ChatGPT

Repository structure:

```
WiFi_Sniffing_Project/
├── README.md
└── project_report.pdf
```

README.md:

Wi-Fi Sniffing

Wi-Fi sniffing (packet sniffing) involves capturing and analyzing wireless network traffic to monitor activity and find vulnerabilities [1] [2]. This project explores how to use packet-capture tools to inspect 802.11 Wi-Fi packets, identify sensitive data flows, and improve network security. It demonstrates practical steps to capture Wi-Fi traffic (e.g. with Wireshark), analyze contents, and apply countermeasures against eavesdropping.

Objectives

- Understand the concept of Wi-Fi packet capturing and analysis.
- Explore common Wi-Fi sniffing tools used in cybersecurity.
- Identify threats and security breaches enabled by wireless sniffing.
- Learn and implement preventive measures to secure Wi-Fi networks.

Tools Used

- **Wireshark** – a free, open-source packet analyzer used to capture and inspect network traffic [2]. It supports both wired and wireless interfaces, showing detailed packet contents.
- **Aircrack-ng** – a suite of wireless security tools for auditing Wi-Fi networks. It can capture 802.11 handshakes and crack WEP/WPA/WPA2 keys [3]. Aircrack-ng is often used to test network encryption robustness.
- **Kismet** – an open-source wireless network detector and packet sniffer. Kismet passively discovers hidden networks and logs all wireless traffic across channels. It can reveal SSIDs, encryption types, and packet details without associating to an access point.
- **Tcpdump** – a command-line network packet analyzer. Tcpdump captures and displays TCP/IP and other packets on a network interface [4]. It is useful for quick captures and scripting.

Implementation Steps

1. **Setup tools:** Install Wireshark and enable packet capture privileges on your system.
2. **Enable monitor mode:** Put your wireless adapter into monitor (promiscuous) mode so it can capture all Wi-Fi packets. For example, on Linux use `airmon-ng` (from Aircrack-ng) to create a mon0 interface.

3. **Start packet capture:** Launch Wireshark and select the monitor-mode wireless interface. Begin capturing on the target Wi-Fi channel. (In Wireshark: *Capture* → select interface → *Start* [5].)
4. **Capture traffic:** Let Wireshark collect packets. Optionally, use Aircrack-ng's `airodump-ng` to capture WPA2 handshakes for later analysis.
5. **Analyze packets:** Use Wireshark's filters to inspect the data. Look for unencrypted traffic, login credentials, or patterns of interest. Wireshark displays packet fields (headers and payload) to reveal contents [5].
6. **Document findings:** Note any sensitive information (e.g. HTTP credentials) found. Propose security improvements such as stronger encryption or network segmentation.

   Example: Wireshark acts like a "magnifying glass for packets" showing exactly what's traveling over the network [6]. By selecting a capture interface and pressing the capture button, Wireshark will display live packet data [5]. Aircrack-ng can also be used in parallel to capture packets and test encryption keys [3].

Risks and Countermeasures

- **Eavesdropping Risk:** Wireless packets are broadcast in the open, so an attacker within range can capture unencrypted data (web pages, emails, passwords) using sniffing tools [7]. This can lead to credential theft or session hijacking.
- **Rogue Access Points/Evil Twins:** Attackers may set up fake Wi-Fi hotspots to lure users, intercepting all data.

Countermeasures:
- **Strong Encryption:** Use WPA3 (or WPA2 with AES) to encrypt Wi-Fi traffic. Strong encryption makes sniffed packets unreadable without the key [8] [9]. Avoid outdated protocols like WEP or TKIP.
- **Avoid Untrusted Wi-Fi:** Do not use public or unsecured Wi-Fi networks for sensitive activities [10]. If public Wi-Fi must be used, assume the network is being monitored.
- **Use VPNs:** A Virtual Private Network encrypts all traffic, so intercepted packets reveal only gibberish [11]. This protects data even on insecure networks.
- **Network Monitoring:** Deploy wireless intrusion detection (WIDS) and regularly audit traffic for anomalies [9]. Monitoring wireless traffic helps spot unknown devices or unusual patterns.
- **Secure Configuration:** Change default router credentials, disable WPS, and segment guest Wi-Fi from corporate LAN. Regular firmware updates and strong passwords reduce risk.

Conclusion and Future Scope

Wi-Fi sniffing is a **dual-purpose** technique in cybersecurity. Ethically used, it helps administrators **monitor network health and detect vulnerabilities**. Illicitly used, it can compromise privacy and security. As wireless networks become ubiquitous, tools like Wireshark and Aircrack-ng remain vital for security assessments [6] [3].

Looking forward, **AI-driven analysis** is emerging. Next-generation sniffing tools leverage machine learning to automatically identify malicious traffic patterns and anomalies [12] [13]. For example, AI models can flag irregular packet behaviors (odd sizes, patterns) without human oversight. This promises faster intrusion detection and smarter wireless defenses.

Future work may involve integrating AI-based anomaly detection into sniffing workflows, and expanding testing to newer Wi-Fi standards (e.g. Wi-Fi 6/6E) and IoT protocols.

Credits

This project report was submitted by **Kapil Patil** (October 2025).

project_report.pdf:
(Original project report by Kapil Patil – Wi-Fi Sniffing, October 2025).

---

[1] What is a Packet Sniffer?
https://usa.kaspersky.com/resource-center/definitions/what-is-a-packet-sniffer

[2] Wireshark - Wikipedia
https://en.wikipedia.org/wiki/Wireshark

[3] [6] What is Wireless Penetration Testing?
https://prescientsecurity.com/blogs/what-is-wireless-penetration-testing

[4] tcpdump - Wikipedia
https://en.wikipedia.org/wiki/Tcpdump

[5] Wireshark Basics | Cycle.io
https://cycle.io/learn/wireshark-basics

[7] What is Packet Sniffing? Types, Examples, and Best Practices
https://www.knowledgehut.com/blog/security/packet-sniffing

[8] [9] [11] What are the risks of wireless networks in intranet security? - Tencent Cloud
https://www.tencentcloud.com/techpedia/118683

[10] 5 essential tips for using public Wi-Fi securely | Verizon
https://www.verizon.com/home/internet/guides/5-essential-tips-for-using-public-wi-fi-securely/

[12] Network Analysis & AI-Powered Packet Tools | Wireshark.com
https://wireshark.com/

[13] Leveraging AI for Network Threat Detection—A Conceptual Overview
https://www.mdpi.com/2079-9292/13/23/4611