Leon H. Lincoln, III

Leon Lincoln is currently a system administrator at the Broad Institute of MIT and Harvard.

A Macintosh User since its inception in 1984, he has used the platform in a variety of production environments including printing prepress, desktop publishing and IT support.

As a former Broad Service Desk team member, he has been involved in many facets of the Broad IT (BITS) Department over the years. Current responsibilities include being the Macintosh Architect, JAMF Casper Administrator, Remote Tracker Administrator, JAVA support, as well as being the senior escalation for the ServiceDesk Team.

BROAD INSTITUTE

MACTECH PRO EVENTS

The Professional

Apple Tech's Toolbox

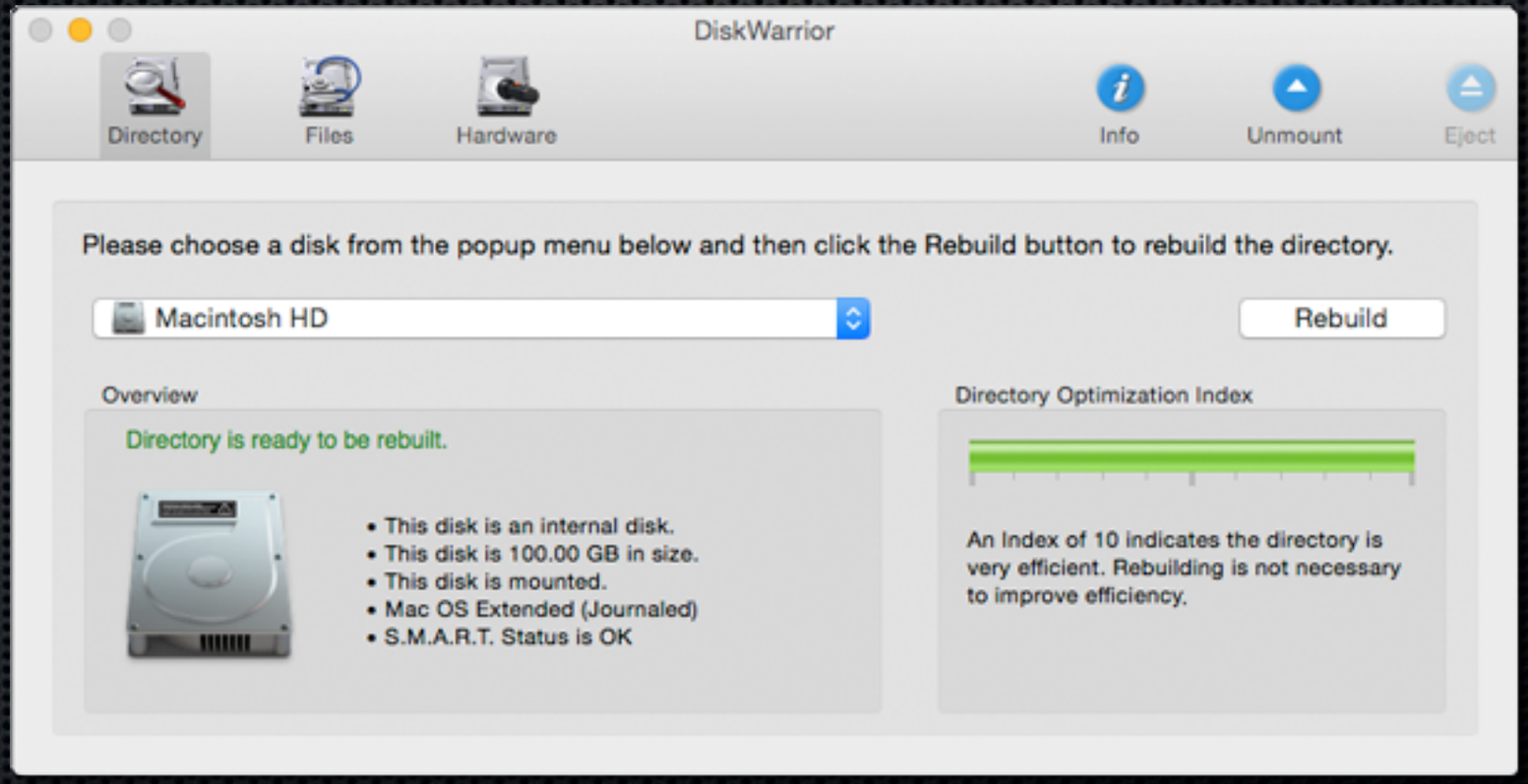
MACTECH PRO EVENTS

Disk Utilities and More

- DiskWarrior
- TechTool Pro
- SubRosaSoft
- Activity Monitor
- Disk Utility
- Terminal

DiskWarrior

With a single click, DiskWarrior reads the damaged directory and finds all salvageable files and folders and builds a new error-free, optimized directory for you to use.



TechTool Pro

- tests the major components on your motherboard: RAM, Processor, Cache along with electrical and temperature sensors

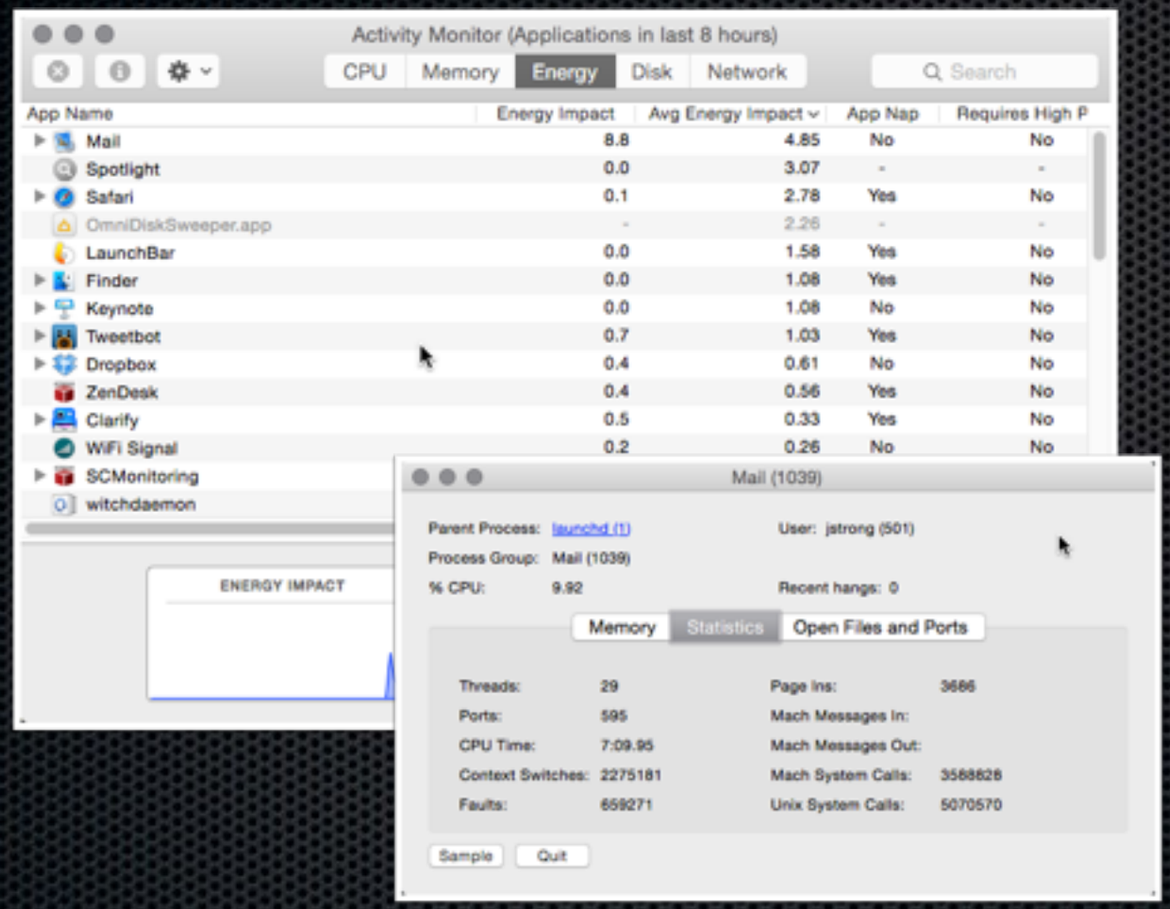
- Fans test spins up the fans in your Mac to make sure that they run at capacity and speed to ensure your Macintosh is running at its best

