CHAMPLAIN COLLEGE

LCDI

The Senator Patrick Leahy Center for Digital Investigation

Access Point Tool Review

Written by
LCDI

175 Lakeside Ave, Room 300A
Phone: 802/865-5744
Fax: 802/865-6446
http://www.lcdi.champlin.edu

June 28, 2013

Disclaimer:

This document contains information based on research that has been gathered by employee(s) of The Senator Patrick Leahy Center for Digital Investigation (LCDI). The data contained in this project is submitted voluntarily and is unaudited. Every effort has been made by LCDI to assure the accuracy and reliability of the data contained in this report. However, LCDI nor any of our employees make no representation, warranty or guarantee in connection with this report and hereby expressly disclaims any liability or responsibility for loss or damage resulting from use of this data. Information in this report can be downloaded and redistributed by any person or persons. Any redistribution must maintain the LCDI logo and any references from this report must be properly annotated.

Contents

Introduction

Background:
According to techterms.com, an access point is a "device, such as a wireless router, that allows wireless devices to connect to a network."[1] The ability to examine these points could present an investigator with critical evidence and help to evaluate criminal activity.

Purpose and Scope:
We were asked to evaluate access point tools which met certain criteria and could be used for case work. These criteria included network details, GPS views, the ability to plot access points on a map, logging functions, and a reporting feature. We chose to first research inSIDDer home and inSIDDer office by Metageek. These tools are designed for network troubleshooting and are able to get access point information as well. We also researched tools by Ekahau, who made a site surveying tool for troubleshooting and optimizing networks. This tool also provides access point information that could be useful to network administrators. Several of the best tools we have found are developed by a company called Fluke Networks. Fluke Networks is a versatile tech company that has several areas of focus. One of their specialties is Wi-Fi analysis and troubleshooting, and they create tools that can be used for network administrators to review their network and ensure it is set up optimally. However, some of Fluke's tools have a focus not only on network administrators as other network monitoring tools would, but on law enforcement additionally. Because of their ability to adapt classic network monitoring tools and gear them towards law enforcement, we decided to review a small number of tools by Fluke networks. There were two tools by Fluke Networks that really stood out as being extremely powerful for getting access point information. These tools were the AirCheck and the AirMagnet Survey Pro. We requested a demo of these tools, and Fluke networks allowed us to try them for a period of time. Through our demo, we were able to get hands-on experience with each of the tools and evaluate their capabilities for local law enforcement.

Research Questions:
Does the tool provide detailed network information?

Can the tool show GPS mapping views?

Does this tool have the ability to plot access points on a map?

Are there logging functions this tool implements?

Is there a reporting feature for the results?

Terminology:
When looking at access point tools, it is important to have a base knowledge of certain terminology to understand exactly what the tools are doing and what they are capable of. Here are some common terms that arise when dealing with these access point tools.

[1] Tech Terms Access Point Defined http://www.techterms.com/definition/accesspoint

Access Point: An access point is a device that allows for another device, or a client, to connect to a network. An example would be a router. There can be several access points for one network, so that clients can connect to the closest access point and get the best service.

Channel: Channel is the word given to the various bands that communications travel on.

Client: A device that is connected to a network is referred to as a client.

Network: A network is a group of machines linked together is a network.

Signal to Noise Ratio: This is the term used to describe the level of useful signal in comparison to background noise.

SSID: SSID stands for service set identifier. It is the name of the network.

Methodology and Methods

We were given a trial of both AirCheck and AirMagnet to test , with our main goal being to evaluate which was better designed for access point surveying. We will be testing these tools on our local networks to study their capabilities. The AirCheck WiFi Tester is a standalone device that is designed to allow law enforcement to analyze WiFi connections in the area. AirMagnet Survey Pro is designed for optimizing networks; however, it has lots of useful functions that could help law enforcement as shown in the chart below. Here is a quick overview of how the two tools we looked at were able to handle certain functions.

