture samples of network traffic from a wireless network, is not only effective it is also very easy since it does not require a physical connection to the network since after all it is wireless.

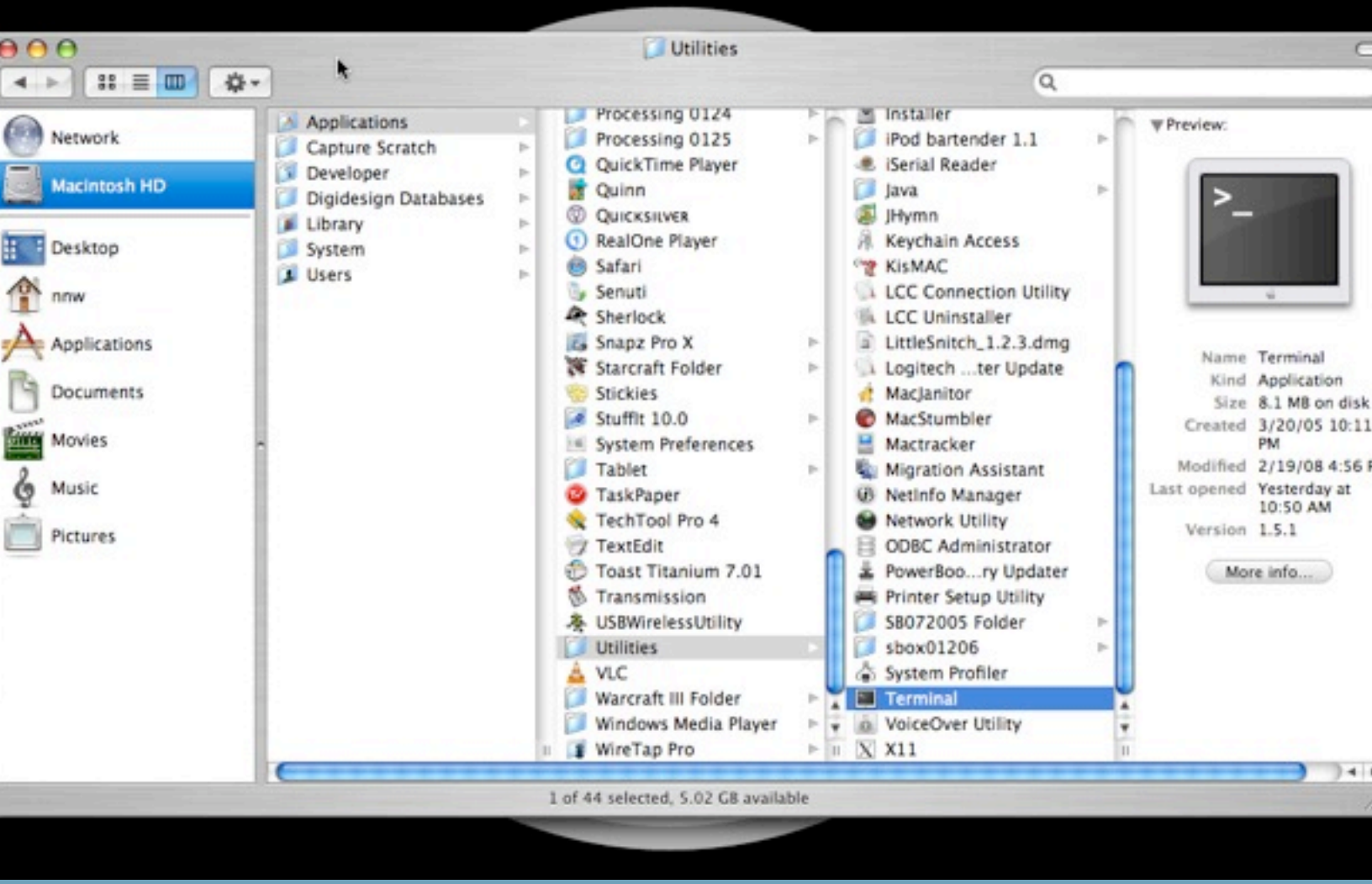
The software that is typically used to do this is network diagnostic software or a dedicated “packet sniffing” application. The Neighborhood Network Watch uses a free Open Source application called TCPDUMP (WinDump for Windows).



