Wi-Fi Signals Intelligence

Basic SIGINT for fun and forensics

What is SIGINT?

In intelligence collection, SIGINT is the analysis of radio signals to derive intelligence. It is related to COMINT (interception of communications) and ELINT (electronic signals intelligence)

Signals intelligence can apply to technologies used in consumer devices, such as Wi-Fi, Bluetooth, LoRa, Zigbee, and cellular signals.

Even beginners can use signals intelligence to learn technical information about hardware, software, and the live presence of devices attributed to people.

Why should you know basic Wi-Fi SIGINT?

- You can identify the presence and manufacturer of Wi-Fi devices like computers, IoT devices, printers, security cameras, routers, gaming systems, smart adult toys, police body cameras, smart weapon holsters, or known vulnerable types of hardware.
- You can identify and track individual devices, monitor their movements, and discover what Wi-Fi networks they have connected to before.
- You can see what websites any device is visiting on a network that is open or you know the password to.
- You can protect yourself from your electronic devices giving away your presence or being tracked

Tools for Signals Intelligence

Software:

Wigle Wi-Fi (web based and Android, free)

Kismet (Linux and MacOS, free)

Wireshark (Cross platform, free)

Hardware:

Wireless Network Adapters ($15-$60)

ESP8266 Microcontroller ($3)

Use Case: Locate & Classify Wi-Fi Devices in Area

For a site survey of all devices, you can locate every fixed device (IoT devices, routers, cameras) and any mobile devices in an area.

Useful for detecting the presence of a Wi-Fi device like a laptop smartphone attached to a high value person.

Capable of identifying the security and precise geographic location of each device from a single drive by or walk through of an area.

Prove a person or device was at a place or identify which devices have permission to connect to which networks (who knows who)

Use Case: Track a Specific Device

Once you identify a device of interest, you can detect it any time it is in range.

Useful for staking out a location - Leave a device that can record the comings and goings of Wi-Fi devices to learn when an individual is home.

Useful for proving someone was present or is present at a location

With a directional antenna, you can receive a signal from a Wi-Fi device being tracked for over 2 miles

Use Case: Find Networks a Device Has Joined

Identify which Wi-Fi networks a device has joined before and stored in their Preferred Network List.

Useful for identifying employees of a company or government agency

By creating many fake Wi-Fi networks with the names target organizations use for their employee-only networks and listening for the replies, we can identify which fake networks nearby smartphones recognize and are trying to join

We can prove a person has connected to a Wi-Fi network at a place they deny going to, learn about where they have been, and unmask employees of sensitive organizations

Use Case: Monitor Websites Visited on Wi-Fi

If you know the password or the network is open, Wireshark can show all websites a person is accessing (including mobile applications on smartphones) in real time

Useful for seeing what websites a person uses frequently, what applications are installed on a smartphone, and what browser someone is using

For websites not using TLS (HTTPS), you can see the contents of the communications (passwords, full websites loaded, forum submissions)

This doesn’t work if the person uses a VPN, as all communication will be encrypted