Experiment No 9

Title: To study security in wireless devices using netstumbler

Objective: To study wireless security

Expected Outcome of Experiment:

CO	Outcome
3	Ability to decide issues and concerns on security and privacy

Prerequisite: Networking

Books/ Journals/ Websites referred:

[1] http://www.techrepublic.com/article/using-netstumbler-and-ministumbler-to-find-rogue-access-points-on-wireless-networks/

[2] http://www.netstumbler.com/downloads/

[3] http://www.smallbusinesscomputing.com/webmaster/article.php/3590656/How-to-Track-Down-Rogue-Wireless-Access-Points.htm

[4] https://en.wikipedia.org/wiki/NetStumbler

Theory/Abstract:

NetStumbler (also known as **Network Stumbler**) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. It runs on Microsoft Windows operating systems from Windows 2000 to Windows XP.

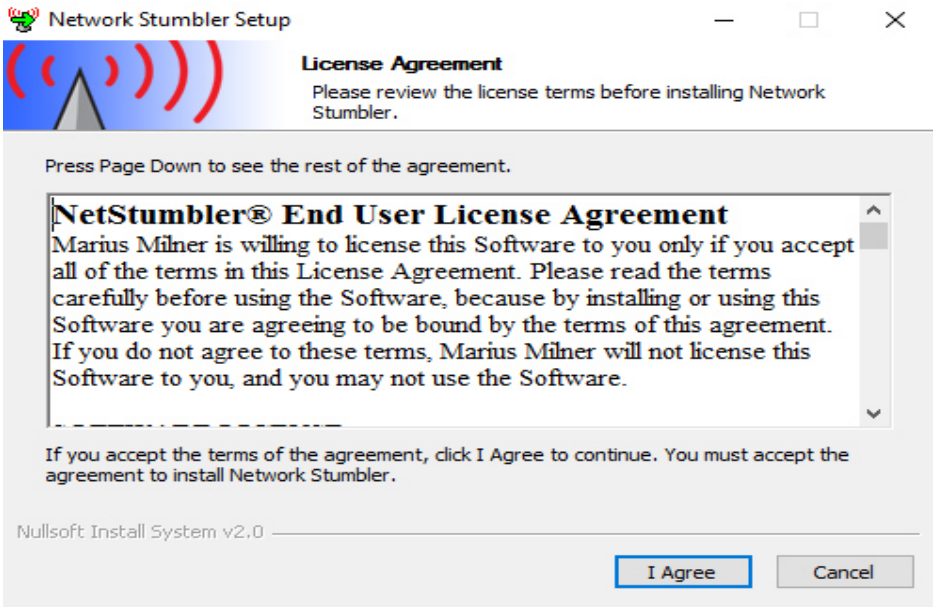
The program is commonly used for:

- Wardriving
- Verifying network configurations
- Finding locations with poor coverage in a WLAN
- Detecting causes of wireless interference
- Detecting unauthorized ("rogue") access points
- Aiming directional antennas for long-haul WLAN links

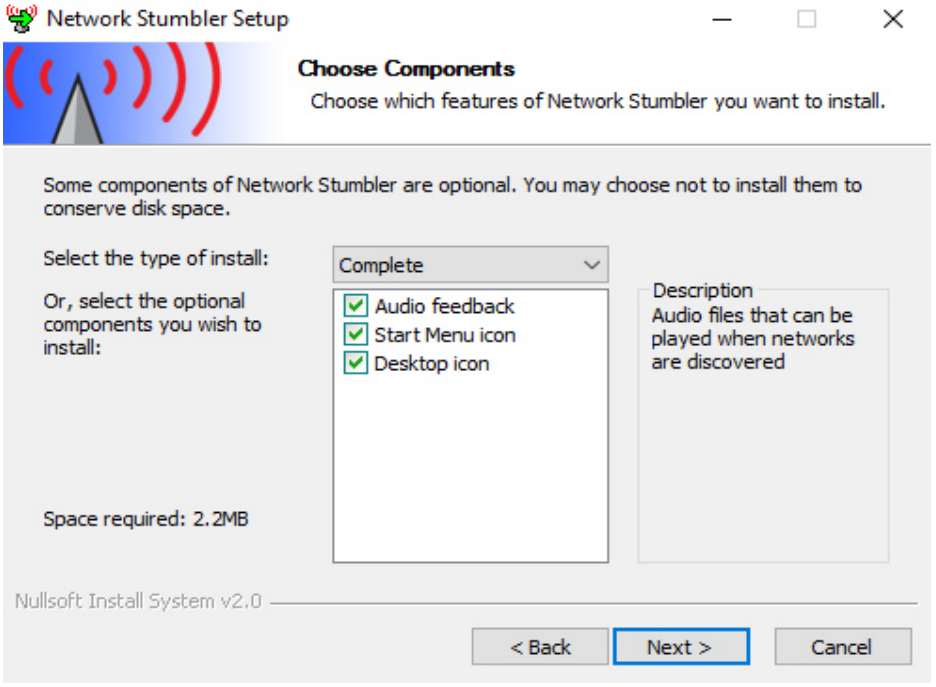
A rogue AP is a Wi-Fi Access Point that is set up by an attacker for the purpose of sniffing wireless network traffic in an effort to gain unauthorized access to your network.