	Network Details	GPS	Logging	Map Plotting	Reporting
AirCheck WiFi Tester	Yes	No	Yes	No	Yes
AirMagnet Survey Pro	Yes	Yes	Yes	Yes	Yes

AirCheck WiFi Tester

Figure 1

Introduction

The AirCheck™ WiFi Tester is a dedicated standalone device designed for examining wireless access points. With a simple display and home screen as shown in **Figure 1**, it is designed so that law enforcement can easily locate access points in the area, look for networks, see what clients are currently communicating, and better analyze their surroundings. It has a friendly and easy-to-read interface that can make access point surveying quick and easy. Costing around $2000, this tool is an investment, but its ability to accurately find access points and open networks can save law enforcement agencies time and money in the long run. The AirCheck™ WiFi Tester is a user-friendly tool set up to make work for law enforcement faster and more efficient.

Network Details

AirCheck has a feature that views network information such as the security type and 802.11 protocols. **Figure 2** (shown below) displays the home screen of the AirCheck WiFi tester. There are several different network features the user can examine. Checking network information simply requires clicking the first button on the home screen.

Figure 2

This brings you to the networks display page, which shows the time the network was picked up, the signal to noise ratio, if the network is locked or unlocked, the number of access points for this network, and the SSID. If the user scrolls over to the next page, it also gives the 802.11 protocol info for each network. Everything is displayed clearly and in an easy to read format. **Figure 3** shows a screen shot of this network screen. As

previously mentioned, more information can be displayed to the user by scrolling to the right, but this shows clearly each network's SSID, signal strength, security, and 802.11 protocol info.

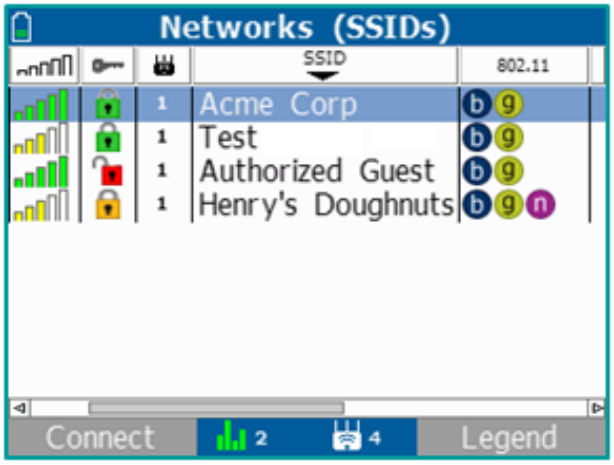

Figure 3

GPS

The AirCheck™ WiFi Tester does not provide GPS mapping. However, it does provide ways to locate access points, networks, and clients. By using the removable antenna, it has the ability look for signals given out by a particular device. The locate button, which appears in the right hand corner, tracks these signals on a graph and displays its strength. A user can then survey the area for strong signal strength and pinpoint a device.

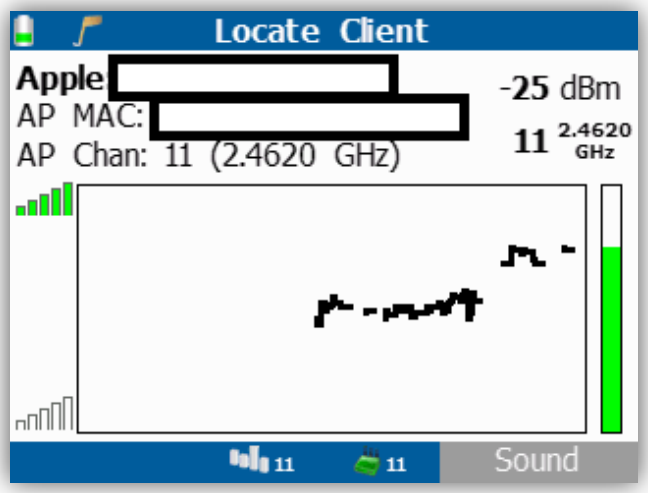

Figure 4

Figure 4 displays a test we ran on one of our own devices. We wanted to see if AirCheck could find a personal iPhone. Because AirCheck can only pick up a device if there is an active Wi-Fi signal or a signal that is currently connected to the network and giving off requests, we decided to stream a video on the phone to establish a constant signal. Then, using AirCheck, we found the device by its MAC address. When we pointed the antenna towards the device, the AirCheck began beeping, and the signal, shown on the graph, went up. The

green bar on the right is also an indicator that informs you of how close to the device you are. Please note that in this example we hid the MAC address and access point.

