ELEKTRO IN RAČUNALNIŠKA ŠOLA VELENJE

TRG MLADOSTI 3, 3320 VELENJE

MLADI RAZISKOVALCI ZA RAZVOJ SAŠA REGIJE

RAZISKOVALNA NALOGA

VARNOST IN RANLJIVOST BREZŽIČNIH OMREŽIJ

Tematsko področje: TELEKOMUNIKACIJE

AVTOR:

Blaž Kristan, 4. TRA

MENTORJA:

Uroš Remenih, inž.

Samo Železnik, inž.

Velenje, 2026

Raziskovalna naloga je bila opravljena na Elektro in računalniški šoli Velenje

Mentorja: Uroš Remenih, inž. inf.

Samo Železnik, inž. inf.

Datum predstavitve: marec 2026

KLJUČNA DOKUMENTACIJSKA INFORMACIJA

ŠD ŠCV, Elektro in računalniška šola, šolsko leto 2025/2026

KG Osnovna zaščita / Šifrirana komunikacija / Ranljivost na napade / Večstopenjska avtentikacija / Odpornost proti napadom

AV KRISTAN, Blaž

SA REMENIH, Uroš / ŽELEZNIK, Samo

KZ 3320 Velenje, SLO, Trg mladosti 3

ZA ŠCV, Elektro in računalniška šola

LI 2026

IN VARNOST IN RANLJIVOST BREZŽIČNIH OMREŽIJ

TD Raziskovalna naloga

OP IX, 29 str., 1 pregl., 20 sl., 19 vir.

IJ SL

JI Sl / En

AI Danes se ljudje vse bolj zanašajo na brezžična omrežja, ki so pogosto tarča napadov in zlorab. Moja raziskovalna naloga se osredotoča na analizo varnosti Wi-Fi sistemov v Velenju, preučevanje njihovih ranljivosti, pogostih napadov ter učinkovitih zaščitnih mehanizmov. Pri raziskavi izvajam varnostne teste in simulacije napadov z namenom odkrivanja pomanjkljivosti v brezžičnih omrežjih. Cilj naloge je izboljšati razumevanje varnostnih tveganj Wi-Fi omrežij ter prispevati k večji kibernetski varnosti v Šaleški dolini.

KEYWORD INFORMATION

ND SCV, School of Electrical and Computer, School Year 2025/2026

CX Basic Protection / Encrypted Communication / Vulnerability to attacks / Multi-Level Authentication / Attack Resistance

AU KRISTAN, Blaž

AA REMENIH, Uroš / ŽELEZNIK, Samo

PP 3320 Velenje, SLO, Trg mladosti 3

PB SCV, School of Electrical Engineering and Computer Science

PY 2026

TI SECURITY AND VULNERABILITIES OF WIRELESS NETWORKS

DT Research Project

NO IX, 29 p., 1 tab., 20 fig., 19 ref.

LA SL

AL Sl / En

AB Today, people increasingly rely on wireless networks, which are often targets of attacks and misuse. My research project focuses on analyzing the security of Wi-Fi systems in Velenje, examining their vulnerabilities, common attack methods, and effective protection mechanisms. As part of the study, I conduct security tests and simulated attacks to identify weaknesses in wireless networks. The objective of this work is to improve the understanding of Wi-Fi security risks and contribute to stronger cybersecurity in the Šalek Valley.

KAZALO VSEBINE

KAZALO TABEL

KAZALO SLIK

SEZNAM OKRAJŠAV, SIMBOLOV IN DRUGIH IZRAZOV

AES (Advanced Encryption Standard) – napredni simetrični šifrirni algoritem, uporabljen v WPA2 in WPA3.

ARP (Address Resolution Protocol) – protokol za pretvorbo IP naslovov v MAC naslove.

BSSID (Basic Service Set Identifier) – fizični naslov (MAC) dostopne točke.

Brute-force attack – napad z grobo silo, pri katerem se preizkušajo vse možne kombinacije gesel.

CRC (Cyclic Redundancy Check) – metoda preverjanja integritete podatkov.

Cracking – postopek razbijanja gesel ali šifrirnih ključev.

Dictionary attack – napad z uporabo seznama pogostih gesel (wordlist).

Downgrade attack – napad, ki prisili uporabo starejšega, šibkejšega varnostnega protokola.

EAP (Extensible Authentication Protocol) – protokol za avtentikacijo uporabnikov v Enterprise omrežjih.

FTP (File Transfer Protocol) – protokol za prenos datotek med napravami.

GHz – enota frekvence; označuje frekvenčni pas Wi-Fi omrežja.

GPU – grafični procesor za pospeševanje izračunov (npr. razbijanje gesel).

Handshake – začetni postopek avtentikacije med napravo in dostopno točko.

Hash – kriptografska zgoščena vrednost, ki predstavlja pretvorbo podatkov.

IEEE (Institute of Electrical and Electronics Engineers) – organizacija, ki razvija standarde.

Injection (packet injection) – vbrizgavanje paketov v omrežje za ustvarjanje ali manipulacijo prometa.

IV (Initialization Vector) – dodatna vrednost, uporabljena pri šifriranju za večjo varnost.

JSON (JavaScript Object Notation) – format za zapis strukturiranih podatkov.

Man-in-the-Middle (MITM) – napad, pri katerem napadalec prestreza komunikacijo med napravami.

MIC (Message Integrity Code) – vrednost za preverjanje integritete podatkov.

Monitor mode – način delovanja omrežne kartice za zajem vsega Wi-Fi prometa.

QoS (Quality of Service) – mehanizem za upravljanje prioritet omrežnega prometa.

RADIUS (Remote Authentication Dial-In User Service) – strežnik za centralno avtentikacijo uporabnikov.

SAE (Simultaneous Authentication of Equals) – avtentikacijski mehanizem protokola WPA3.