TCPDUMP

TCPDUMP is a command line based application, which mains it has no graphical interface and require you to operate it by using text commands. This may seem intimidating at first but it is really quite simple. Before getting started with teaching you how to operate TCPDUMP you must make sure that you have administration access on your computer or be the administrator of the computer you are using since TCPDUMP requires this.

The following two pages will discuss how to operate TCPDUMP. So, let's get started.



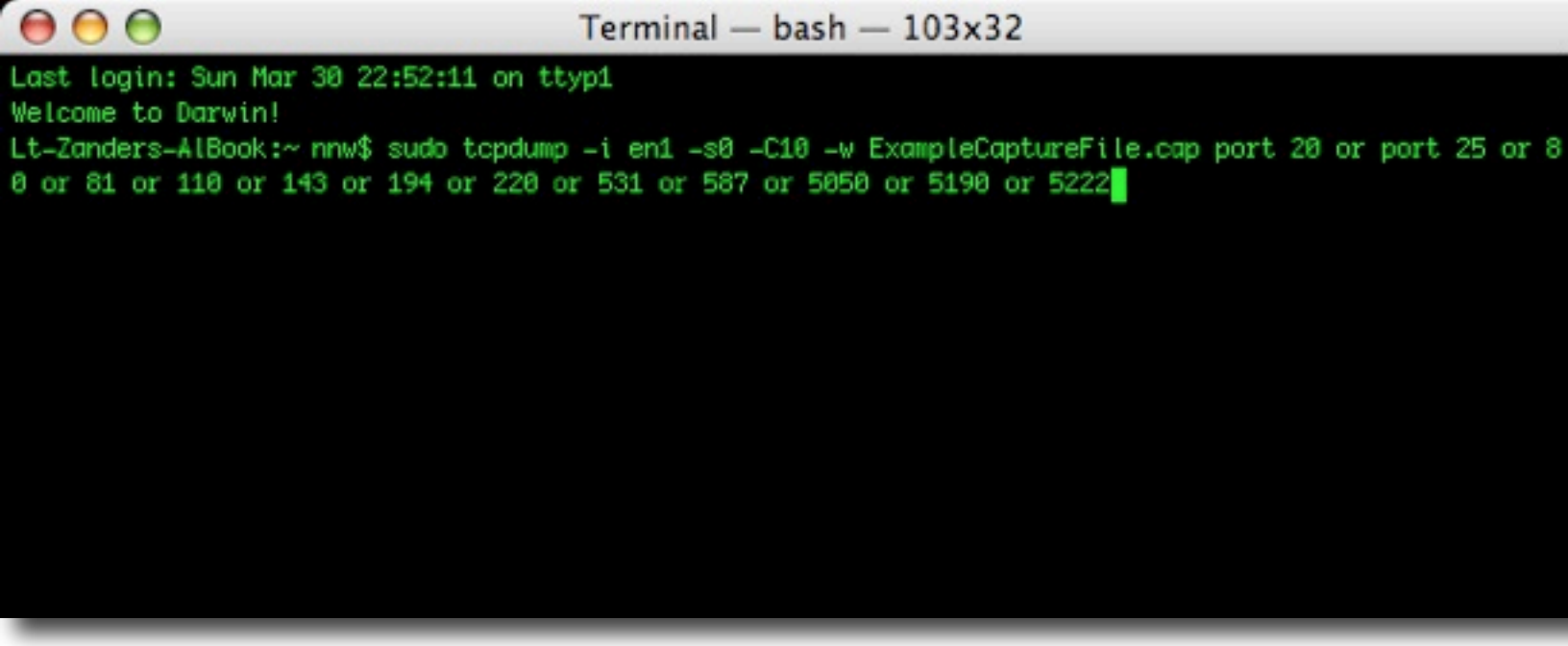
Where To Find The Command Line

Since, TCPDUMP is a command line application it will be run from the command line. Most operating systems allow you to access the command line through an application that will run at the same time as the normal graphical user interface you are used to.