Logging

You can save your session by hitting the save button (the button with the floppy disk on it- see **Figure 5**). By connecting the device to your PC and using the provided software, you can upload your session into a dated report of all of your findings from the time you powered on the device to shutting it off. Multiple sessions can be saved and stored by the date and time. Screenshots can also be taken by pressing the back button and the home button at the same time as seen in **Figure 5**.

Figure 5

Plotting on a Map

Map plotting is not available; however, the "locate" feature, as described in the GPS section, makes it easy to find and track down clients, access points, or networks that can then be manually plotted on a map.

Reporting

There is reporting software that comes with the AirCheck device. It can display the information you see during your AirCheck survey, including information about the devices, SSID, security, access points, channels, etc. The software builds the reports for you automatically based on what it logged from the session you select.

Additional Features

Depending on the scope of your search and what you know, you can approach the AirCheck's search feature several different ways. You can start by looking at a network, access point, channel, or client. You can also see the traffic, noise, and access points on each channel, as seen in **Figure 6**. The channel view allows the user to view the activity over a broad range and narrow down on which channels appear to show suspicious network trends.

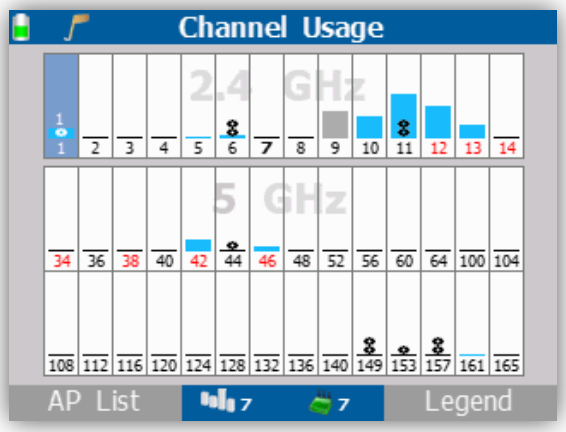

Figure 6

Conclusion

After participating in a demo of Fluke Network's AirCheck WiFi Tester, our team has a better understanding of the tool and its importance in access point surveillance.

The AirCheck WiFi tester could be a valuable tool for access point surveys with its extensive but easy to use features. It is a stand-alone device that is simple to use, allowing almost any individual to operate it. The tool costs $2,000, which may seem expensive when compared to other devices, but it offers information that can save an investigator time and money over time. As one example, if an investigator were to go to a suspect's residence, he or she could determine if there are open networks or other access points in the area that the suspect could have been connecting to, and this can define the scope f the search by either expanding or narrowing it accordingly. A case study of the Martinez California Police Department shows how officers originally used iPhones to look for open networks, which was inefficient as the iPhones were not designed for that purpose. After getting AirCheck, the department was able to narrow down searches and became aware of what it was dealing with.[2] Other network analysis tools come at a lower price, but are geared more towards analyzing a network for connection problems. They are designed for network administrators primarily. The AirCheck saves money by preventing law enforcement from wasting their time, effort, people, and resources because they can be aware of their suspect's surroundings and resources.

There are other access point programs, but none of the other tools we looked over were comparable to this specific program in either simplicity or accuracy. A number of other access point programs operate on a laptop and involve complicated setup, making them difficult to access when doing field work. Laptops are comparatively fragile and not designed for this job. The AirCheck WiFi tester is built with a four hour battery life for field work. The screen is bright and can be seen easily, even when outdoors in the sun. A laptop would have to sacrifice battery life for the same level of brightness.

This tool allows a user multiple ways to approach a search. You can start by looking at channels, clients, access points, or networks. If you know what you are looking for, this will determine how you approach your investigation. Additionally, from each of these points, you can get more information about the other points. For example, if you are in clients, you can get information about the network each client is on, and if you are in networks, you can get information about the network's clients. The information you have at the beginning of the investigation will decide how you use the survey tool. With this tool, a search can be narrowed and allows for an easy and efficient investigation.

[2] Fluke Networks Case Studies http://www.flukenetworks.com/content/law-enforcement-resource-page

AirMagnet Survey Pro

Introduction

AirMagnet Survey Pro is an advanced piece of software that is run off a laptop and is capable of access point mapping features. It is designed for planning an efficient and cost effective network. The tool has useful functions, but proper set up is often difficult due to the required floor plans or GPS maps needed to use the tool. Along with initial setup, the tool requires lots of user knowledge in order to operate it correctly. A user may need extensive training in order to operate it to its full potential; however, there is training available followed by a certification test if an individual is willing to pay for it. Despite the complications for a user to operate the tool due to the initial time and knowledge necessary, it has a lot of useful functions when analyzing access points.