Social engineering – manipulacija ljudi za pridobitev zaupnih informacij ali nepooblaščenega dostopa.

SSID (Service Set Identifier) – ime brezžičnega omrežja.

Sniffing – prestrezanje in analiza omrežnega prometa.

TKIP (Temporal Key Integrity Protocol) – starejši šifrirni mehanizem, uporabljen v WPA.

WEP (Wired Equivalent Privacy) – prvi Wi-Fi varnostni protokol, danes zastarel.

Wi-Fi (Wireless Fidelity) – tehnologija brezžičnega lokalnega omrežja.

Wordlist – seznam možnih gesel, uporabljen pri napadih na gesla.

WPA – naslednik protokola WEP.

WPA2 – izboljšana različica WPA z AES šifriranjem.

WPA3 – najnovejši Wi-Fi varnostni standard.

1. UVOD

Brezžična omrežja so danes ključen del informacijske infrastrukture. Omogočajo hitro in enostavno povezovanje v domačem, poslovnem in javnem okolju. Njihova razširjenost pa prinaša večjo izpostavljenost različnim varnostnim tveganjem, kot so nepooblaščen dostop, prestrezanje podatkov, napadi na delovanje omrežja in zlorabe slabo konfiguriranih dostopnih točk. Zato je razumevanje ranljivosti brezžičnih omrežij ter ustreznih zaščitnih mehanizmov vedno pomembnejše za podjetja in posameznike.

Namen raziskovalne naloge je preučiti varnost Wi-Fi omrežij na območju Velenja. Raziskava se bo osredotočila na najpogostejše ranljivosti in načine napadov ter ocenila učinkovitost obstoječih varnostnih ukrepov. Izvedeni bodo kontrolirani varnostni testi in simulacije napadov, da se ugotovi dejansko stanje zaščite izbranih brezžičnih omrežij. Posebna pozornost bo namenjena prepoznavanju napačnih konfiguracij, zastarelih varnostnih protokolov in drugih dejavnikov, ki lahko povečajo tveganje za uspešen napad.

Cilj te raziskovalne naloge je izboljšati razumevanje varnostnih tveganj brezžičnih omrežij ter podati priporočila za boljšo zaščito Wi-Fi infrastrukture v lokalnem okolju.

2. PROBLEM

Brezžična Wi-Fi omrežja omogočajo prenos podatkov brez fizične povezave. Vendar pa prav zaradi prenosa po zraku predstavljajo večje varnostno tveganje kot žična omrežja. Signal je dostopen vsem napravam v dometu. To napadalcem omogoča prestrezanje prometa, izvajanje napadov tipa man-in-the-middle, postavljanje lažnih dostopnih točk in druge oblike zlorab. Stopnja varnosti je močno odvisna od uporabljenih varnostnih protokolov (WEP, WPA, WPA2, WPA3), pravilne konfiguracije dostopnih točk ter ustreznega nadzora omrežja.

Kljub napredku varnostnih mehanizmov še vedno obstajajo številne ranljivosti. Te izhajajo iz zastarelih protokolov, nepravilnih nastavitev ali neustreznega upravljanja omrežja. Zato je razumevanje delovanja brezžičnih omrežij in njihovih varnostnih pomanjkljivosti ključno za zaščito podatkov in zmanjšanje tveganja zlorab.

2.1 HIPOTEZE

2.1.1 Hipoteza 1

Omrežja, ki uporabljajo zastarele protokole (WEP, starejši WPA), so bistveno bolj ranljiva za napade kot omrežja z WPA2 ali WPA3.

2.1.2 Hipoteza 2

Uporaba sodobnih usmerjevalnikov zmanjšuje varnostne ranljivosti Wi-Fi omrežij.

2.1.3 Hipoteza 3

Večina analiziranih Wi-Fi omrežij uporablja neoptimalne varnostne nastavitve.

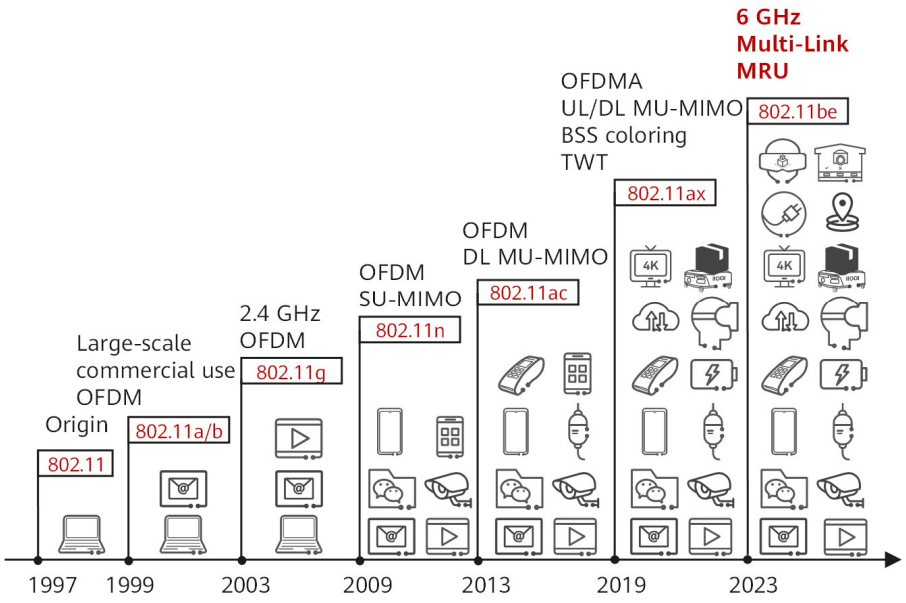
3. PREGLED STANJA TEHNIKE

3.1 Zgodovina razvoja brezžičnih omrežij Wi-Fi

Razvoj brezžičnih lokalnih omrežij se je začel v devetdesetih letih, ko je organizacija IEEE izdala prvi standard IEEE 802.11 leta 1997, ki je omogočal hitrosti prenosa 1–2 Mb/s. [1]