- test reports cycle count, percent of total capacity remaining, along with the battery's overall condition

SubRosaSoft

- FileSalvage is device and file system independent, which means that the user can recover files from a normal Mac OS hard drive, USB key, PC disk, Linux disk, FAT32 disk, FLASH card, scratched CD, Digital Cameras, iPods, and almost any other media or file system that can be recognized in Mac OS X.
- FileSalvage can also recover data from mechanically unsound devices.
- can analyze and recover files from most third party tool disk images such as standard ISO, EnCase® (unencrypted images only), UNIX dd, Drive Genius™, and SubRosaSoft CopyCatX™

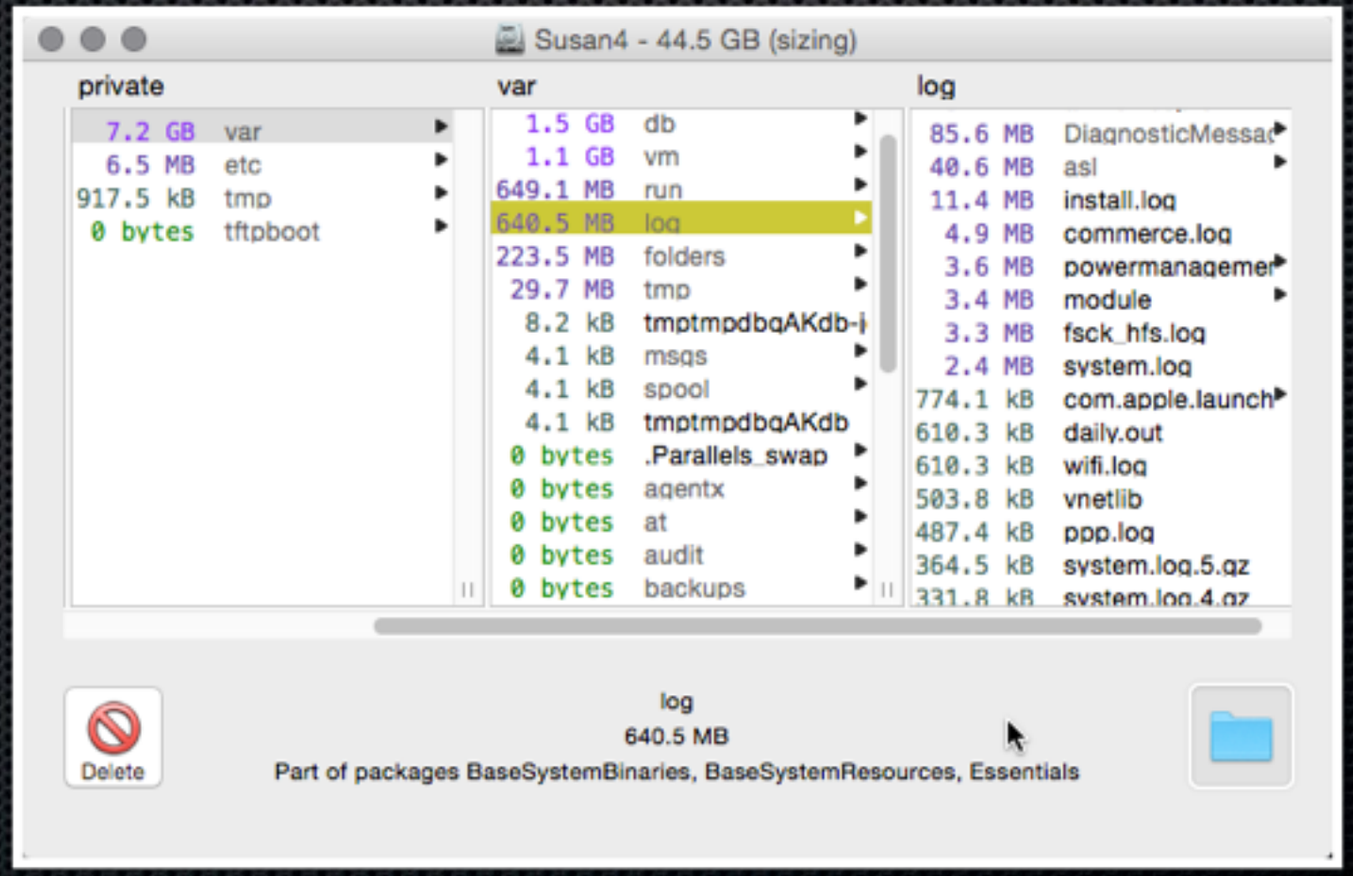
Which Process Is That?



- What Applications are running
- Which are draining the battery
- Get Info for stats & files used

Out of Space?

- OmniDisksweeper
  - sudo /path/to/OmniDiskSweeper.app/Contents/MacOS/OmniDiskSweeper
  - Command . to quit the app.



Disk Utility

- can erase, format, repair, and partition hard drives, as well as create RAID arrays. You can also use it to create a clone of any drive, including your startup drive.
- can unlock encrypted drives if password is known

Terminal Commands

- df - display free space
- du - display disk usage statistics
  - -h (human readable)
  - -d # (depth)
  - -c (grand total)

`du -h -d 1 -c ~` - get your home directory stats

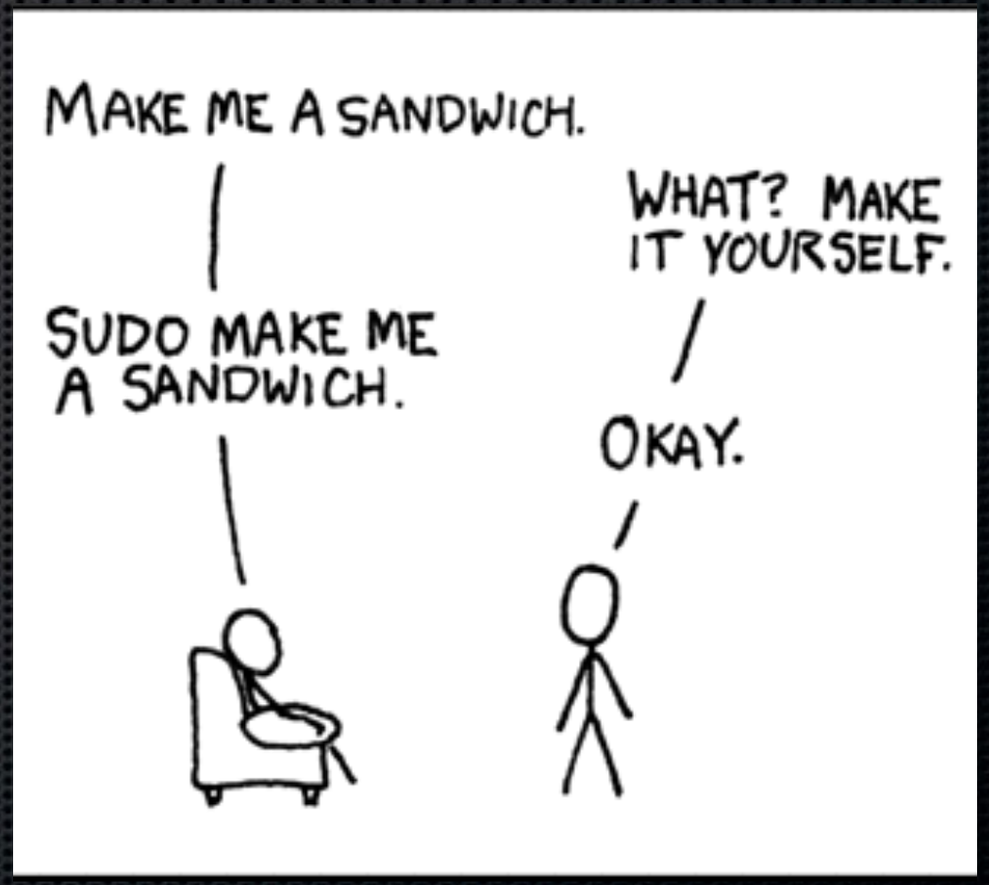
```
 11G  /Users/llincoln/Desktop
 10G  /Users/llincoln/Documents
3.1G  /Users/llincoln/Downloads
1.4G  /Users/llincoln/Dropbox
 11G  /Users/llincoln/Library
  0B  /Users/llincoln/Movies
 99G  /Users/llincoln/Music
8.4G  /Users/llincoln/Pictures
144G /Users/llincoln
144G total
```