If you are using the Windows operating system the application will be called “Console” and will be available in the “Applications” part of the “Start” menu.

If you are using the Mac OS X operating system it will be called “Terminal” and will be located in the folder called “Utilities” that resides in the “Applications” folder.

For Unix and Linux users you are likely well acquainted with the command line and if not you will be able to look up directions on how to access the command line by consulting the documentation for your operating system.



sudo tcpdump -i en1 -A -s0 -C10 -w ExampleCaptureFile.cap port 20 or 25 or 80 or 81 or 110 or 143 or 194 or 220 or 531 or 587 or 5050 or 5190 or 5222

Figure 1a

The Command

The command in figure 1 will be the full command that you will be typing into your command line to run TCPDUMP to capture all network traffic from the network to a file. TCPDUMP will collect network traffic that is coming from the following types of applications: email clients, instant message clients, instant relay chat clients (IRC), file transfer protocol clients (FTP), and web browsers.

In the following pages we will be breaking down the anatomy of this sequence of commands so you can have a better understanding of what is going on and how to operate TCPDUMP.

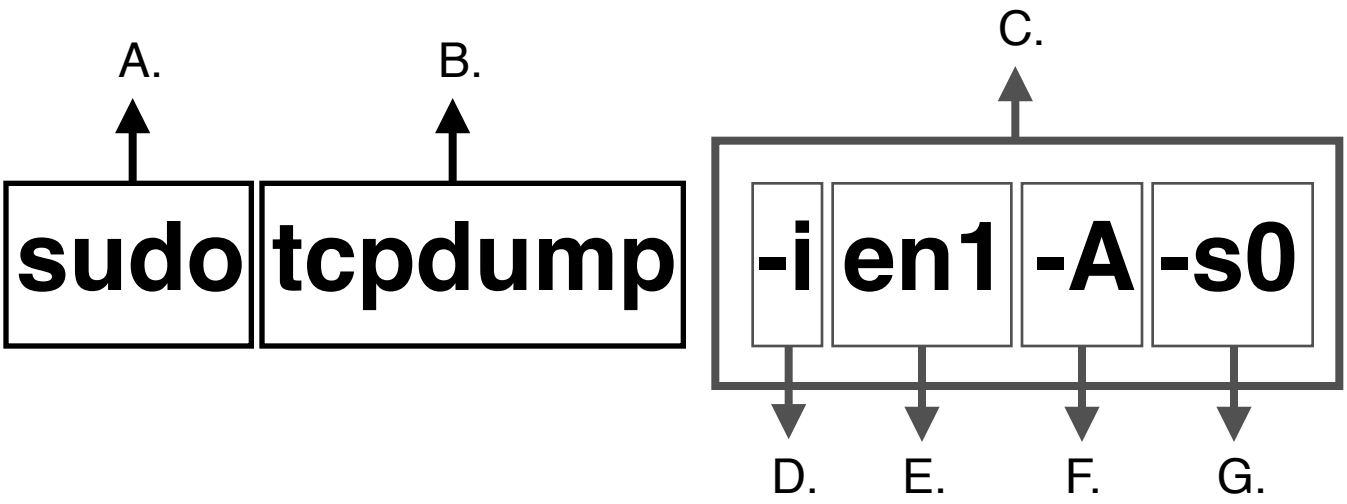


Figure 1b

TCPDUMP Breakdown Part 1 (figure 1b)

A. Sudo will allow give you the proper authority needed to run tcpdump. You will be prompted for your administration password when you run this command.