Z nadaljnjim razvojem so nastajale nove različice standarda (802.11a/b/g/n/ac/ax/be), ki so prinašale višje hitrosti prenosa, izboljšano zanesljivost povezave ter naprednejše varnostne mehanizme.[2]

Vzporedno z razvojem standardov so se razvijali tudi varnostni protokoli. Prvotni protokol WEP, uveden skupaj z zgodnjimi standardi Wi-Fi, se je zaradi varnostnih pomanjkljivosti izkazal za nezadostnega, zato so bili kasneje uvedeni WPA, WPA2 in WPA3, ki zagotavljajo bistveno višjo raven šifriranja in avtentikacije v brezžičnih omrežjih.[3]



Slika 1: Razvoj Wi-Fi standardov [1]

[1] Huawei Technologies Co., Ltd., *WiFi:* https://info.support.huawei.com/info-finder/encyclopedia/en/WiFi.html

[2] One World Rental, *History of WiF:* https://oneworldrental.com/blog/history-of-wifi-timeline-of-all-wifi-generations-with-specs-details/

[3] TechTarget, *Wireless security & encryption basics:* https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

3.2 VARNOSTNI PROTOKOLI

3.2.1 WEP

Varnostni protokol za zaščito brezžičnih omrežij, uveden skupaj z zgodnjimi standardi IEEE 802.11. uporablja osnovne metode šifriranja, ki so se sčasoma izkazale za ranljive. Zato ga danes ne štejemo več za varnega. Zaradi pomanjkljivosti v načinu generiranja ključev je mogoče zaščito WEP relativno hitro razbiti. Njegova uporaba v sodobnih omrežjih ni več priporočljiva. WPA (Wi-Fi Protected Access) WPA je bil uveden kot začasna izboljšava protokola WEP. Uporablja izboljšane metode šifriranja (TKIP) ter dinamično generiranje ključev. To je povečalo varnost, vendar danes prav tako ne zagotavlja več zadostne ravni zaščite.[3]

3.2.2 WPA

WPA je bil uveden kot začasna izboljšava protokola WEP. Uporablja izboljšane metode šifriranja (TKIP) ter dinamično generiranje ključev, kar je povečalo varnost, vendar danes prav tako ne zagotavlja več zadostne ravni zaščite.[3]

3.2.3 WPA2

WPA2 predstavlja nadgradnjo WPA in uporablja naprednejši šifrirni algoritem AES, ki zagotavlja višjo stopnjo zaščite podatkov. Dolga leta je bil najpogosteje uporabljen varnostni standard v domačih in poslovnih omrežjih.[3]

3.2.4 WPA3

WPA3 je najnovejši varnostni standard, ki uvaja boljše metode avtentikacije, močnejše šifriranje in večjo odpornost proti napadom z ugibanjem gesel. WPA2/WPA3 Enterprise[3]

3.2.5 WPA2/WPA3 Enterprise

Različica WPA2/WPA3 Enterprise je namenjena predvsem poslovnim, izobraževalnim in institucionalnim omrežjem, kjer je treba zagotoviti višjo raven varnosti in centraliziran nadzor dostopa. Ta različica se razlikuje od Personal, ki uporablja eno skupno geslo za vse uporabnike. Enterprise različica uporablja individualno avtentikacijo za vsakega uporabnika s pomočjo standarda.[4]

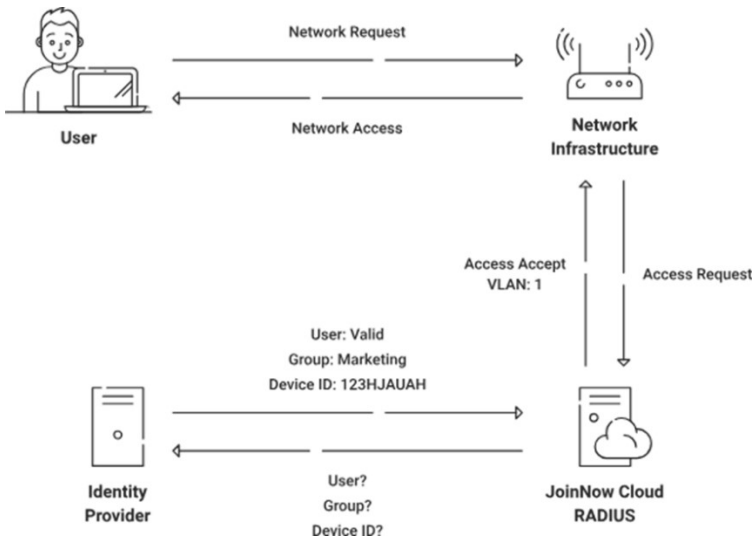
Pri tem načinu preverjanja identitete sodelujejo tri ključne komponente:

odjemalec (supplicant) – naprava uporabnika, ki se želi povezati v omrežje,

dostopna točka (authenticator) – posreduje zahtevo za avtentikacijo,

RADIUS strežnik – preveri uporabniške podatke in odloči, ali je dostop dovoljen.

