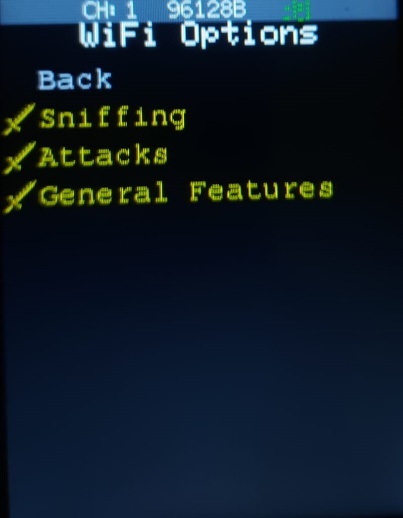
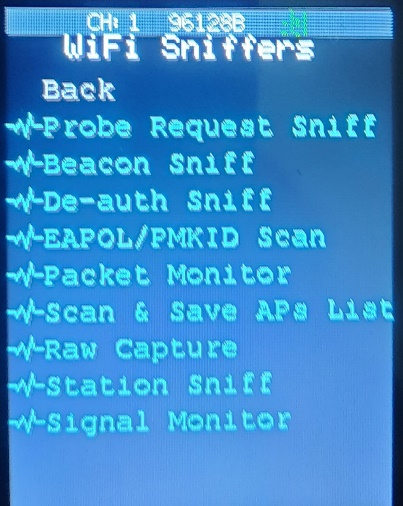
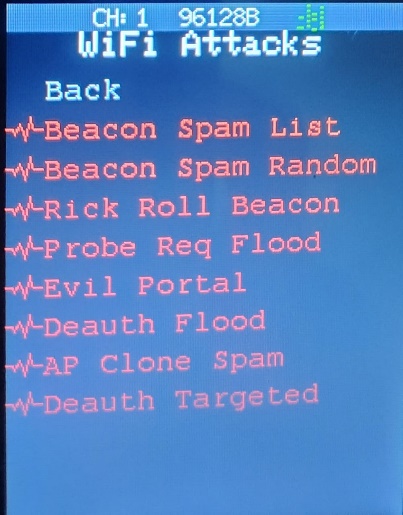
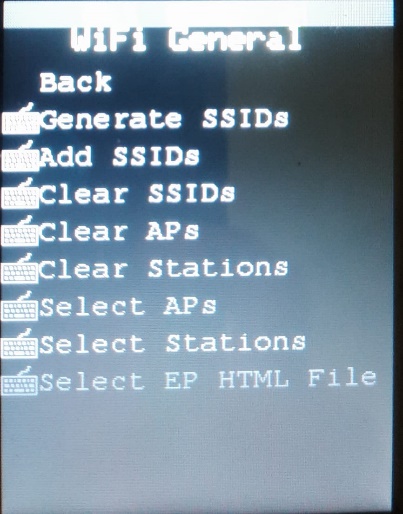
Here is the basic information about the window lets go through one by one.

**Wi-fi Options**

Wi-fi Sniffing (Silently Listening)