B. Tells the computer to run the application TCPDUMP.

C. This is the flag section. Flags basically are parameters that tell the program how operate.

D. “i” - This flag that tells TCPDUMP that I want to designate which networking interface I want to use.

E. “en1” - This flag goes hand in hand with the “-i” flag. This is where the network interface is chosen. Computers often have more than one networking card in them. Typically one that is wired (Ethernet) and another which is wireless (Wireless Ethernet).

These interfaces are given a corresponding number starting with “0” and progressing sequentially. Wired network cards are typically 0 and hence you would use the flag “en0” to run tcpdump on the wired ethernet interface.

Wireless cards are typically “1” therefore you would use the command “en1” when running tcpdump from the wireless networking card.

F. “-A” - This flag tells tcpdump to output the contents of the packets into ASCII, which is a fashion that allows it to be easily read.

G. “-s0” - This flag automatically adjust the amount of information to capture from each packet to its actual size, so nothing gets lost or truncated.

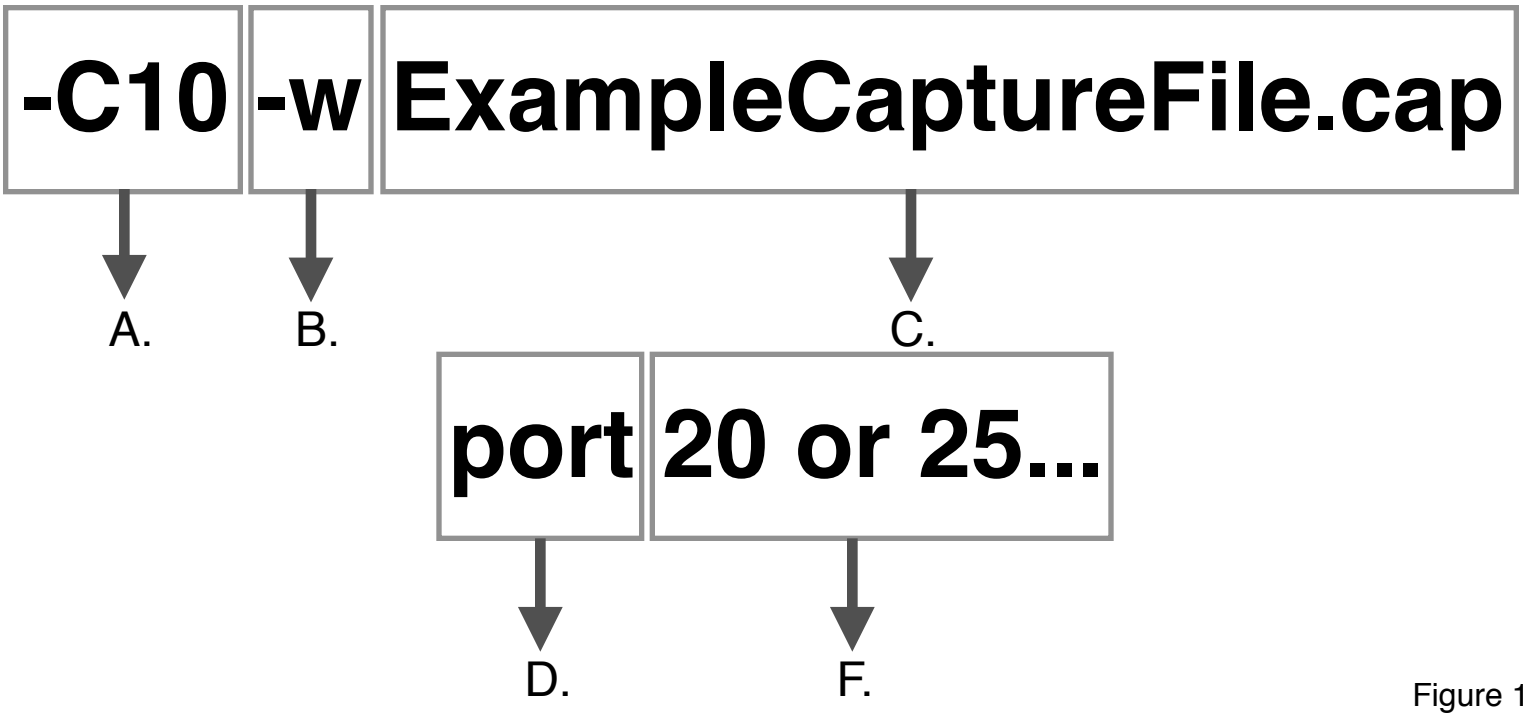


Figure 1c

TCPDUMP Breakdown Part 2 (figure 1c)