Avtentikacija se izvaja preko protokola EAP (Extensible Authentication Protocol), ki omogoča različne metode preverjanja identitete, kot so prijava z uporabniškim imenom in geslom, žetoni ali digitalna potrdila. Takšen pristop omogoča centralizirano upravljanje uporabnikov, natančno določanje pravic dostopa ter bistveno večjo varnost v primerjavi z omrežji, ki uporabljajo skupno geslo.[4]



Slika 2: Shema avtentikacije WPA2/WPA3

[4] Cloudi-Fi. *WPA2/WPA3-Enterprise:* https://www.cloudi-fi.com/blog/wpa2-enterprise-802-1x

4. MATERIALI IN METODE DELA

4.1 IZBIRA STROJNE OPREME

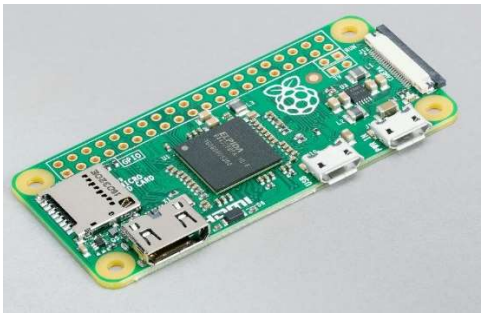
4.1.1 Antena

Pri raziskavi je bila uporabljena nizkocenovna brezžična USB antena Flyrong RF150US z veznim naborom(*chipset*) RT5370. Antena podpira način spremljanja (*monitoring*) ter vbrizgovanje paketov (*packet injection*), kar omogoča zajemanje brezžičnega prometa, zaznavanje dostopnih točk in izvajanje kontroliranih varnostnih testov Wi-Fi omrežij. Zaradi široke podpore v operacijskih sistemih Linux in združljivosti z orodji za analizo brezžičnih omrežij predstavlja primerno rešitev za raziskovalne in izobraževalne namene.

Slika 3: Nizkocenovna antena

4.1.2 Raspberry Pi Zero

Kot osnovna računalniška platforma je bil uporabljen Raspberry Pi Zero, ki zaradi majhne porabe energije, kompaktne velikosti in zadostne procesorske zmogljivosti omogoča izvajanje orodij za spremljanje in analizo brezžičnih omrežij ter avtomatizacijo meritev.



Slika 4: Raspberry Pi Zero

4.1.3 Usmerjevalniki

Usmerjevalnik (router) je osrednja omrežna naprava, ki omogoča povezovanje več naprav v lokalno omrežje ter njihovo povezavo z internetom. Poleg usmerjanja omrežnega prometa ima pomembno vlogo tudi pri zagotavljanju varnosti brezžičnega omrežja, saj omogoča nastavitev šifriranja, avtentikacijskih mehanizmov, nadzor dostopa ter upravljanje povezanih naprav. S pravilno konfiguracijo usmerjevalnika je mogoče bistveno zmanjšati tveganje nepooblaščenega dostopa in drugih varnostnih zlorab.

Slika 5: Linksys usmerjevalnik uporabljen v raziskovalni nalogi

V raziskavi sta bila uporabljena usmerjevalnika TP-Link in Linksys. Usmerjevalnik TP-Link je bil uporabljen predvsem zaradi podpore standardu Wi-Fi 7, kar je omogočilo testiranje sodobnih varnostnih protokolov in novih brezžičnih tehnologij. Usmerjevalnik Linksys pa je bil uporabljen zaradi možnosti konfiguracije starejših varnostnih protokolov, vključno z WEP, kar je omogočilo primerjalno analizo varnosti med zastarelimi in sodobnimi zaščitnimi mehanizmi.

Slika 6: Tp-link usmerjevalnik uporabljen v raziskovalni nalogi

4.2 IZBIRA PROGRAMSKE OPREME

4.2.1 Linux terminal

Linux terminal predstavlja osnovno delovno okolje za izvajanje varnostnih analiz, upravljanje omrežnih vmesnikov in uporabo specializiranih varnostnih orodij. Omogoča neposreden dostop do sistemskih ukazov, kar omogoča natančen nadzor nad delovanjem sistema ter avtomatizacijo postopkov s skriptami. Zaradi stabilnosti, prilagodljivosti in široke podpore varnostnih orodij je Linux standardna platforma pri testiranju omrežne varnosti.

4.2.2 Python

Python je programski jezik, ki se uporablja za razvoj skript za avtomatizacijo nalog, analizo zajetih podatkov ter obdelavo rezultatov varnostnih testiranj. Veliko število razpoložljivih knjižnic omogoča enostavno delo z omrežnimi protokoli, obdelavo podatkov in razvoj lastnih varnostnih orodij. Zaradi enostavne sintakse in dobre berljivosti kode je primeren tako za raziskovalne projekte kot tudi za razvoj kompleksnejših rešitev.

Slika 7: Logo python programskega jezika

4.2.3 Aircrack-ng paket orodij

Aircrack-ng je zbirka specializiranih orodij za spremljanje, zajemanje in analizo prometa v brezžičnih omrežjih. Paket vključuje orodja za preklop omrežnih kartic v monitor način, zajemanje handshake paketov, analizo omrežnega prometa ter testiranje odpornosti Wi-Fi omrežij proti napadom na gesla. Zaradi široke uporabe v izobraževalnem in raziskovalnem okolju predstavlja eno izmed osnovnih orodij pri analizi varnosti brezžičnih omrežij.[5]

[5] Aircrack-ng Project. Aircrack-ng dokumentacija: https://www.aircrack-ng.org/

4.2.4 Pwnagotchi programska oprema

Pwnagotchi je programska oprema, namenjena avtomatiziranemu zbiranju handshake paketov v brezžičnih omrežjih, pri čemer uporablja algoritme za optimizacijo načina delovanja glede na okolje. Sistem običajno deluje na majhnih vgrajenih napravah in omogoča dolgotrajno pasivno spremljanje omrežij. Uporablja se predvsem v raziskovalne in izobraževalne namene za preučevanje varnosti brezžičnih omrežij ter analizo učinkovitosti zaščitnih mehanizmov.[6]

