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://medium.com/@attify/firmware-analysis-for-iot-devices-fb8df961c19d

    d. https://roman1.gitbook.io/blog/embedded-device-exploitation/introduction-to-firmware-analysis

    e. https://interrupt.memfault.com/blog/static-analysis-with-codechecker

2. NETGEAR
    a. https://www.securityweek.com/netgear-routers-plagued-serious-vulnerabilities/

    b. https://kb.netgear.com/30560/CVE-2015-8288-Use-of-Hard-coded-Cryptographic-Key

    c. https://www.ispreview.co.uk/index.php/2020/03/security-vulnerabilities-strike-50-models-of-netgear-routers.html

    d. https://www.opencve.io/cve/CVE-2016-11059

    e. https://kb.netgear.com/000061982/Security-Advisory-for-Multiple-Vulnerabilities-on-Some-Routers-Mobile-Routers-Modems-Gateways-and-Extenders

3. D-LINK
    a. https://www.greynoise.io/blog/debugging-d-link-emulating-firmware-and-hacking-hardware

    b. https://www.youtube.com/watch?v=0KLd29xC9XQ&t=7s

    c. https://www.opencve.io/cve/CVE-2019-20213

    d. https://www.opencve.io/cve/CVE-2019-17621