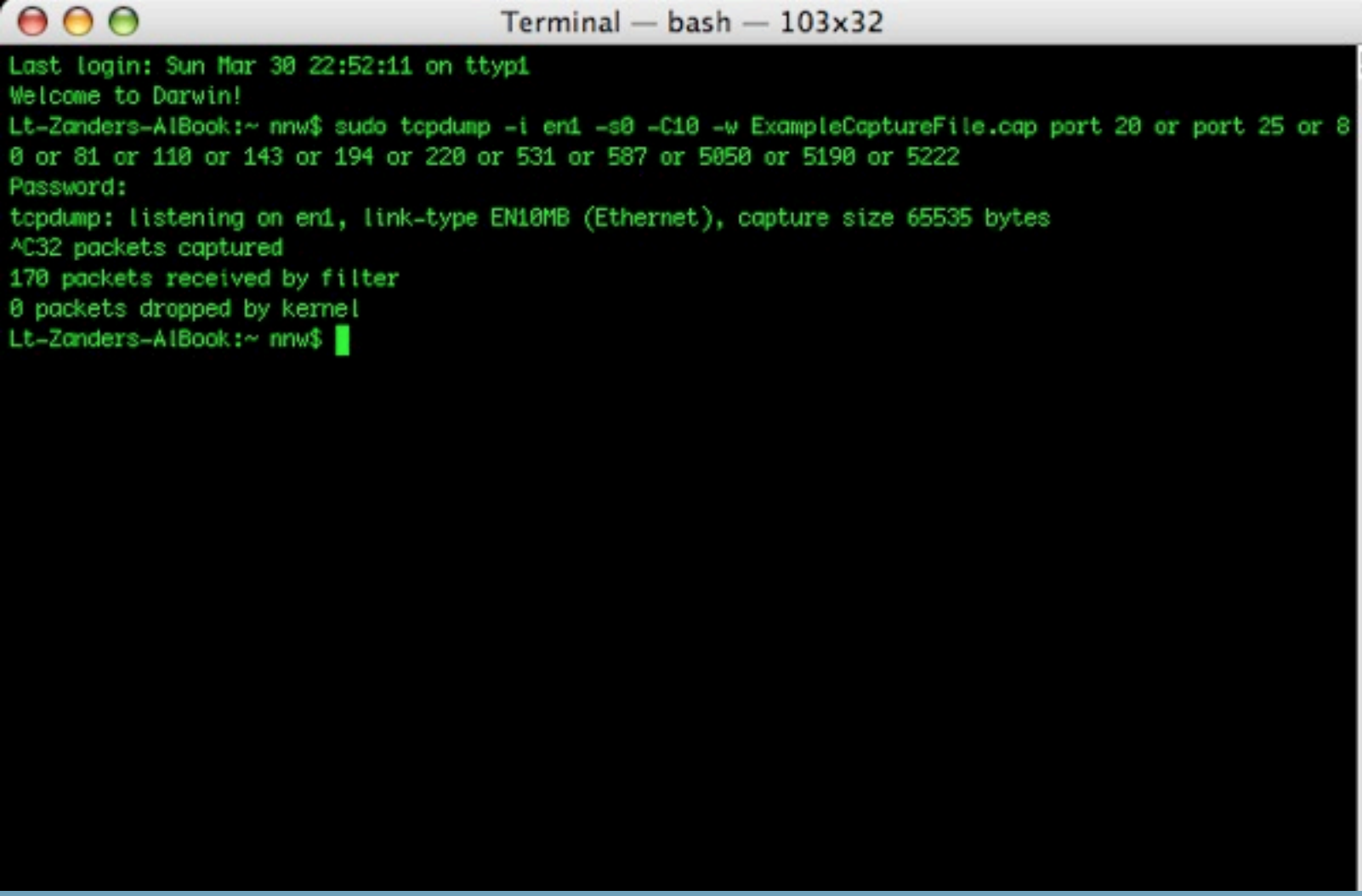
A. “C10” – This flag sets the max size, in megabytes (MB), of the capture files that will be written with the information coming from the network. This is currently set to make 10 megabyte (MB) files. The trailing number can be increased or decreased, however very large files become hard to process or take excessive time and resources. It’s recommended to keep these files under 10 megabytes or under, ie. “C10” or “C5”.