4.2.5 Hashcat

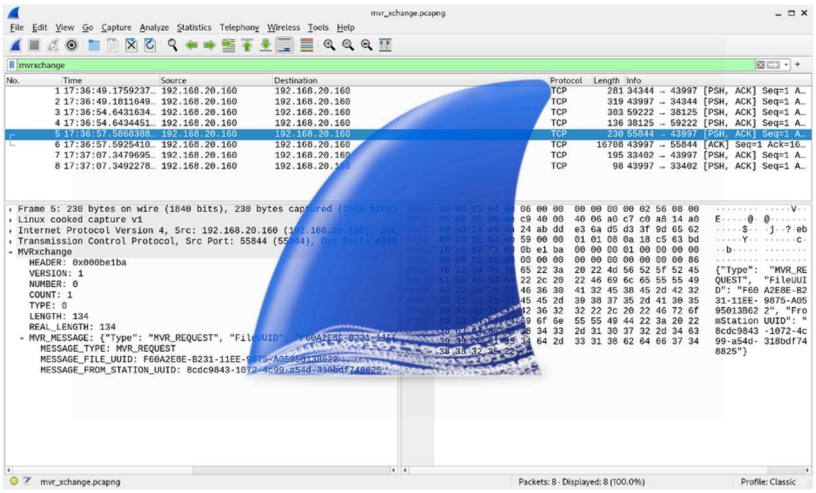
Hashcat je napredno orodje za razbijanje (cracking) zgoščenih vrednosti gesel (hash). Namenjeno je testiranju varnosti gesel z uporabo različnih napadalnih metod, kot so slovarski napadi, brute-force napadi ter kombinirani napadi. Hashcat izkorišča zmogljivost grafičnih kartic (GPU), kar omogoča bistveno hitrejše preverjanje velikega števila možnih gesel v primerjavi s klasičnimi CPU rešitvami. Orodje podpira številne hash algoritme (WPA/WPA2, MD5, SHA-1, NTLM in druge) in se pogosto uporablja v varnostnih raziskavah ter penetracijskem testiranju.[7]

[6]Pwnagotchi je programska oprema: https://pwnagotchi.ai/

[7] Uradna stran projekta: https://hashcat.net/hashcat/

4.3 Wireshark

Wireshark je napredno orodje za zajemanje in analizo omrežnega prometa (packet analyzer), namenjeno diagnostiki omrežij, odpravljanju napak ter varnostnim analizam. Omogoča prestrezanje podatkovnih paketov v realnem času in njihov podroben pregled na različnih nivojih omrežnega modela (Ethernet, IP, TCP, HTTP, DNS in drugi protokoli). S pomočjo zmogljivih filtrov lahko uporabnik natančno izloči relevantni promet, kar omogoča učinkovito odkrivanje nepravilnosti, omrežnih napadov ali napačnih konfiguracij. Orodje se pogosto uporablja v izobraževanju, omrežnem inženiringu ter penetracijskem testiranju, saj omogoča poglobljen vpogled v delovanje komunikacijskih protokolov.[8]



Slika 8: Logo ter prikaz aplikacije Wireshark

[8] Uradna starn Wiresharka : https://www.wireshark.org

4.4 POTEK DELA

4.4.1 POTEK INSTALACIJE POTREBNE PROGRAMSKE OPREME

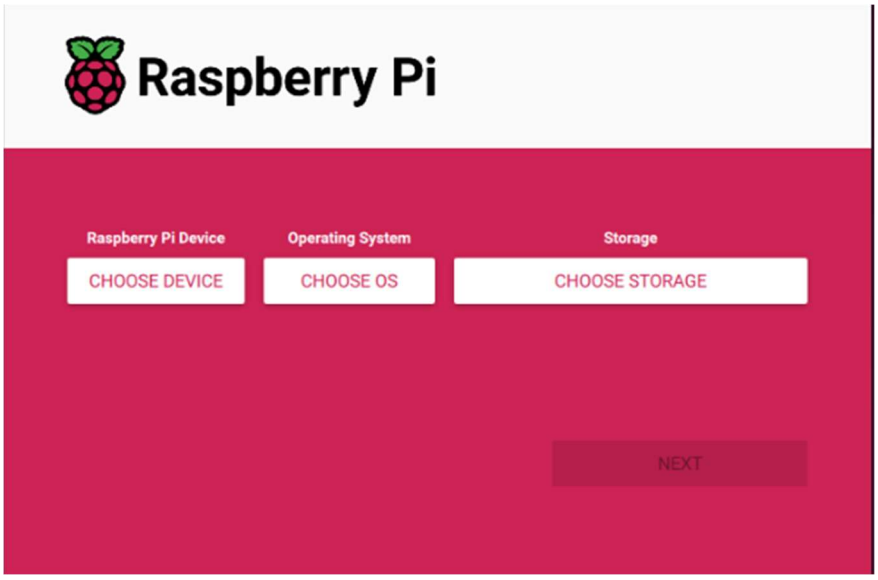
4.3.1.1 INŠTALACIJA PRIMERNEGA OPERACIJSKEGA SISTEMA

Za izvedbo naloge je bila potrebna uporaba operacijskega sistema Linux. Izbral sem distribucijo Kali Linux, ki je namenjena varnostnim testiranjem in je dostopna na uradni spletni strani (https://www.kali.org/get-kali/#kali-installer-images). Operacijski sistem sem namestil neposredno na disk računalnika, saj takšna namestitev omogoča popolno funkcionalnost strojne opreme, predvsem omrežnih kartic in monitor načina delovanja, ki pri uporabi virtualnega okolja (VirtualBox) ni delovala optimalno.