* Probe Request Sniffer

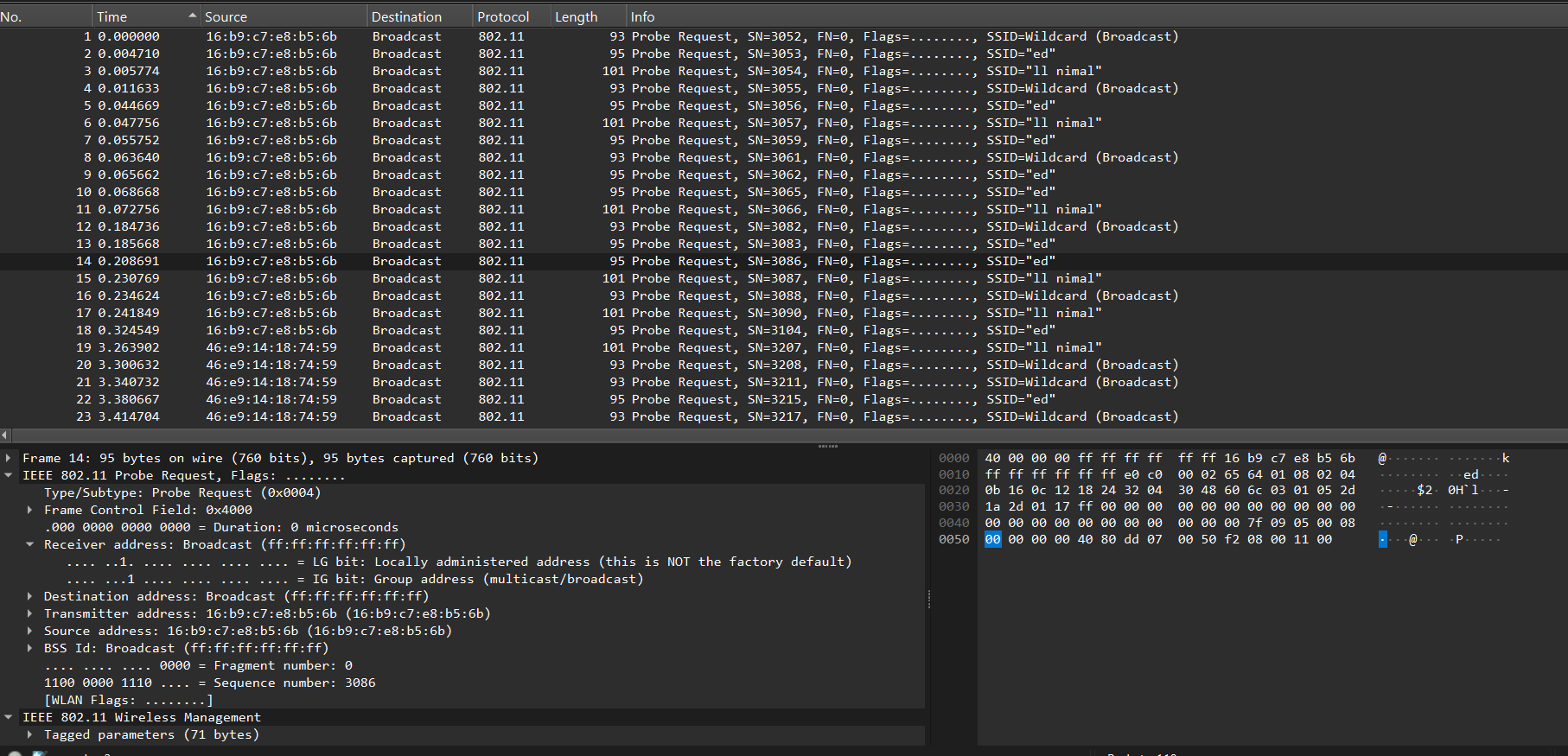
Check for probe request, when a wi-fi device is basically pining other devices looking for nearby SSID. It will show up down as a list of mac address. It is going to show any nearby sell phones (looking for AP) If the cell phone is idle, it requests hundreds of probe request for an hour. Determine which wi-fi devices are in any given area.

* Beacon Sniffer

Sniffing out wi-fi AP nearby only.

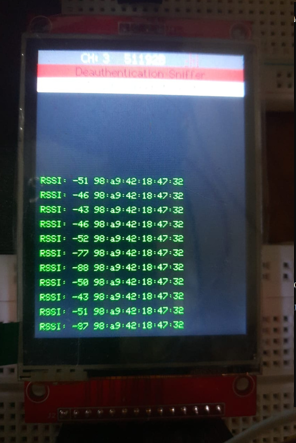
* Scan and Save Aps List

Save the APs nearby to analyze.

*Wireshark analysis on beacon Sniffing:*

* De-auth Sniffer

Searching for the DE authentication packets. If some one is going to attack we can observe the kick off device (AP) from this (ex: router)

*Demonstration of how it uses:*

1. Offensive Mode.

The first screenshot demonstrates a DE authentication Attack being sent to the target access point: Dialog 4G 842. The attack parameters were configured through the PEN Tool's touchscreen interface.

1. Defensive Monitoring

The second screenshot shows real-time monitoring of the targeted AP's MAC address and RSSI using the PEN Tool. This operation is performed ethically within an authorized testing area.

1. Validation of Attack

The third image confirms that devices connected to the targeted AP were successfully identified using the ARP table on a terminal. During the DE-auth attack, these connected clients were disconnected (kicked off) as expected.

Attacker can get the snip handshake when the device tries to reconnect and attacker can do MIM attacks during that time. (logins, credentials, bank details, etc.)

* EAPOL/PMKID Scan

Search for specific packet sent over wi-fi

Extensive Authentication Protocol over Lan (Four-way handshake packets device uses to authenticate credentials with the access point) Devices uses to authenticate credentials with an AP we used those earlier again to crack through hashcat

PMKID- Pairwise Master Key Identifier (Similar to the handshake packets but only one of them and it doesn’t require the device to be de-authenticated and re-authenticated. This way hacker can get the only one file and use that to grab the hash over the Wi-fi network. (Hash- simply a string of data that’s converted to another type. Typically, Encryptions). Then we can save them into the SD card.

EAPOL ss here….

* Raw Capture

Showing around me MACs with RSSI resulting how strong the receiving signal strength.

* Station Sniffer

First select an specific AP (Wi-fi general 🡪 Select AP) through saving the AP in the Save AP option. So it sniff out any device that is attach to that chosen AP. (Popping a list)

Offensive attack: We can give a targeted de-auth attack directly. More over evil twin attack through sending de-auths.