Got Root?

sudo allows great power from the normal user-space.

The *sudo* Terminal command can be used by administrators to execute commands as root.

sudo command requires a non-blank admin password . [HT202035]



Terminal Commands

- Run an app with root permissions using sudo
  - Allows great power from the normal user-space
- Which process is that?
  - Use Activity Monitor to see what that random "java" app is.
  - # /Applications/Utilities/Activity\ Monitor.app/Contents/MacOS/Activity\ Monitor
    Find the process in question and Get Info to see what files it's using.
- Where is all the space?
  - OmniDisksweep the entire disk: http://www.omnigroup.com/more
  - sudo -s, then
    # /path/to/OmniDiskSweeper.app/Contents/MacOS/
    OmniDiskSweeper

Terminal Commands

- VIM Tutor

```
WM31E-84C:~ llincoln$ vimtutor

===============================================================
    =  W e l c o m e  t o  t h e  V I M  T u t o r  -  Version 1.7   =
===============================================================
```

Vim is a very powerful editor that has many commands, too many to explain in a tutor such as this. This tutor is designed to describe enough of the commands that you will be able to easily use Vim as an all-purpose editor.

The approximate time required to complete the tutor is 25-30 minutes, depending upon how much time is spent with experimentation.

Using SSH

- Logging into a client system, even while they are working on it
- running command line tools for fun and profit
- ssh (SSH client) is a program for logging into a remote machine and for executing commands on a remote machine. It is intended to replace rlogin and rsh, and provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections and arbitrary TCP ports can also be forwarded over the secure channel

SSH to another host

- done from terminal
- allows you to copy files to or from a remote host via the scp command
- allows you to perform tests remotely without taking control of the users environment
- can use “ps aux” to list all active processes and which accounts owns the process
- allows you to kill processes or restart services

Man, demystified

- ManOpen
  - Free install
  - Command-O to Open
  - Command-Shift-A to “apropos”

- Right Click on terminal command to launch or

- Use Preview via Terminal
  - `man -t command | open -f -a Preview`

Add to your .bashrc:

```
alias pman='man -t "*" | open -f -a Preview’
```

Text & Package Tools

- TextWrangler
- CSV Pro
- Pacifist
- Suspicious Package Quick Look Plugin
- Packages

TextWrangler

Feature	Benefit
It's free	One less thing to sell
Opens anything	View details like line endings
Process lines containing	isolate or delete excess info
Multi-File Search/Find All	Shows many instances
Opens binary plists	No need to convert

http://barebones.com/products/bbedit/comparison.html
http://barebones.com/products/textwrangler/benefits.html

Wrangling CSVs

- Handles line breaks with ease
- Split columns on a space, or any other character
- Rearrange columns as needed
- Great developer support
  (feature requests added, bugs fixed)

Packages, demystified

- Pacifist
  - Just what's in the package?
  - What are the scripts going to do before, or after?

- Suspicious Package Quick Look Plugin
  - Select any installer package in the Finder, and choose Quick Look from the File menu — or just press the spacebar.
  - Suspicious Package will examine the package, and show a preview in the Quick Look window.

Packaging, demystified

- Packages
- “Just make a package”..yeah right. Right!
- Learn by example feature
- Put files where they need to be, permissions included
- Let your end-users run scripts with a pkg

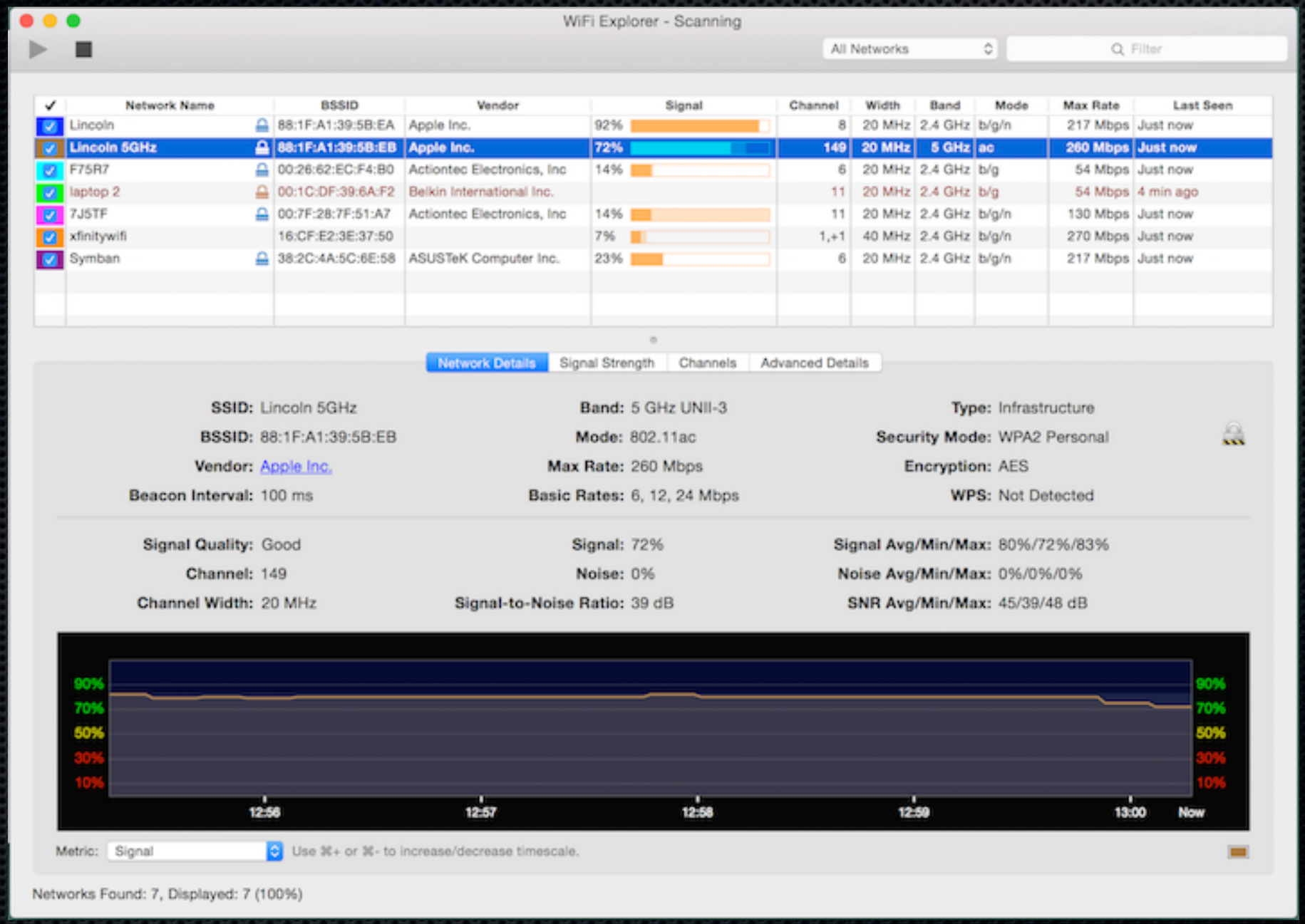
Network Utilities

- WiFi Explorer
- Bonjour Browser
- Open Port Check Tool: http://www.canyouseeme.org
- Subnet calculator: http://www.subnetmask.info
- http://www.whatismyip.com
- http://www.downforeveryoneorjustme.com/