Network Details

The AirMagnet Survey Pro can provide an investigator with a large amount of network information. When starting a survey, it asks for floor plans to be imported for an indoor view, or a GPS map to be used for an outdoor survey. The floor plan's dimensions must be added and the unit of measurement must be selected as well. For GPS outdoor surveys, the map must be imported and the unit of measurement has to be selected. During our demo, we were unable to do this as we only had a test version of the tool. However, they provided premade tests that we were able to look at. From these premade tests, you could see channels and SSIDs of the area, as well as the access points associated with each channel or SSID. They also integrated of filters, so that a user can filter out and look at only what he or she needs to see.

GPS

A GPS survey is possible for outdoor investigations with the AirMagnet Survey Pro; however, it requires the integration of an external GPS device (**Figure 7**). The GPS continually collects data and imports it to the computer. Otherwise a map can be imported, and the unit of measurement be selected.

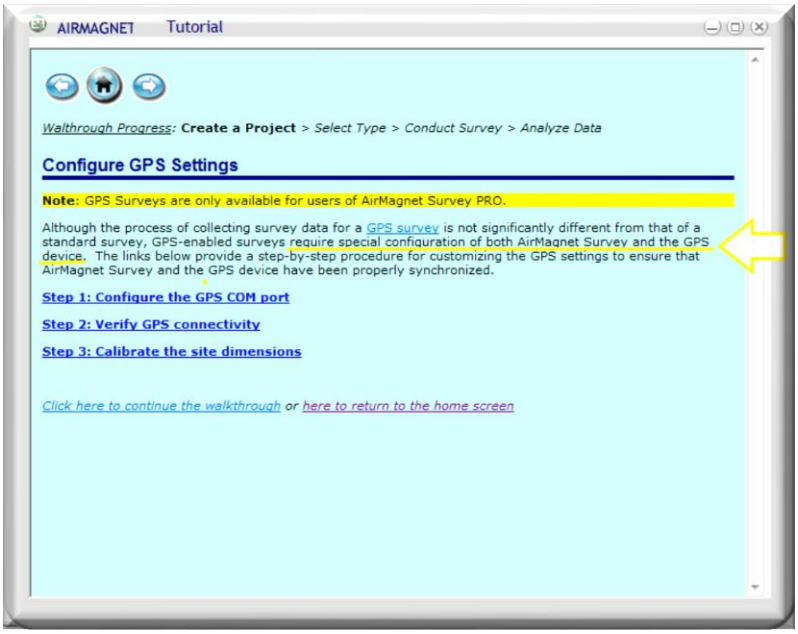

Figure 7

Logging

There are a couple of different tests that can be logged with AirMagnet Survey Pro. One test is the passive test. During passive tests, the tool automatically records all RF signals from all the access points in the area. With active tests, the AirMagnet Survey Pro program imitates a device so you can see exactly how that device would react to different locations. Both surveys can be logged and opened later.

Plotting on a Map

This tool allows the user to plot access points on a map. A map must be imported or GPS integration must be used in order to access this tool. This makes it easy to see where all the access points in a large area are. The signal strength is displayed for each access point on an individual channel or SSID in a color coded fashion, making it easy to view a particular target or the full area. In **Figure 8** a specific network has been filtered out, showing one individual network's signal strengths.

