# Wireless Network Scanning

Contents

[Wireless Network Scanning 1](#_Toc149988964)

[Lab Description 1](#_Toc149988965)

[Android WiFi Scanning WiFiman by Ubiquiti 1](#_Toc149988966)

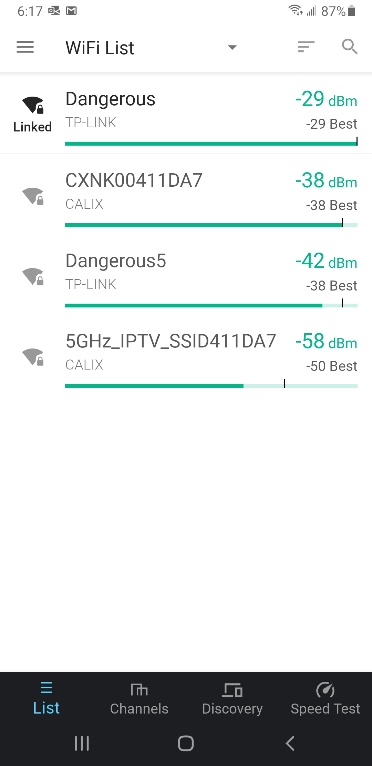
[Airport Utility for iOS 2](#_Toc149988967)

[Vistumbler for Windows 5](#_Toc149988968)

[Assignment Submission 7](#_Toc149988969)

Time required: 60 minutes

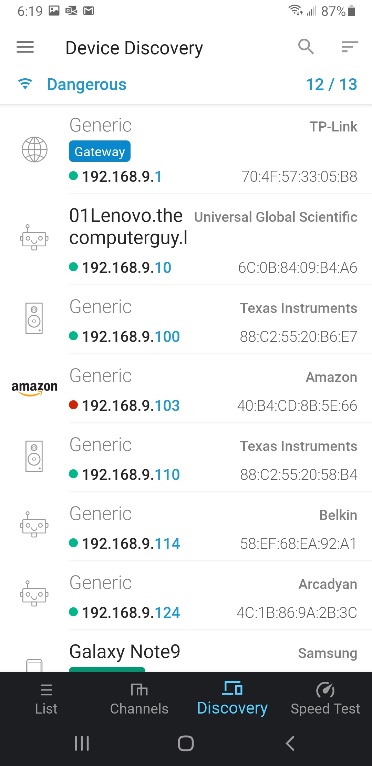
## Lab Description

Most Wi-Fi users are surprised to see just how far their wireless signal will reach, and if the network is unprotected this makes it easy for an attacker hiding several hundred feet away to break into the network. There are several tools available that will show the different wireless signals from Wi-Fi networks that can be detected.

# Android WiFi Scanning WiFiman by Ubiquiti

**NOTE:** Do this lab if you have an Android device.

WiFiman by Ubiquiti is available and Android devices.

1. Install the app and open it.
2. The app will automatically start scanning for Wi-fi signals. The screenshot below gives an example of what you should see.
3. Explore the features of the app.
4. Research how to take a screenshot on your smartphone or tablet. Replace the screenshots in this document with a screenshot of the channel graph and the AP list.
5. Insert a screenshot of the networks in your area using the settings of the sample screenshots.

Click or tap here to enter text.

1. What channel is your network programmed to?

Click or tap here to enter text.

1. What security is your network programmed to?

Click or tap here to enter text.

1. What is the signal strength of your network?

Click or tap here to enter text.

1. If your network is on the same channel as other networks, find a channel 1, 6, or 11 that isn’t as crowded. Change your Wi-fi channel on your wireless router if possible.
2. Please describe what you found on this step?

Click or tap here to enter text.

# A screenshot of a phone Description automatically generatedAirport Utility for iOS

**NOTE:** Do this lab if you have an iOS device.

1. Download the Apple [AirPort Utility](https://itunes.apple.com/us/app/airport-utility/id427276530?mt=8) from iPhone/iPad app store.
2. Navigate to **Settings** > **AirPort Utility** > **Turn on “Wi-Fi Scanner” mode**
3. A screenshot of a phone

   Description automatically generatedLaunch AirPort Utility app and top right will show **“Wi-Fi Scan”** option in blue.
4. Select scan duration from 10 to 60 seconds or continuous scanning.