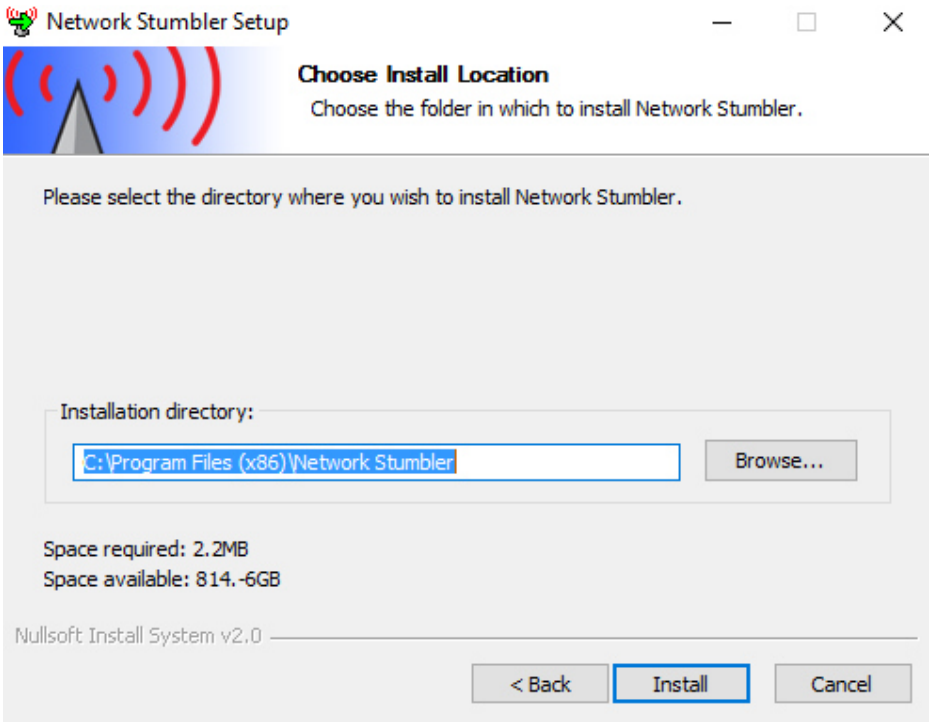
1. **Installation of netstumbler steps.**

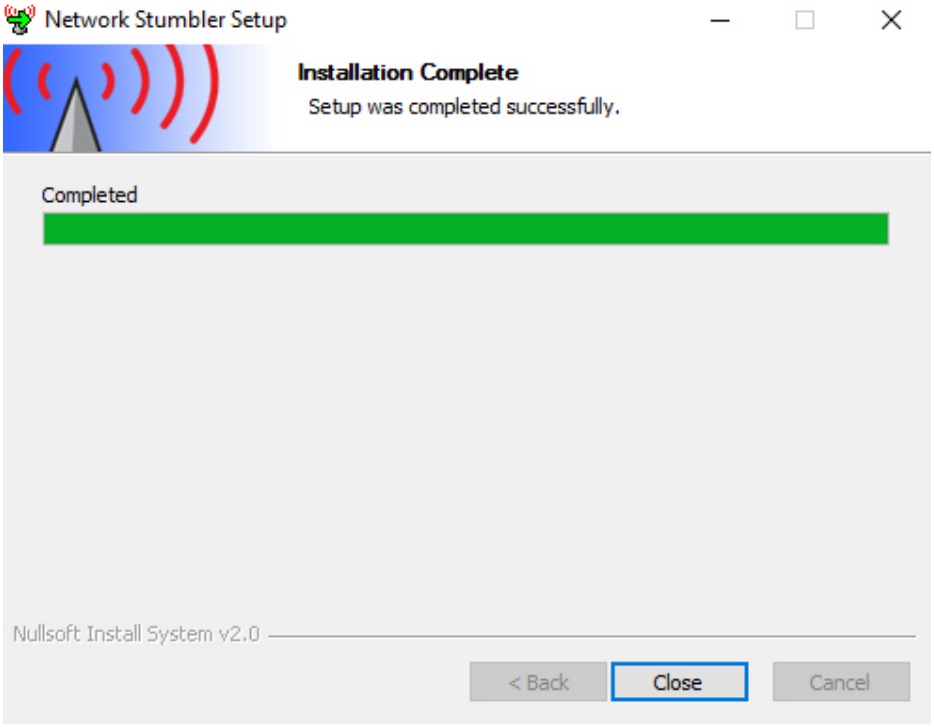
Downloading the .exe file and running it:



Installation wizard:



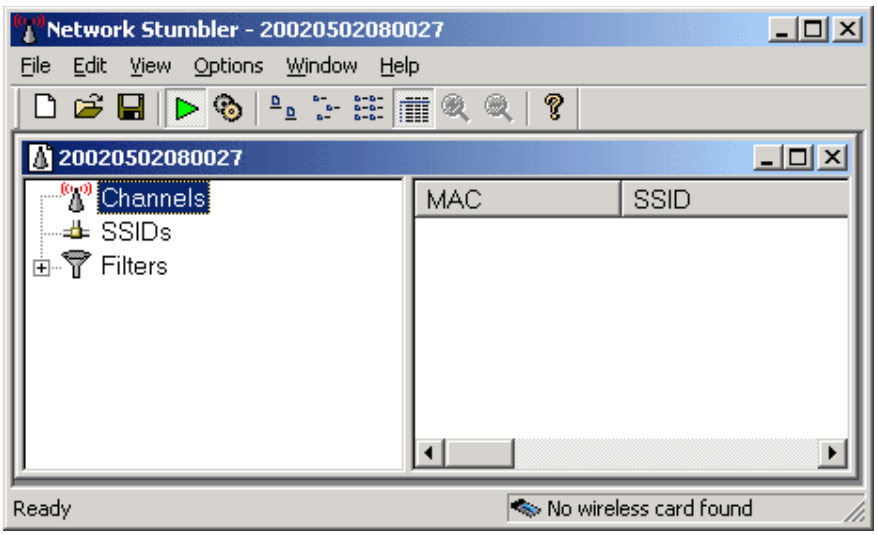

Network Stumbler Setup
Choose Install Location
Choose the folder in which to install Network Stumbler.
Please select the directory where you wish to install Network Stumbler.
Installation directory:
C:\Program Files (x86)\Network Stumbler
Browse...
Space required: 2.2MB
Space available: 814.-6GB
Nullsoft Install System v2.0
< Back
Install
Cancel


Network Stumbler Setup
Installation Complete
Setup was completed successfully.
Completed
Nullsoft Install System v2.0
< Back
Close
Cancel

2. **Checking vulnerability of wireless system.**

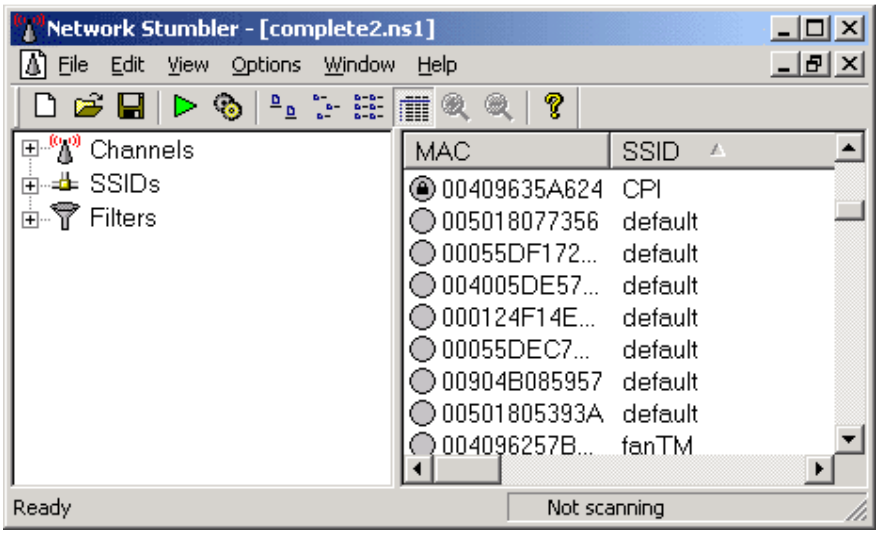
NetStumbler screen immediately after startup:

NetStumbler starts up ready to scan



After scanning:

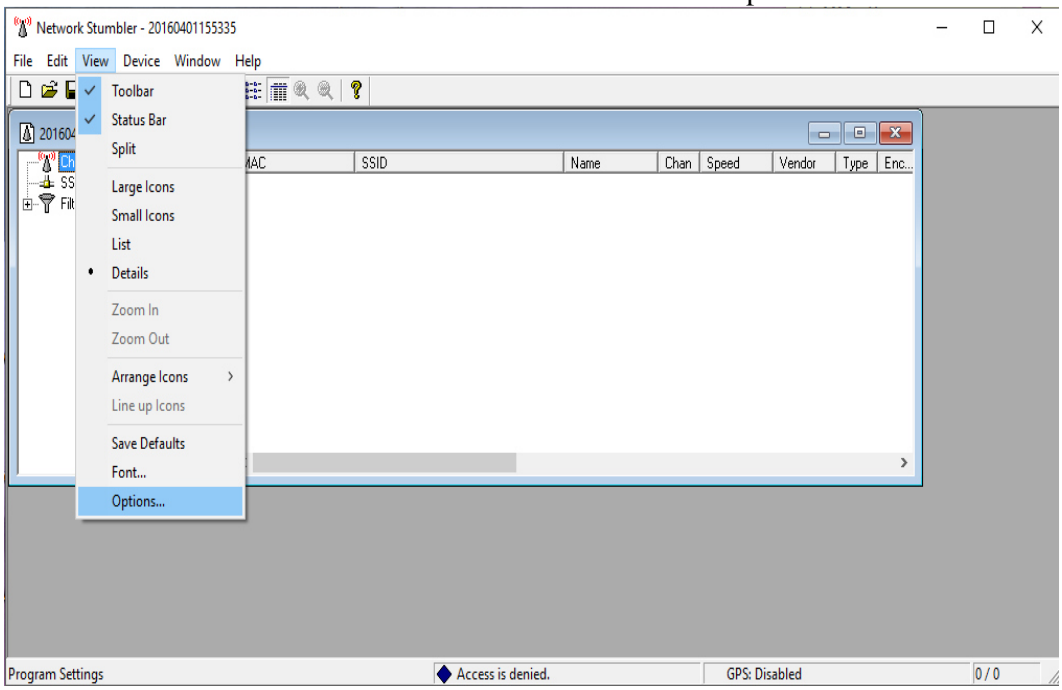
list of access points and their locations