WI-FI Explorer

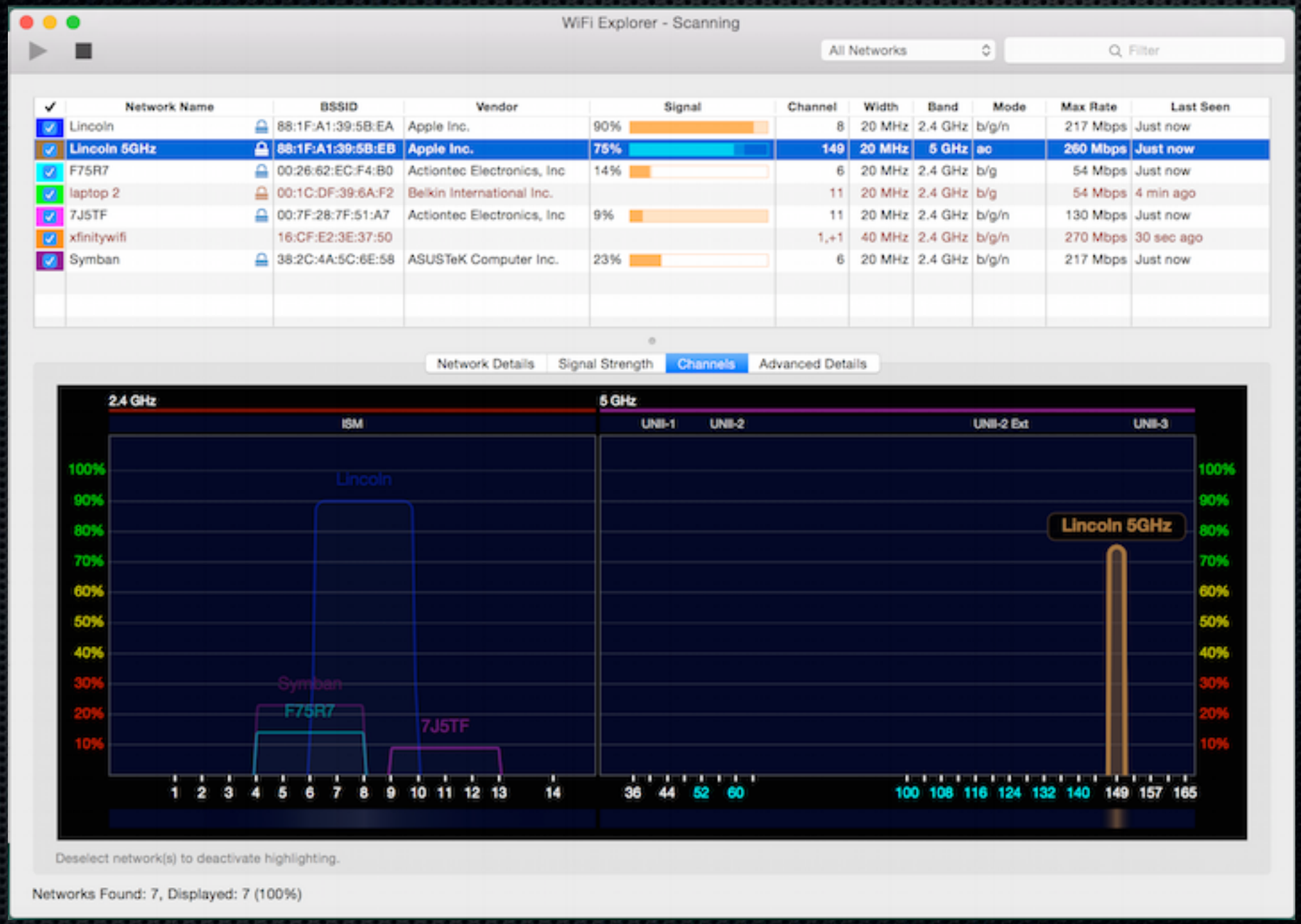
- Scan, monitor, and troubleshoot wireless networks
- Quickly identify channel conflicts, signal overlapping or configuration problems.
- Get an insight into the network details
- Graphical visualization of the Wi-Fi environment
- Supports current standards of 2.4/5 GHz frequency bands as well as 20/40/80/160 MHz channels
- Works with 802.11a/b/g/n/ac networks

WiFi Explorer



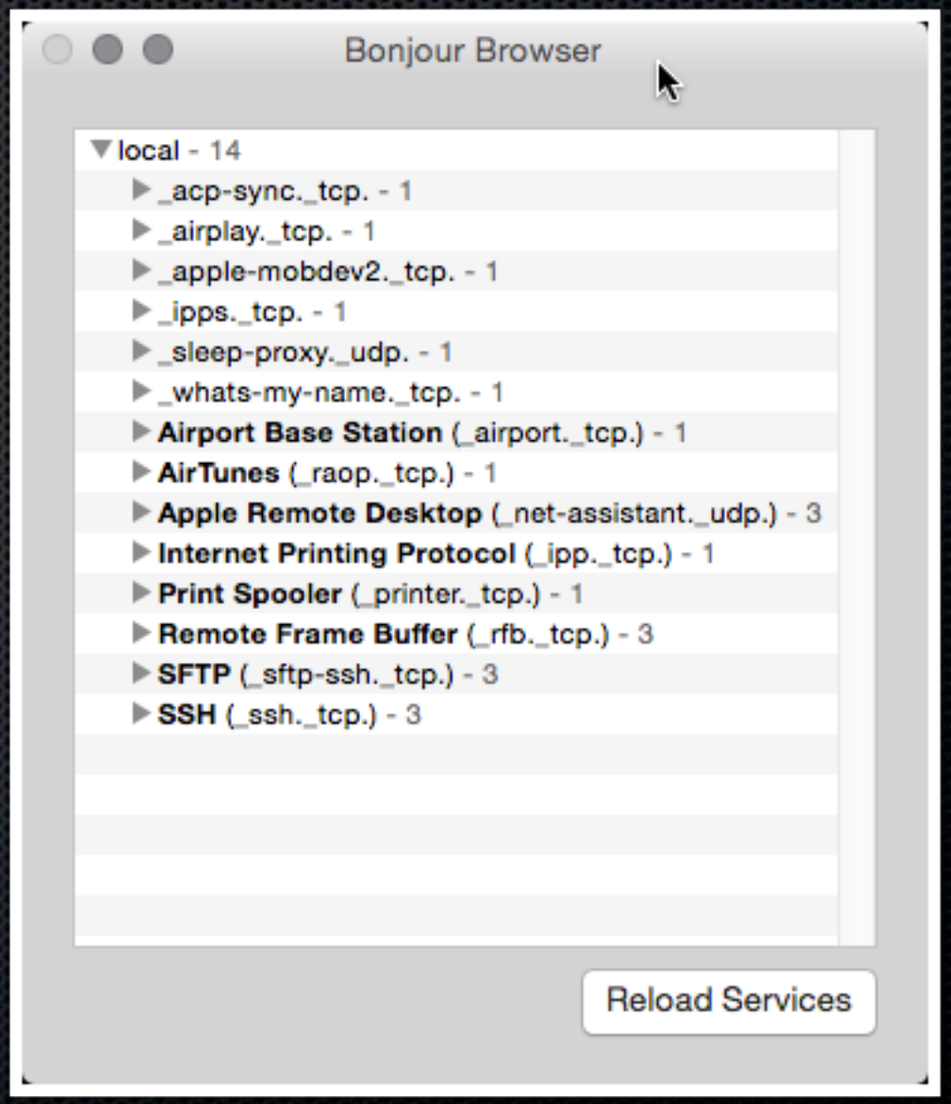
WiFi Explorer

WiFi Explorer



Hello, Who's on my LAN?