Slika 9: Primer izgleda operacijskega sistema

4.3.1.2 VZPOSTAVITEV PROGRAMA PWNAGOTCHI

Programsko opremo Pwnagotchi sem namestil na napravo Raspberry Pi Zero s pomočjo PiImager programa, saj je ta platforma priporočena tudi na uradni strani projekta zaradi nizke porabe energije, stabilnega delovanja in dobre združljivosti z brezžičnimi vmesniki. Po namestitvi sistema sem konfiguriral omrežni vmesnik za delovanje v monitor načinu ter nastavil osnovne parametre delovanja programske opreme. Napravi sem dodal tudi zaslon Waveshare 4 InkPaper, ki omogoča prikaz trenutnega stanja naprave, zaznanih omrežij in zajetih handshake paketov. Dodan je bil tudi PiSugar modul, ki omogoča napajanje prek baterije, polnjenje ter večjo prenosljivost naprave. Tako konfigurirana naprava je omogočala samodejno in neprekinjeno izvajanje testiranj varnosti brezžičnih omrežij.



Slika 10: Program za namestitev Pwnagotchija na kartico

Za potrebe raziskave je bilo testiranje izvedeno v nadzorovanem testnem okolju. Najprej sem z računalnikom opravil skeniranje vseh zaznanih brezžičnih omrežij v okolici, nato pa sem konfiguriral whitelist omrežij, ki jih naprava ni smela zajemati. S tem sem zagotovil, da so se meritve izvajale izključno nad izbranimi testnimi omrežji. Testiranje je potekalo v 5. nadstropju šole, kjer sem z izbiro lokacije dodatno omejil doseg zaznavanja oddaljenih omrežij ter tako zmanjšal možnost nenamernega zajemanja podatkov iz omrežij, ki niso bila vključena v raziskavo.

Slika 11: Izdelek na katerem je pwnagotchi program

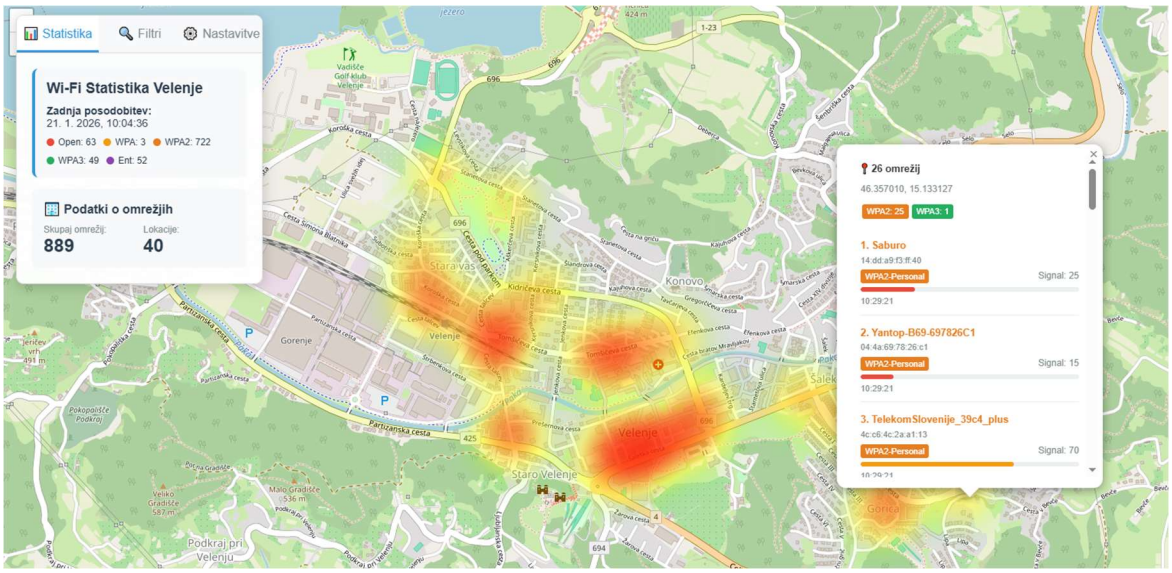
4.4.2 SKENIRANJE VELENJA S PYTHON PROGRAMOM

Za analizo razpoložljivih brezžičnih omrežij sem razvil Python program, ki samodejno izvaja periodično skeniranje Wi-Fi omrežij ter pridobljene podatke zapisuje v strukturirano JSON datoteko. Program v določenih časovnih intervalih zazna razpoložljiva omrežja, pri čemer za vsako omrežje zajame ključne podatke, kot so ime omrežja (SSID), naslov dostopne točke (BSSID), vrsto zaščite ter jakost signala.

Sistem za vsako zaznano omrežje vodi evidenco zaznav skozi čas in posodablja podatke o najmočnejšem izmerjenem signalu ter času zadnje zaznave, s čimer se prepreči podvajanje zapisov in zagotovi pregled nad spremembami v okolju. Po zaključku skeniranja program podatke organizira v poenostavljeno izhodno strukturo, ki vsebuje skupno število zaznanih omrežij, osnovno statistiko glede na tip zaščite ter seznam omrežij z njihovimi ključnimi parametri. Takšen način obdelave omogoča pregledno analizo razširjenosti posameznih varnostnih protokolov in predstavlja osnovo za nadaljnjo varnostno oceno brezžičnega okolja.

Koda programa je podana v prilogi.

4.4.3 OBDELAVA PODATKOV TER VIZUALNI PRIKAZ



Slika 12: Heat map skeniranih omrežij v Velenju

4.4.4 ZAČETNO TESTIRANJE WEP VARNOSTNEGA PROTOKOLA

Pri testiranju varnosti protokola WEP sem uporabil starejši Linksys brezžični usmerjevalnik, ki sem ga konfiguriral za uporabo WEP šifriranja. Za primer sem nastavil geslo (passphrase) Velenje1, iz katerega se generira 64-bitni ali 128-bitni WEP ključ, ki se nato uporablja za prijavo v omrežje.

V testno omrežje sem povezal eno napravo, na kateri sem izvajal običajne uporabniške aktivnosti, kot so brskanje po spletu in uporaba družbenih omrežij, s čimer sem ustvaril realistično okolje stalnega omrežnega prometa. Generiranje večje količine prometa je pri analizi WEP pomembno, ker vsaka poslana podatkovna enota vsebuje tudi t. i. inicializacijski vektor (IV), ki sodeluje pri šifriranju podatkov.