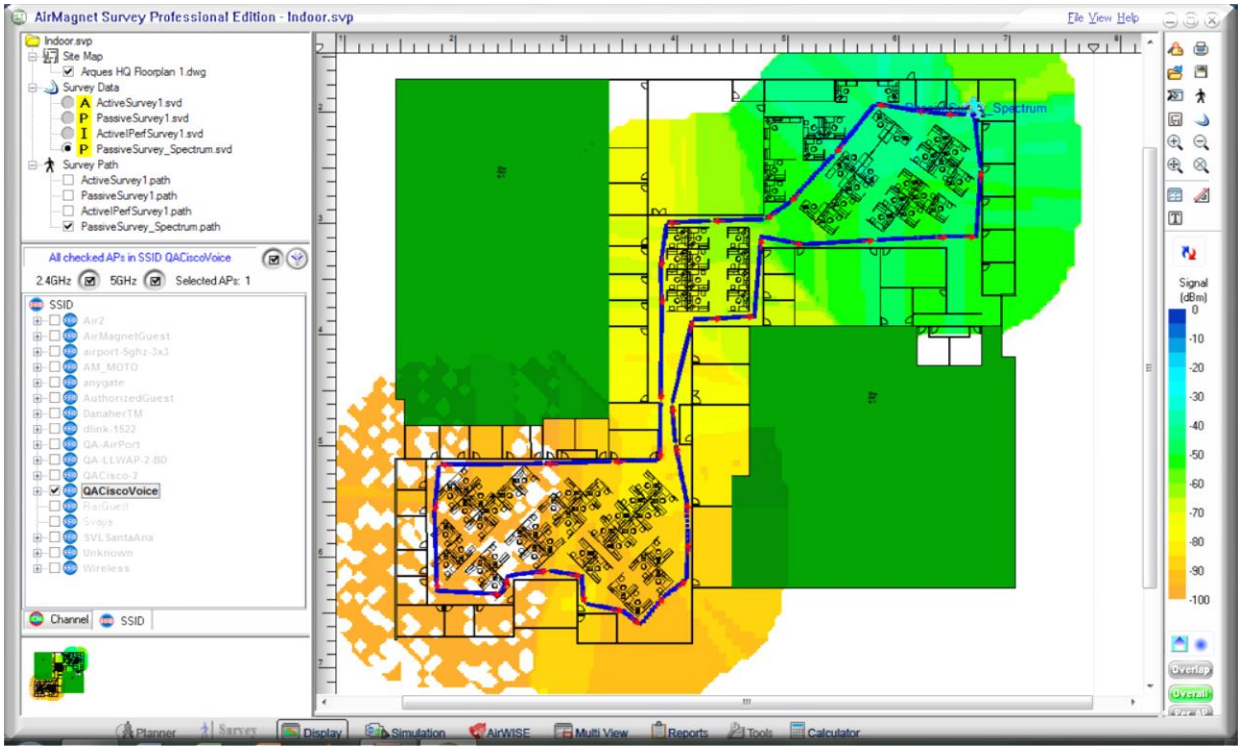

Figure 8

Reporting

We were able to print the picture of the map with the filters we selected. In this printed report, it lists the access point name, the channel it is on, SSID, power, and signal strength. By adjusting the filters and choosing exactly what is relevant, you can customize your report. There is a separate reporting feature we did not have access to in the trial version.

To access this feature, there are specific requirements, including having AirMagnet Survey Pro installed on your laptop, the AirMagnet Spectrum Analyzer Adapter inserted in a wireless network card slot on the system, and the spectrum analyzer feature enabled on AirMagnet survey.

Additional Features

Investigators can use this tool to map out a path that was walked during a site survey, helping investigators keep track of where they looked and what information they gathered in a specific area. From this path, they can see the access point information they collected from that session. The path outlined in red shows the data gathered from an individual session, as seen in **Figure 9**. . Investigators can have multiple sessions with multiple paths. They can then use the filters to select which path and which session they would like more information on.