B. “–w” –This flag tells tcpdump to not display the traffic captured but rather write this information out to a file, in the users home directory.

C.“ExampleCaptureFile.cap” – This is the name for the file that will be written. Note it must include the “.cap” extension at the end of the name. This name can be whatever you want, however it’s a good idea to name this after the name of the network as it allows you to keep track of the files with ease. The date is also useful information as well. A better name could look something like this: “BensCafe-01-01-07.cap”.

D. “port” - This flag sets TCPDUMP to only capture traffic from the designated numbered port. If this flag is left out TCPDUMP will capture traffic from every port.

E. “20 or 25” - Are the numbered ports that TCPDUMP will capture traffic from. Most applications use a specific port to transfer data through. Each port number is separated by the word “or”. To see a full list of the ports used refer to Appendix 2.

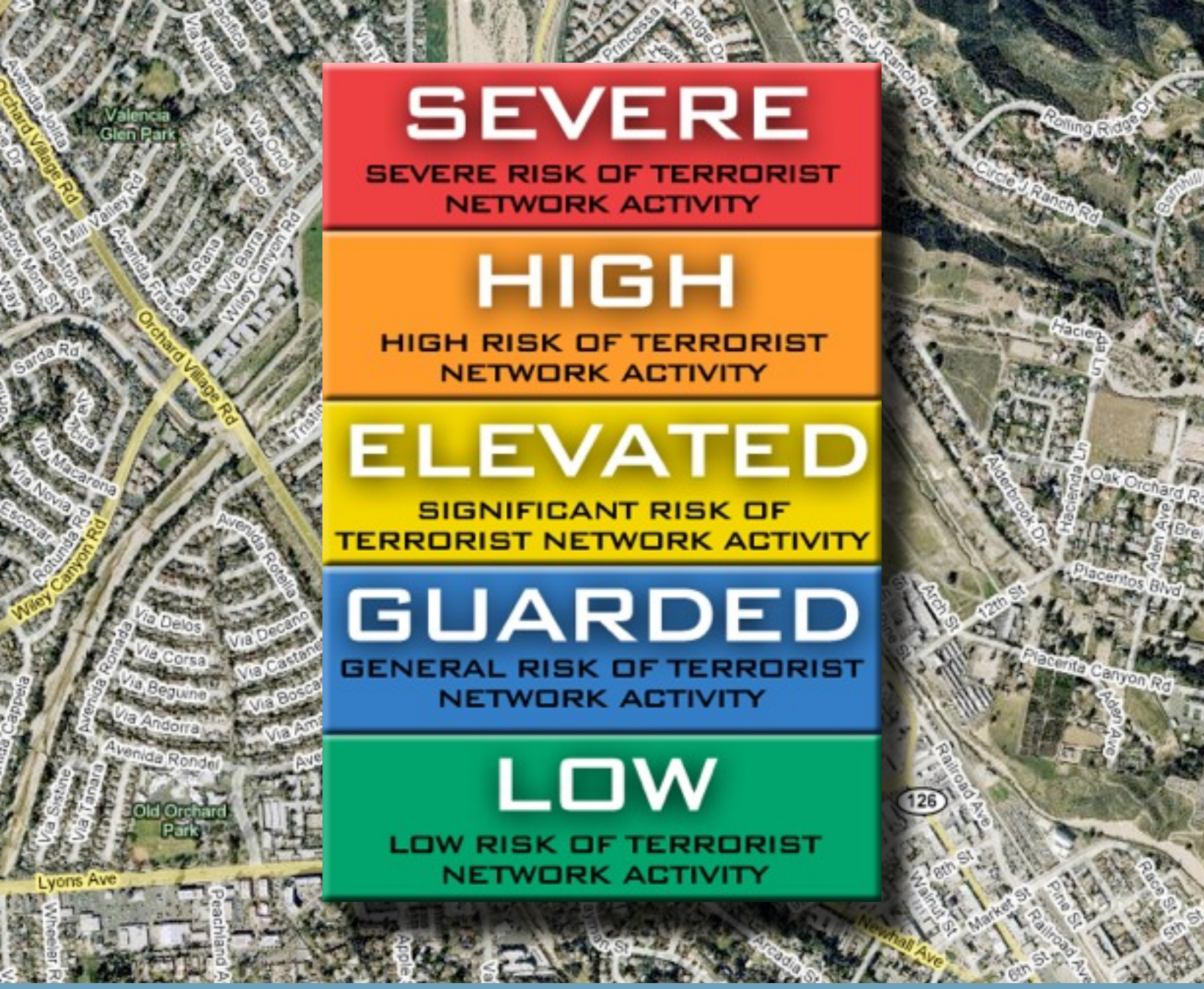


Running The Command

After typing in the full command hit the “return” or “enter” key and TCPDUMP will now begin capturing aka “sniffing” traffic with the parameters that were discussed in the previous pages. It will automatically make sequentially numbered files as they hit the file size threshold.

You should collect for a minimum of a half hour, preferably and hour or more if possible. After you are ready to end the capture session, press the “Control” and “C” keys to stop TCPDUMP. TCPDUMP will stop and will let you know how many packets you captured as well as how many were lost or dropped.