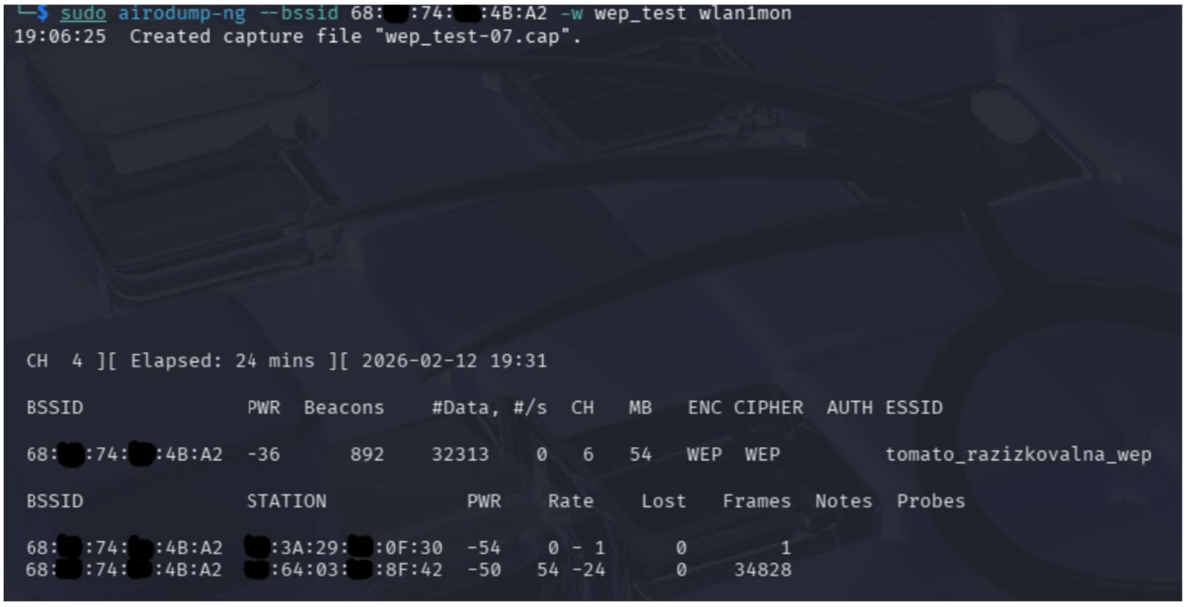
Inicializacijski vektor predstavlja dodatno vrednost, ki se doda s šifrirnim ključem, ki se doda ključu, da vsako sporočilo izgleda nekoliko drugače. Težava pri WEP je, da je število možnih števil omejeno, zato se po določenem času začnejo ponavljati. Če napadalec zbere veliko število paketov, v katerih se isti IV ponovi večkrat, lahko primerja šifrirane podatke in postopoma izračuna dejanski šifrirni ključ omrežja. Več kot je prometa v omrežju, hitreje pride do ponavljanja IV, zato je za demonstracijo ranljivosti potrebno ustvariti stalno izmenjavo podatkov.

4.4.4.1 POSTOPEK IZRABLJANJA ŠIBKOSTI VARNOSTNEGA PROTOKOLA WEP

Za izvedbo testiranja sem najprej omrežno kartico preklopil v monitor način z ukazom:

sudo airmon-ng start wlan1

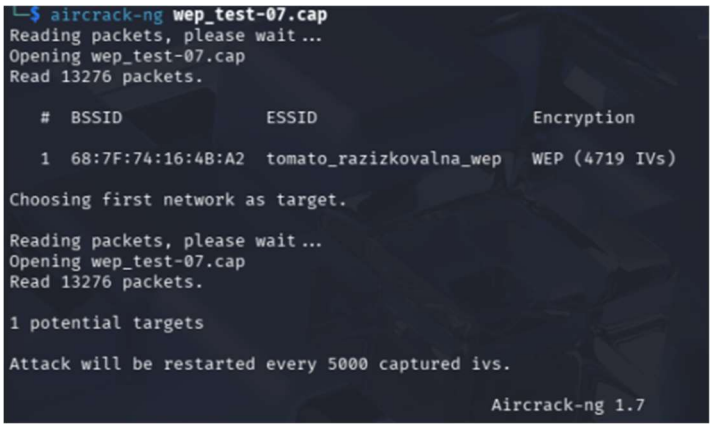
Ukaz je samodejno preklopil omrežni vmesnik wlan1 v monitor način ter ustvaril nov vmesnik wlan1mon, kjer oznaka mon pomeni monitoring. S tem je bilo omogočeno zajemanje prometa vseh brezžičnih omrežij v dosegu. Po identifikaciji ciljnega testnega omrežja sem z orodjem airodump-ng začel spremljanje in shranjevanje omrežnega prometa v datoteko tipa .cap, ki vsebuje zajete pakete, potrebne za nadaljnjo analizo. V ukazni vrstici sem navedel BSSID ciljnega usmerjevalnika, določil ime izhodne datoteke (v mojem primeru wep_test.cap) ter podal tudi uporabljeni omrežni vmesnik, namenjen spremljanju prometa.