Figure 8

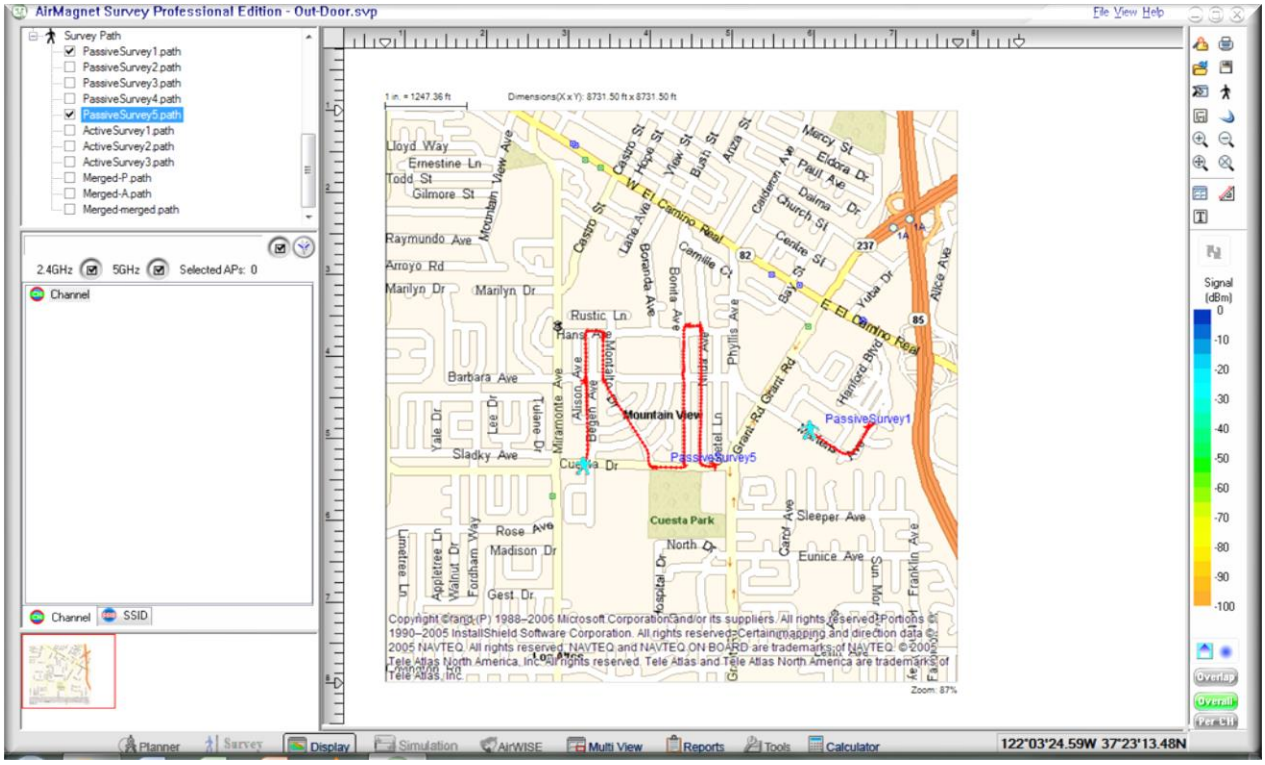

Figure 9

Conclusion

This tool is capable of showing large amounts of relevant data in a visually appealing manor. The mapping feature with color coded signal strengths makes it easy to quickly look at access point information; however, the initial setup is complicated. Getting the map imported perfectly is difficult as most people do not have floor plans readily accessible, and using the tool requires technical knowledge. There are training courses and certifications specifically for the use of the AirMagnet Survey Pro. The use of this tool during an investigation would most likely have to be delegated to a dedicated person who knows how to use it, because it is not something that could be picked up by any user. It is also not ideal for the field because it has to be run on a laptop with a limited battery life.

Recommendations

We tested two tools by Fluke Networks used to look at access point information. They both have their strengths and weaknesses, and they could both benefit investigators. The best tool is really determined by the situation and what the investigator is trying to do.

If an investigator needs to quickly get to a site and wants a reliable, easy to use tool to grab access point information, AirCheck would be preferable over its counterpart. It is easy to use, built for use on the go, and can quickly give officials the information they need without any complications.

If an investigator wanted to plot the access points of an area so they would have a map for future references and an idea of the area, he or she would most likely use AirMagnet. It has thorough mapping capabilities and a clear picture; however, it requires some setting up and knowledge, and is not ideal for last minute field work. Additionally, it should be noted that access points and networks can change, so the maps should be updated.

Ideally, investigators would have access to both. AirMagnet would be preferable to get the big picture of an area they are looking into, and AirCheck could be used once they get to the scene to look at the specific details. Using both would be the best, but not necessary.

AirCheck and AirMagnet are both great tools. Which tool is better for investigators really just depends on what they are trying to do and what they are looking for.

	Network Details	GPS	Logging	Map Plotting	Reporting
AirCheck WiFi Tester	Yes, gives information about specific networks, access points, and devices.	No, but includes antenna to locate access points, networks, and devices.	Yes, automatically saves session and the user's findings.	No, but using the antenna devices can be located and manually plotted on a map.	Yes, included software.
AirMagnet Survey Pro	Yes, gives information about channels and networks that can be filtered to show the details the user wants.	Yes, but user must provide the GPS or the floor plans for an area and manually map it out.	Yes, several different kinds of tests can be run with different logging functions.	Yes, but user must import floor plans or GPS map themselves	Yes, included software.