

## Useful applications for your computer

Written by David Rivenburg, AD500

Tuesday, 23 February 2010 17:29 - Last Updated Sunday, 17 October 2010 20:37

---

[Backtrack](#) , formerly known as the *Auditor Security Collection CD*, is a bootable Linux CD (Live CD) that runs in RAM. You can boot this tool, use it and then reboot to your hard drive with no footprint or disruption at all. Tools here include Kismet and other great wireless tools. Tools are provided to test the external hardening of networks against attack.

[Ethereal](#) is the best deal around. It's almost universally acclaimed as THE packet sniffer for nearly any OS. Formerly, special network cards and unique software were needed to do this task. Costs of \$4000 to \$8000 were paid by major corporate I/T departments to get fewer features than this package delivers for free.

[Kismet](#) is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic. When used with a GPS receiver, maps of detected wireless networks can be generated.

[Network Stumbler](#) , also known as NetStumbler, is an excellent tool if you run Windows and have a compatible card. It can make use of a GPS signal, writes log files and is easily used to measure or peak up signal strength on wireless networks. "War Driving" is the term used when you run NetStumbler or a similar tool while mobile. It is amazing the number of wireless systems already deployed and even more amazing at how many of those have the default channel, SSID and no WEP in use.

[Insider](#) is another wireless scanning tool for Windows systems. It has additional graphing and some improved features from NetStumbler including waterfall displays, graphing per channel and more. It should be a core tool you carry.

[s3d](#) is a 3d network display server for Linux which can be used as 3d desktop environment.

[SPLAT!](#) provides site engineering data such as the great circle distances and bearings between sites, antenna elevation angles (uptilt), depression angles (downtilt), antenna height above mean sea level, antenna height above average terrain, bearings and distances to known obstructions based on U.S. Geological Survey and Space Shuttle Radar Topography Mission elevation data, path loss and field strength based on the Longley-Rice Irregular Terrain Model, and minimum antenna height requirements needed to establish line-of-sight communication paths and Fresnel Zone clearances absent of obstructions due to terrain. You can try out the online version [here](#) but you will have to work with existing sites in the database. Alternately, you can register, insert 2 or more of your own sites and then do your own path studies.