- Bonjour Browser
  - Effortlessly discovers Macs and recent printers on your LAN.
  - Displays great information for locating devices.
  - Bring your copy & paste!

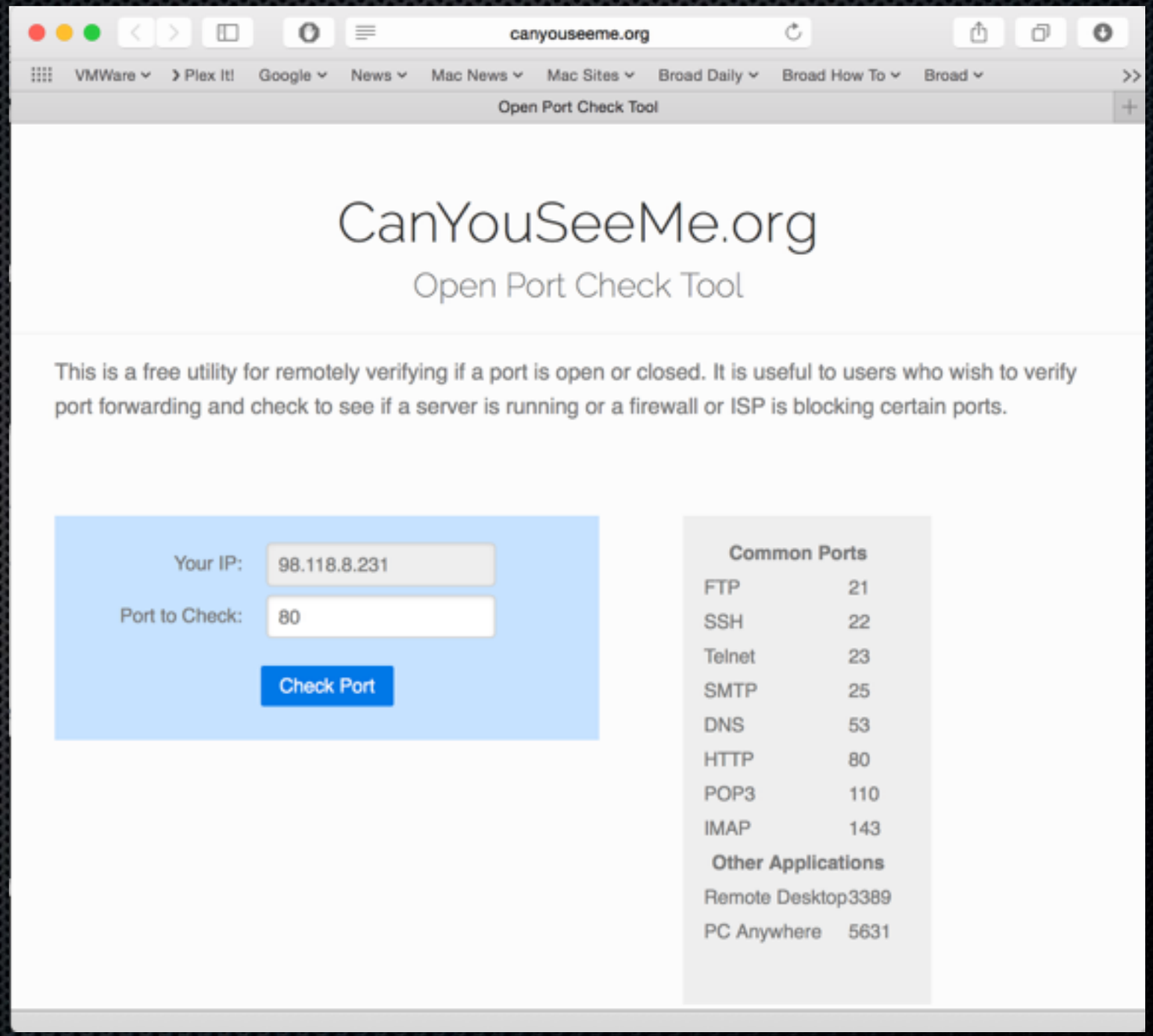


Hello, Who's on my LAN?

- Use **arp -a**
  - Address Resolution for discovery.
  - ping 255.255.255.255
  - arp -a for a list of all discovered devices
  - The result is a list of IP and MAC addresses

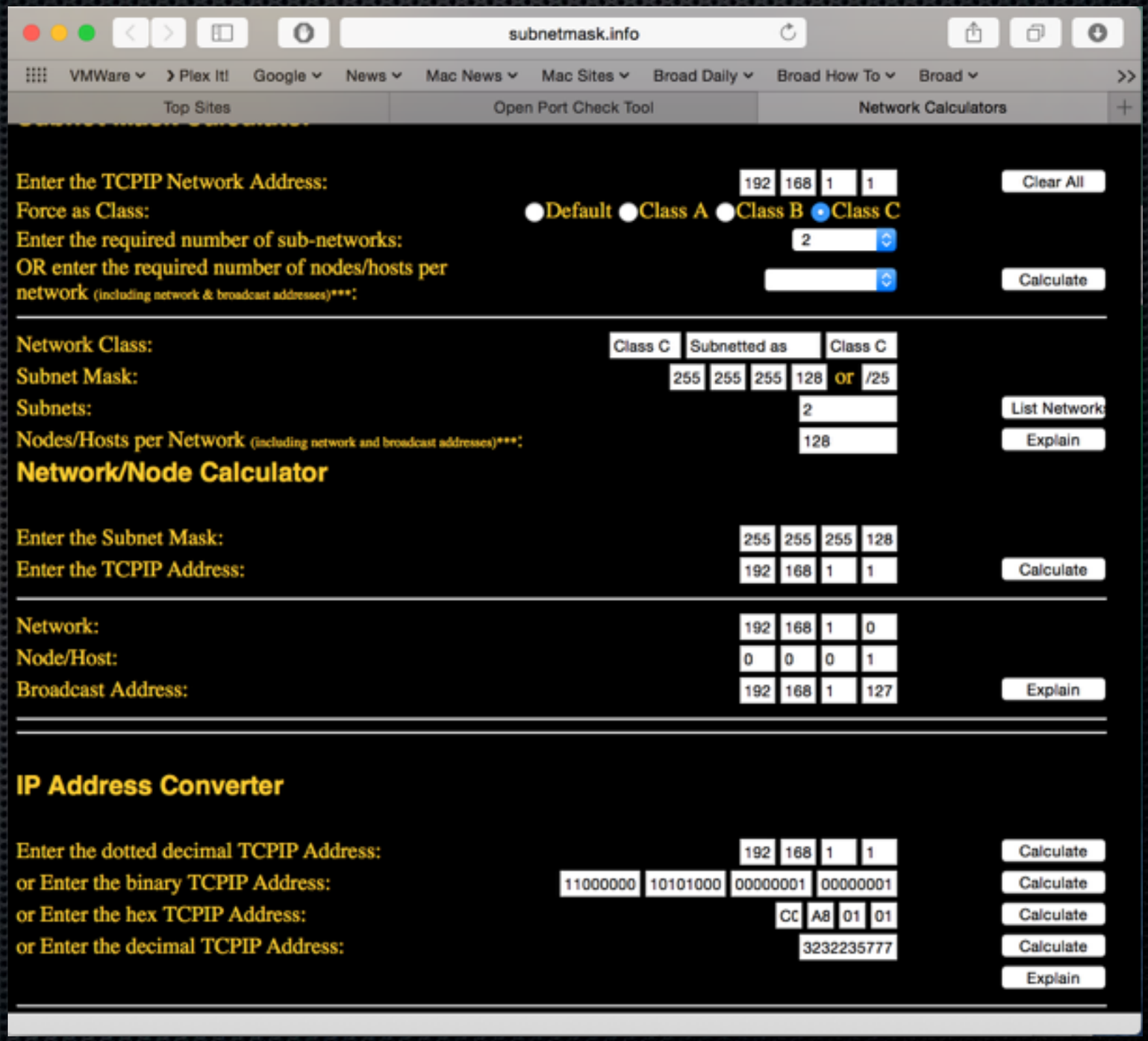
Open Port Check

- Free Utility
- verify your ports
- check if port forwarding is working
- Launch this website from the device you want to check