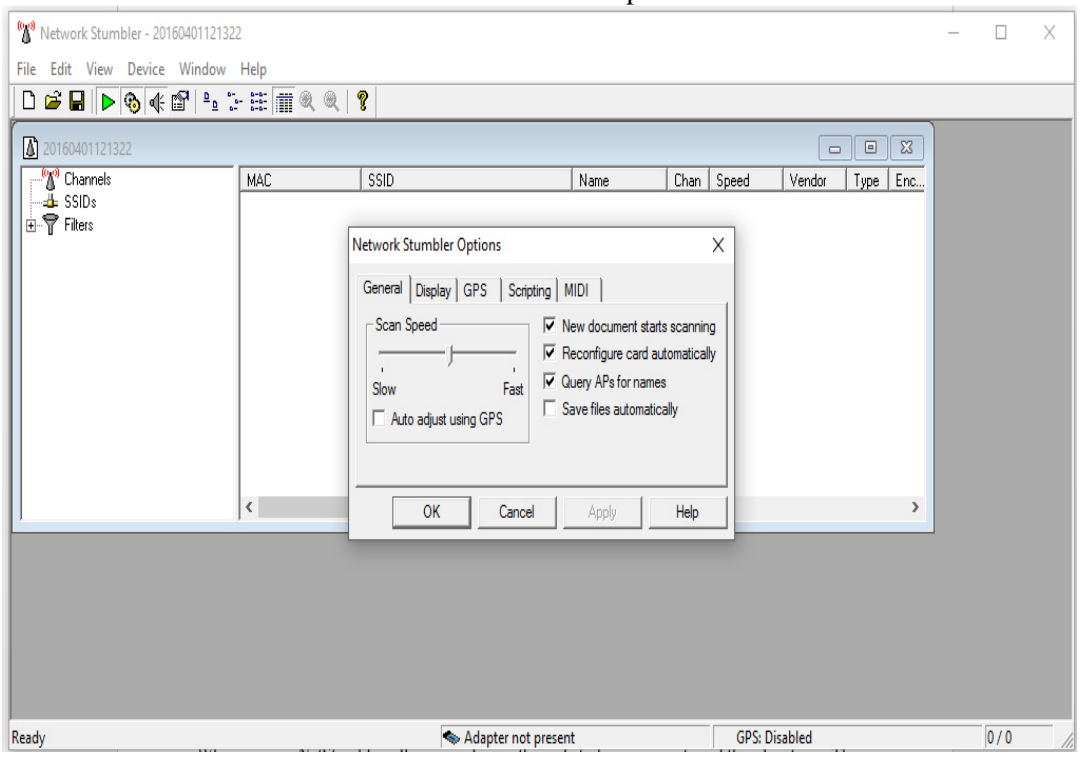
Saving sessions

Before you shut down NetStumbler, you should save the session with the Save command on the file menu. Or, if you prefer, you can autosave the file by selecting the Options menu and then selecting AutoSave. A check mark will appear to the left of the entry when it's selected.

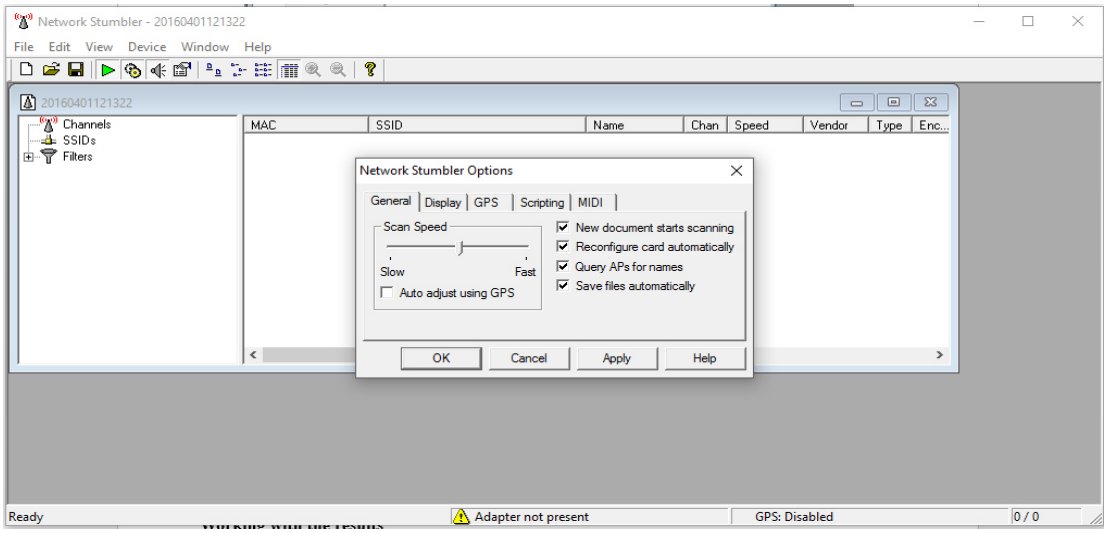
To set autosave mode-Go to view select options



Network Stumbler options



In Network Stumbler options tick the respective check box(i.e Save files automatically)



You can merge existing files data into the current file by selecting File and then Merge.

Working with the results

When you run NetStumbler, all you wind up with is a list of access points and their locations. Those access points have to be mapped. Start by making sure you've merged all of your NetStumbler files together into one large file, as described above.

The **next step** is to convert the data in NetStumbler into a format that you can map. The conversion process takes two steps. The first is to export the data from NetStumbler by selecting File | Export | Summary and save the export file to your system. Next, connect to the NetStumbler Web site and select the option for MapPoint Converter. This brings you to a Web page that translates the summary file into a series of rows that you can then use to create a map using Microsoft MapPoint.

You must first copy the results of the script into an Excel workbook. Once you've saved the Excel workbook, you can import the data into MapPoint. The results may look something like the figure given below:

NetStumbler is a great tool for finding rogue access points, and for determining how far away your access points can be detected. After you find the rogue points on your network, you can determine a course of action.

Conclusion: Thus we have studied netstumbler.