Sources utilized to conduct static and dynamic analysis of Wi-Fi router firmware.

1. Learning's
    a. https://book.hacktricks.xyz/hardware-physical-access/firmware-analysis
    b. https://github.com/secjey/static-firmware-analysis
    c. https://ravi73079.medium.com/unveiling-vulnerabilities-a-deep-dive-into-firmware-penetration-testing-part-1-904599cd79be
    d. https://prabhankar.medium.com/firmware-analysis-part-1-cd43a1ad3f38
    e. https://github.com/attify/firmware-analysis-toolkit
2. TENDA
    a. https://boschko.ca/tenda_ac1200_router/
    b. https://www.youtube.com/watch?v=NCjdctjMtsI
    c. https://www.tendacn.com/download/detail-3762.html
    d. https://www.opencve.io/cve/CVE-2022-42060
    e. https://www.opencve.io/cve/CVE-2022-42058
3. ASUS
    a. https://gitbook.seguranca-informatica.pt/arm/reverse-iot-devices/reverse-asus-rt-ac5300
    b. https://www.zerodayinitiative.com/blog/2020/5/27/mindshare-how-to-just-emulate-it-with-qemu
    c. https://medium.com/@cq674350529/analyzing-the-vulnerability-in-asus-router-maybe-from-tfc2021-51dcc08b2911
    d. https://nvd.nist.gov/vuln/detail/CVE-2018-1160
4. APPLE
    a. https://wikileaks.org/ciav7p1/cms/page_21561396.html
    b. https://www.cvedetails.com/cve/CVE-2010-0962/
    c. https://support.apple.com/en-ca/103996