Subnet Mask Calculator

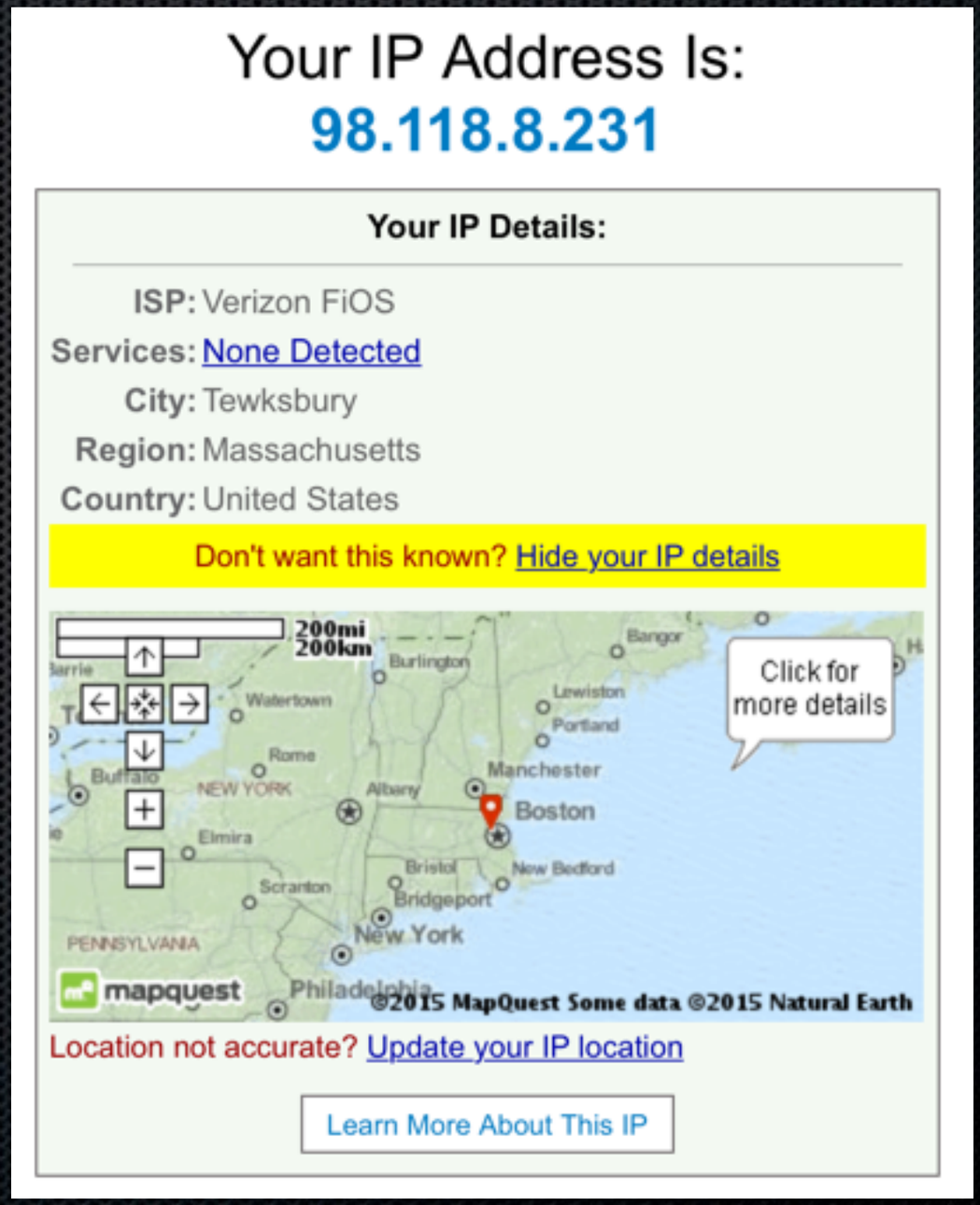
- Easy to Use
- Powerful
- FREE!!!



MACTECH PRO EVENTS

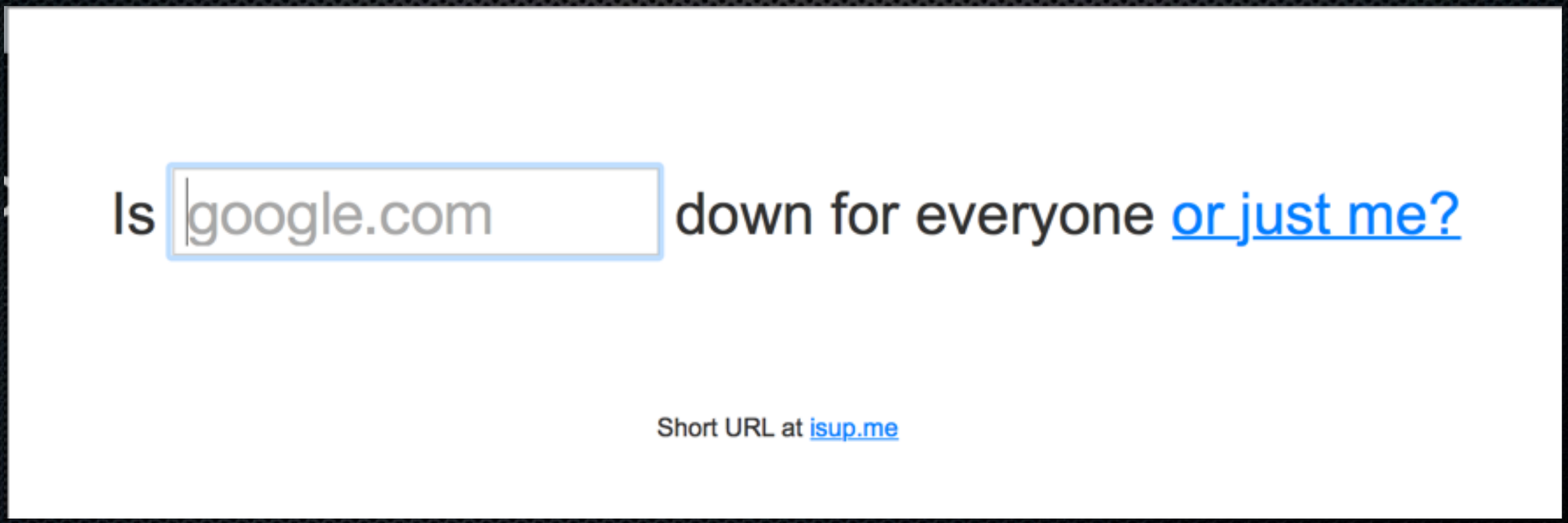
What is my IP

- Easy
- run from system you want to check



downforeveryoneorjustme.com

- website allows you to checks sites from outside your network



Stream Watching

tcpflow

- What's the benefit? Follow along:
- Download TCPFlow - Rudix
- Figure out which network-interface has the interesting traffic (en0, etc)
- Follow one of these examples:
  - `sudo /usr/local/bin/tcpflow -c -i en0 host 10.0.1.1`
    - Watches all traffic to 10.0.1.1
  - `sudo /usr/local/bin/tcpflow -c -i en1 tcp port 80`
    - Watches all traffic on port 80

