LINKEDIN POST

The Wireshark Wi-Fi Wiki, a Reference Worth Bookmarking

By **Keith Parsons, CWNE #3** · 2026-09-18 · originally on LinkedIn

I have been looking things up in the Wireshark Wi-Fi wiki, on and off, for more than twenty years.

I have never read it.

That is not a complaint. It is the highest compliment you can pay a reference. Nobody reads a dictionary. You go to it with a question, you get your answer, you close it. Twenty years of that adds up to a lot of answers.

So when a student asks me for the display filter that isolates management frames, or how to get an adapter into monitor mode on their particular laptop, or why their decryption is not working, I usually do not type out the answer. I send them there to go find it.

The Wi-Fi page explains how 802.11 frames look in a capture, rather than the fake Ethernet view most tools hand you, and it documents the display filter syntax from the source. wlan.addr, wlan.fc.type, eapol, with worked examples.

The CaptureSetup/WLAN page covers monitor mode across Windows, macOS, Linux and the BSDs.

The HowToDecrypt802.11 page spells out what decryption needs, including the passphrase:SSID format and the requirement that you capture all four handshake packets.

Parts of that wiki are old. The concepts are right and the filter and decryption reference is solid. Some of the per operating system capture instructions are a decade or more out of date. Trust the syntax completely. Verify the platform steps against whatever you are running today.

It is free. No login, no paywall, no vendor spin. It belongs to the Wireshark project and it is licensed GPLv2.

What is the one reference you keep going back to that you have never actually read front to back?

By Keith Parsons, CWNE #3, Wireless LAN Professionals. Free to read and share. Facts