A white screen shot of a phone

Description automatically generated

A screenshot of a phone

Description automatically generated

1. Scanning Mode should look similar to this...
2. Insert a screenshot.

Click or tap here to enter text.

1. What channel is your network programmed to?

Click or tap here to enter text.

1. What security is your network programmed to?

Click or tap here to enter text.

1. What is the signal strength of your network?

Click or tap here to enter text.

A screenshot of a phone

Description automatically generated

1. Click a row to view signal history for BSSID/access point.
2. Insert a screenshot.

Click or tap here to enter text.

1. A screenshot of a phone

   Description automatically generatedChannel usage summary can be viewed by clicking “i”/info button on bottom right after stopping scan.
2. Insert a screenshot.

Click or tap here to enter text.

# Vistumbler for Windows

**NOTE:** Vistumbler must be installed on a physical machine with a wireless card. For students on the Scottsbluff campus, there is a computer in the back of the room that has a wireless card.

Vistumbler is wireless network scanner written in AutoIT for Windows. The main purpose of vistumbler is to map and visualize the access points around you.

Vistumbler can be used to display the security information that is beaconed out from WLANs. Note that Vistumbler does not allow you to “crack” any WLANs but instead only displays information. In this project, you use Vistumbler to view this information. This project works best when you are in an area in which you can pick up multiple WLAN signals.

1. Use your web browser to go to [www.vistumbler.net](http://www.vistumbler.net) (The location of content on the Internet may change without warning. If you are no longer able to access the program through this URL, use a search engine and search for “Vistumbler.”)
2. Click eXe Installer (Mirror).
3. You may receive a warning. Choose run anyway.
4. Follow the prompts to download and install Vistumbler using the default settings.
5. If the program does not start after the installation is complete 🡪 Go to start 🡪 type in Vistumbler. If necessary, expand the window to full screen.
6. Click Scan APs. If no networks appear, click Interface and then select the appropriate wireless NIC interface.
7. Note the columns Signal and High Signal.
8. Insert a screenshot.

Click or tap here to enter text.

1. How could they be used in a site survey?

Click or tap here to enter text.

1. Click Graph 1.
2. Click one of the APs displayed at the bottom of the screen. Allow Vistumbler to accumulate data over several minutes.
3. What information is displayed on this graph?

Click or tap here to enter text.

1. Click Graph 2.
2. Click another one of the APs displayed at the bottom of the screen. Allow Vistumbler to accumulate data over several minutes.
3. What information is displayed on this graph?

Click or tap here to enter text.

1. How is this different from the previous graph?

Click or tap here to enter text.

1. Click No Graph to return to the previous screen.
2. Use the horizontal scroll bar to move to the right. Note the columns Authentication, encryption, Manufacturer, and radio Type.
3. How would this information be useful to an attacker?

Click or tap here to enter text.

1. Use the horizontal scroll bar to move back to the far left.
2. In the left pane, expand the information under Authentication.
3. What types are listed?

Click or tap here to enter text.

1. Expand the information under these types and note the information given for the wireless LAN signals.
2. In the left pane, expand the information under encryption.
3. Insert a screenshot

Click or tap here to enter text.

1. Which types are most secure?

Click or tap here to enter text.

1. Which types are least secure?
2. Click or tap here to enter text.
3. Expand the information under these types and note the information given for each WLAN.
4. Insert screenshot.

Click or tap here to enter text.

1. One of the features of Vistumbler is its ability to use audio and text-to-speech information so that the location and strength of WLANs can be detected without the need to constantly monitor the screen. Be sure that the speakers on the laptop computer are turned on.
2. Click **Options** 🡪 Click **Speak Signals**. Vistumbler will “speak” the percentage of signal strength.
3. Carry the laptop away from the AP and note the changes.
4. How would this be helpful to an attacker?

Click or tap here to enter text.

1. Close Vistumbler.

## Assignment Submission

Attach this completed document to the assignment in Blackboard.