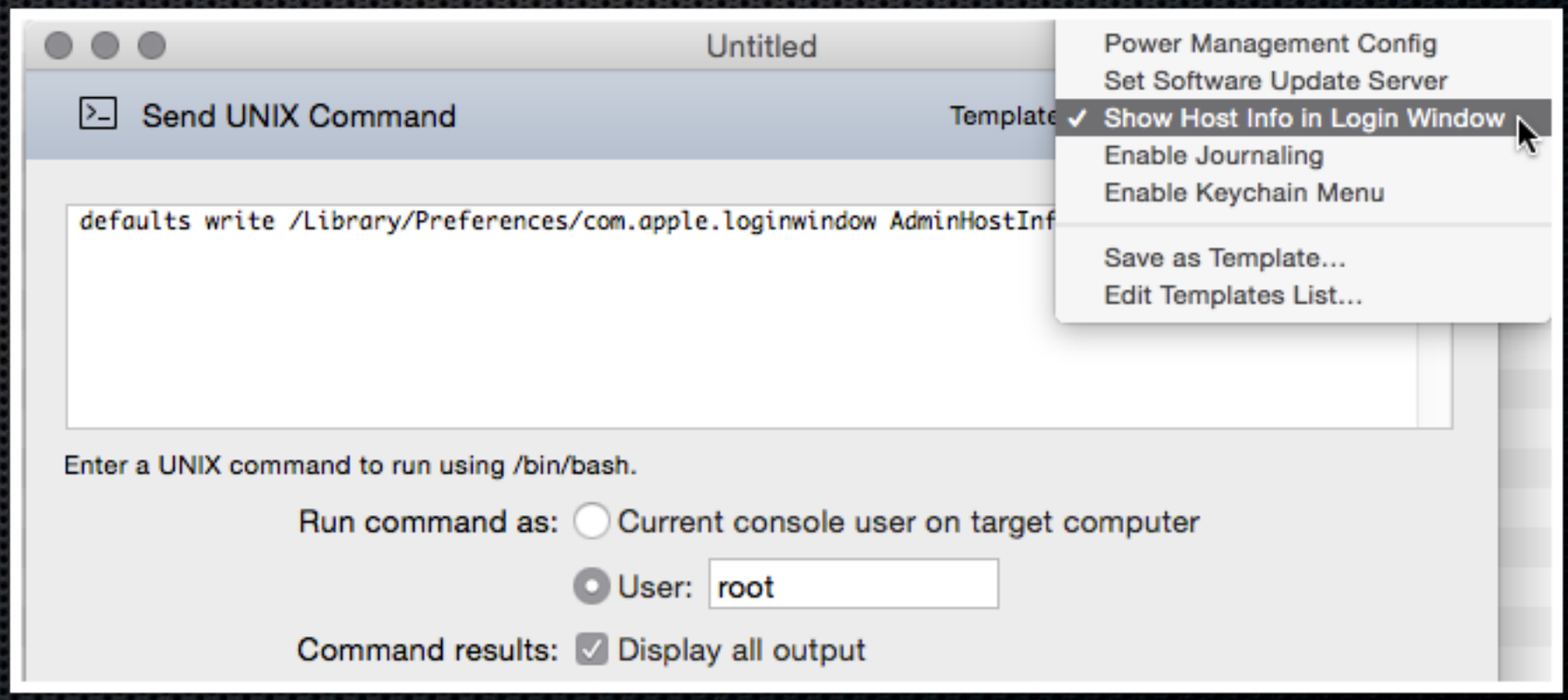
- This is especially handy when troubleshooting smtp process, or directory server setup (before enabling ssl)
- Learn more at: http://www.office.mvps.org/troubleshoot/tcpflow.html

Screen Sharing

- Apple Remote Desktop (ARD), now $75
- Screen Sharing
- TeamViewer

ARD - Apple Remote Desktop
Save time, improve memory

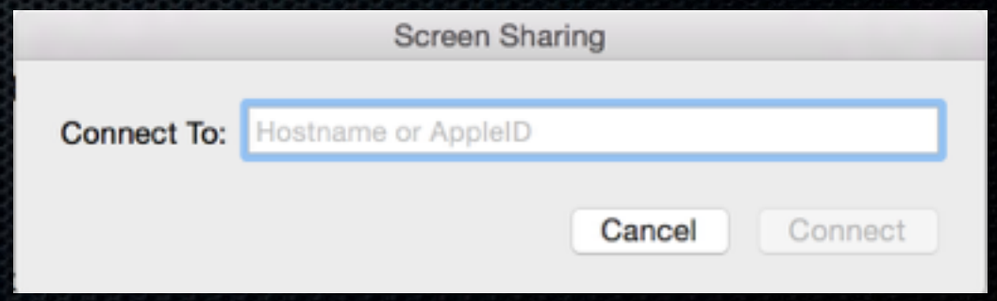
- Save common items to the sidebar.
- Save scripts as templates
- Repeat!
- Remember!



~/Library/Application\ Support/Remote\ Desktop/Presets/UnixCommandTask.plist

Screen Sharing

- https://support.apple.com/kb/PH18689?locale=en_US&viewlocale=en_US
- Can be launched by running the app or using vnc://ipaddress or dnsname
- Allows you to login to a different account than the active user
- great for checking processes



Team Viewer

- Remote Support and Remote Access
  - works with out port forwarding or special settings on proxy or firewalls
  - end user for support does not need to install any software

Hey, where's my stuff?

- EasyFind
  - It's fast!
  - Finds anywhere on the filesystem, even inside files
  - So much control you'd think it was Sherlock
- FoxTrot
  - Indexes data for fast, up to date results
  - Search a network share? OK
    - SMB, NAS, OS X Server
  - Pro Versions can keep a running current index

Dude, where's my screenshot?

- SnapNDrag
  - Simple screenshots of sections, windows, etc.
  - Keeps all screenshots in a central library
  - Resize, edit in Preview, revert to original
  - Rename & share

- Skitch
  - Advanced options for marking up images.

- Clarify
  - Quickly generate instructions with screenshots
  - Customize with branded template
  - Professional looking

Get off of my Mac

- BatChmod
  - Keeps all my 755s 755, recursively, if I want.
  - Strip xattr from files with ease.