That’s it, you have now successfully “sniffed” a network. Congratulations. All that is left to do is to send your files to your local Neighborhood Network Chapter for analysis. If your city does not have a chapter established for your city or town please email your collection files to hnap@dhsnnw.org.



Results & Ratings

After the network capture files have been analyzed by one of the Neighborhood Network Watch's Data Analysis Divisions (DAD), results will be emailed back to you. The results will include a rating for each network as well as an overall rating for the vicinities you may have collected in.

Appendix 1: Additional Information On Software

This appendix contains a list of places where you can learn about the software that is used for network collections, by the Neighborhood Network Watch as well as the Home Network Awareness Program.

TCPDUMP

•Wikipedia: tcpdump

•Official TCPDUMP Website

•TCPDUMP Manual at OpenBSD.org

•WinDump Website

•WinDump Installation

•WinDump Manual

Packet Sniffing

•Wikipedia: Packet Sniffing

•How Stuff Works: Packet Sniffing

WiFi Stumblers

•Kismet / Kismac - All platforms (limited Windows hardware options)

•MacStumbler - Mac OS X

•Net Stumbler - Windows & Windows CE

Appendix 2: Ports

This appendix contains a list of all the ports that are to be sniffed by participants in the Neighborhood Network Watch's Home Network Awareness Program (HNAP). The list has the port number followed by the type of traffic that is typically sent through this port.

Port Usage Table

Port Number	Type of Traffic
20	FTP
25	Email
80	Web
81	Web
110	Email Receiving
143	Email
194	IRC
220	Email
531	Instant Message
587	Email
5050	Instant Message
5190	Instant Message
5222	Instant Message

Neighborhood Network Watch

Department of Homeland Security

PUBLISHED BY

NEIGHBORHOOD NETWORK WATCH
DEPARTMENT OF HOMELAND SECURITY
WASHINGTON, DC 20528

HTTP://WWW.DHSNNW.ORG | HTTP://WWW.DHS.GOV