* Signal Monitor

Need to connect to a directly to a network and it shows the signal strength for that network.

Wi-Fi Attacks

* Beacon Spam List

Spam any Aps and SSIDs that are in in our saved list. Add a AP using the (General🡪Add AP)

\*Our own AP is in the Network

* Beacon Spam Random

Create many numbers of APs and send it to the Network. Really annoying thing.

* Rick Roll Beacon

Sends out the Rick Astley’s classic song as SSID phrases.

* Probe Request Flood

Send Probe request to AP over and over in a rapid rate. Can jam the access point. Devices in the network can’t be connected to that AP.

* De-auth Flood

Send the de-authentication packets to the all AP in the network. Just like the demonstration in the above.

* AP Clone Spam

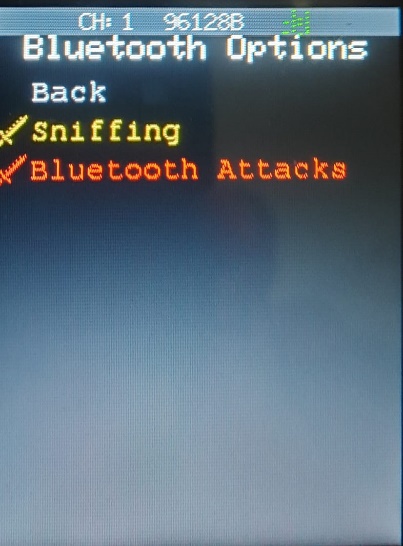
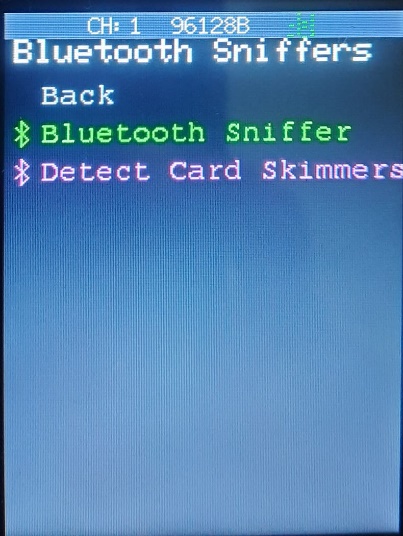
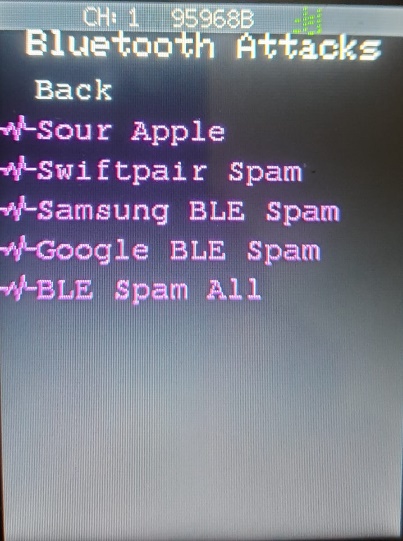
Send out cloned SSIDs for any ither access point n the list.

* Deuth Targeted

First, Select Stations (AP and others devises that are on attached to our network). When running this by selecting one of station (MAC) it will attack on the network and try to de-authenticate just one device. De-off one device.

Wi-fi General

Normal Functionalities are there. (Add Generate, Clear SSIDs, Select APs, Stations)

**Bluetooth Options**

Sniffing

* Bluetooth Sniffers

Sniffing out the Bluetooth signal devices.

* Detect card Skimmers

Detect the credit card skimmers that people are installing on credit card or ATM readers. (Supermarkets)

Bluetooth Attacks

* Sour Apple

Spoofs BLE advertisements that Apple devices. Broadcasts fake BLE advertisements imitating peripherals

* Swift Pair Spam

Continuously sends BLE advertisements mimicking devices ready to pair. Target: Windows 10 and 11 systems. Windows shows popups like “Tap to connect” over and over. This is designed to be annoying or distracting rather than fully exploitative.

* Samsung BLE Spam

Samsung Android devices are targeted. Spoofs BLE devices that Samsung phones will attempt to auto-recognize or interact with. Impact is the Samsung phones may auto-launch Bluetooth dialogs or notifications. This can be sued to Testing BLE advertisement parsing behavior in Samsung's OneUI/Android BLE stack.

* BLE Spam

Any BLE-capable device. This broadcast randomized or custom BLE advertisements repeatedly.

Crowded the BLE space by sends multiple fake BLE packets that advertise fake devices.

* BLE Spam All

Universal — All BLE-capable devices. A combo mode that runs all the above attacks together. To simulates BLE DoS or stress test scenario.