- chflags
  - `chflags nohidden` will find that missing volume

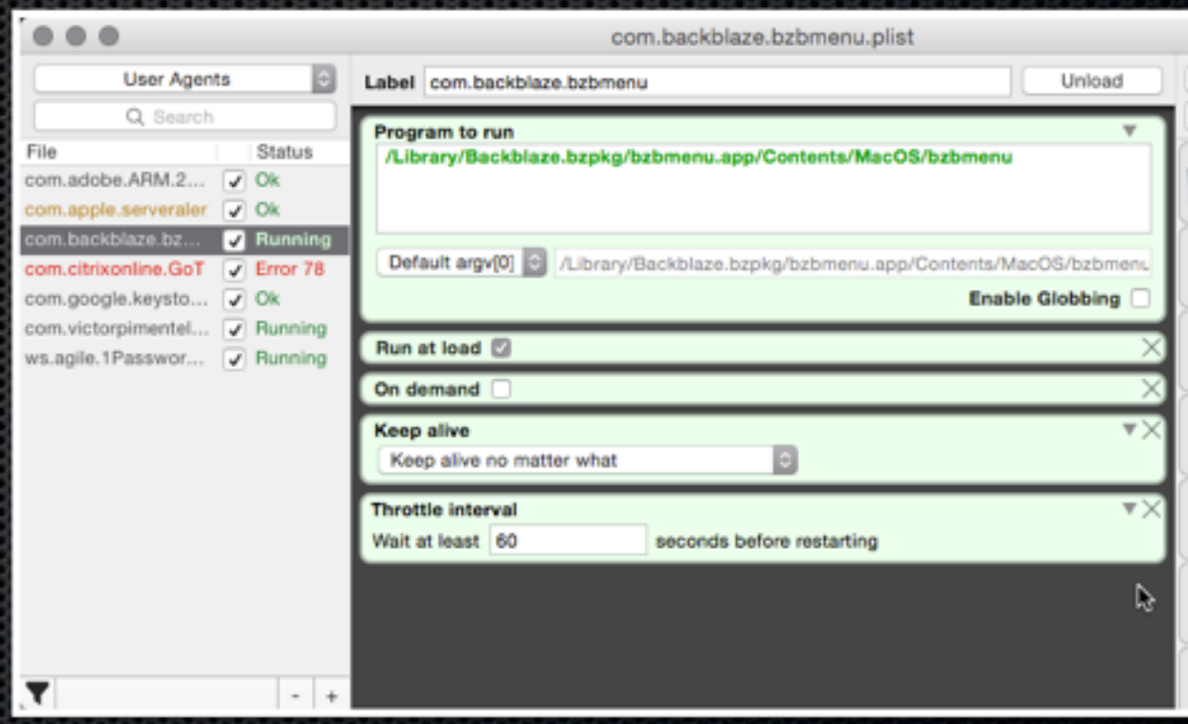
- SideTrash
  - Move a file to the trash via Proxy icon
  - Useful if you like to have the trash available on every Finder window

Too many ads

- Yes, Another Plug for
- AdwareMedic
  - Worst feature?
  - Best feature?
    - It has to be run manually

LaunchD-what?

- LaunchControl
  - Discover what's going on your computer.
  - What's being run, from where, when.
  - Troubleshoot background processes



- launchd.info - Learn what makes a Mac mac.

Email tools

- Emailchemy
  - Convert, Migrate, Manage any format to any format.

- Email Extractor
  - Extracts every email address from a Mailbox & more.

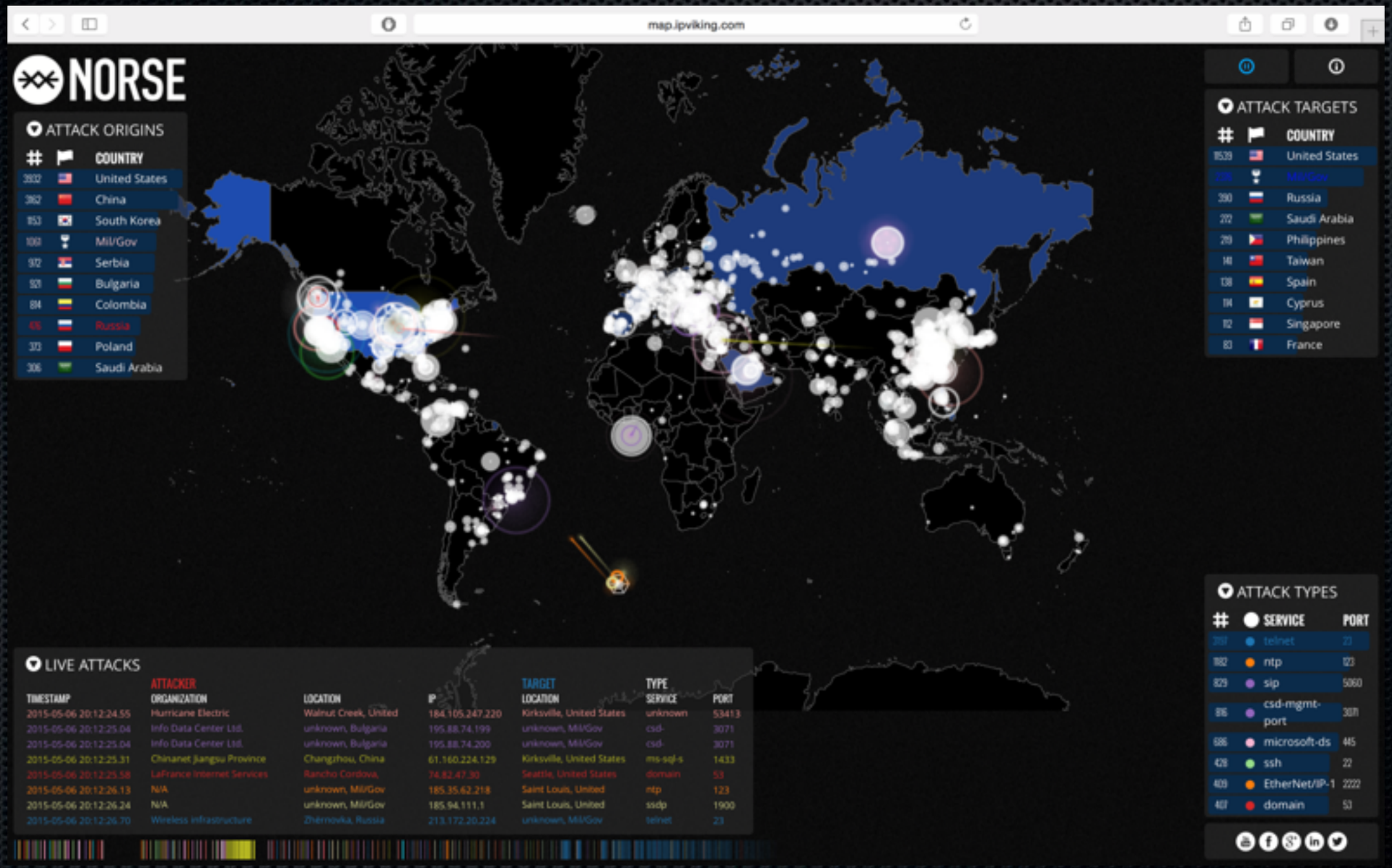
Database Administration

- Sequel Pro - MySQL, Free
- Portico (formerly PG Commander)
  Postgres, simple, friendly
- phpMyAdmin - MySQL, Free, web-based

Mac Models

- MacTracker
  - Determine Max Memory
  - Max Mac OS?
  - Search by Serial Number
  - Settle Bets
    Learn your Apple History
- EveryMac - online runner up

Network Threats



Questions?

Leon Lincoln, III
llincoln@broadinstitute.org
Linkedin: llincoln3

Email Grooming

- MxToolbox
- emailreg.org
- multirbl.valli.org/dnsbl-lookup/
- ProjectHoneyPot
- http://www.mcafee.com/threat-intelligence/ip/default.aspx
- http://www.reputationauthority.org/lookup.php
- SenderBase.org
- SenderScore
- http://www.kloth.net/services/dnsbl.php
- www.c-sirt.org/lang/en-us/incidents-on-ip

Web security tools

- www.internetofficer.com/seo-tool/redirect-check/
- InlineStyler - Convert CSS rules into inline attributes
- Sucuri.net
- https://www.changedetection.com

More Resources

- Common Ports for Apple Software [HT202944]
- DisplayMenu - Get the display menu back in 10.9 & 10.10

More Resources

- PhoneView
- iExplore
- Munki
- AutoPkg / AutoPkgr
- Whatskeepingme
- Gemini - duplicate finding
- DiskDiags
- DiskDrill Pro - Data Recovery
- DataRescue - Data Recovery
- R-Studio - Data Recovery
- DriveGenius
- SmartUtility
- Onyx

- Cocktail
- iStumbler
- iNet
- Netspot Pro
- Transmit
- MacUpdate
- Grapho
- Draw.io
- Lucid Charts
- Paragon
- Tinkertool
- TimeMachine Editor

Web page tools

- http://www.internetofficer.com/seo-tool/redirect-check/
- http://inlinestyler.torchboxapps.com
- http://www.sucuri.com
- https://www.changedetection.com