Slika 13: Ponavljajoče se spremljanje ter shranjevanje prometa v določenem omrežju

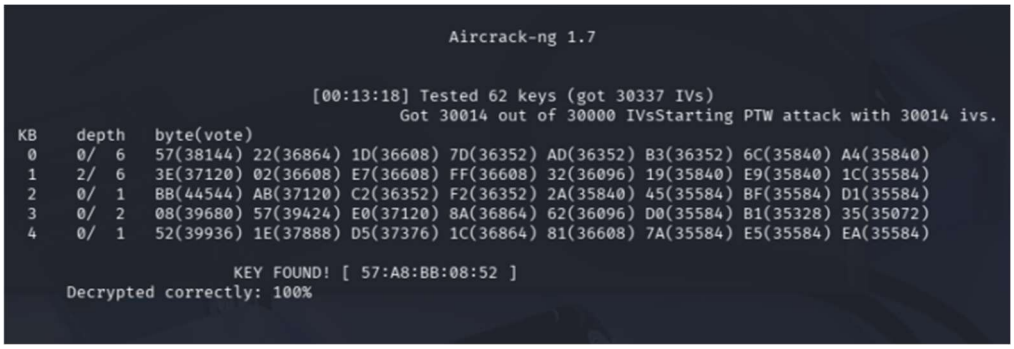
Po zajemu zadostnega števila paketov, predvsem inicializacijskih vektorjev (IV), sem zagnal orodje aircrack-ng, ki iz zajetih podatkov izvede kriptoanalizo WEP šifriranja.

Program pri tem uporabi PTW napadalno metodo, ki na podlagi statistične analize ponavljajočih se IV omogoča izračun dejanskega šifrirnega ključa omrežja.



Slika 14:Zagon orodja Aircrack-ng

V izvedenem testu je bil ključ testnega omrežja uspešno izračunan v približno petih minutah.



Slika 15: Rezultat analize z orodjem Aircrack-ng

Pri analizi varnosti protokola WEP ni bilo uporabljeno klasično brute-force ugibanje gesla, saj ta metoda preverja veliko število možnih kombinacij gesel in je časovno bistveno zahtevnejša. WEP vsebuje znano kriptografsko ranljivost v načinu uporabe inicializacijskih vektorjev (IV), zaradi katere je mogoče šifrirni ključ izračunati neposredno iz zajetega omrežnega prometa s statistično analizo. Zato je bila izbrana metoda analize zajetih paketov (PTW napad), ki omogoča bistveno hitrejše in realnejše prikazovanje dejanske ranljivosti protokola, saj ne temelji na ugibanju gesla, temveč na izkoriščanju konstrukcijske slabosti samega šifrirnega mehanizma.

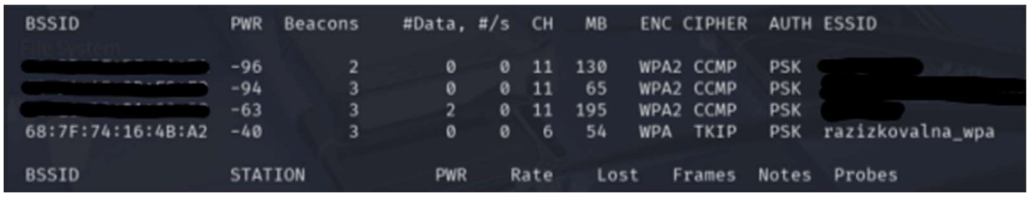
4.4.5 TESTIRANJE VARNOSTNEGA PROTOKOLA WPA / WPA2

Za ta protokola sem pri pregledu stanja tehnike ugotovil, da je pri konfiguraciji usmerjevalnika mogoče nastaviti WPA posamič, WPA2 posamič ter WPA/WPA2 (mixed) posamič.

V tem delu sem nastavil usmerjevalnik na WPA/WPA2(mixed), ki omogoča povezovanje naprav z uporabo obeh protokolov.

4.4.5.1 WPA

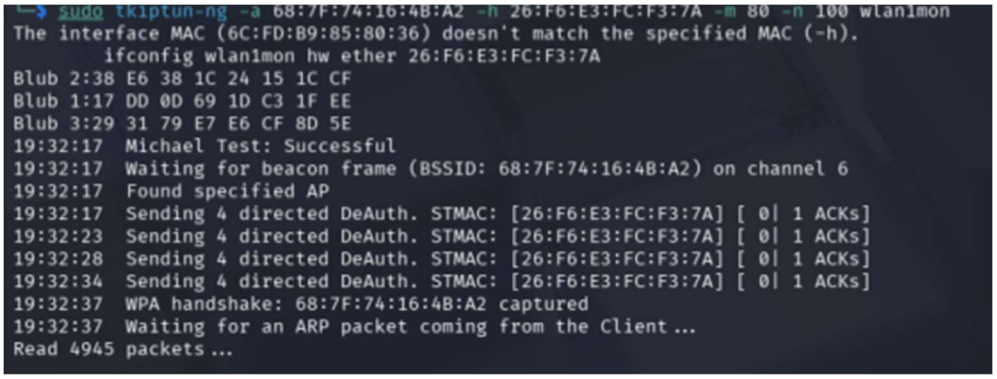
V praktičnem delu sem z brezžično omrežno kartico najprej izvedel skeniranje razpoložljivih brezžičnih omrežij ter identificiral testno omrežje, konfigurirano v izoliranem okolju. Kartico sem nato preklopil v način spremljanja (monitor mode), kar je omogočilo poslušanje prometa med usmerjevalnikom in povezano testno napravo, ki je v omrežju generirala potreben promet.



Slika 16: Iskanje ssid ciljanega omrežja

Za nadaljnjo analizo sem uporabil orodje tkiptun-ng, ki je izvedla napad, tehnično opisan v raziskavi Beck - Tews[9], ter omogoča preverjanje ranljivosti TKIP mehanizma. Cilj postopka je bil zajem ustreznih paketov (predvsem ARP paketov), ki so potrebni za izvedbo nadaljnjih faz napada in preverjanje delovanja izkoriščene ranljivosti.

[9] Beck-Tews, Practical attacks against WEP and WPA https://www.researchgate.net/publication/220332983_Practical_attacks_against_WEP_and_WPA



Slika 17: Uporaba programa definiranega od back&tews

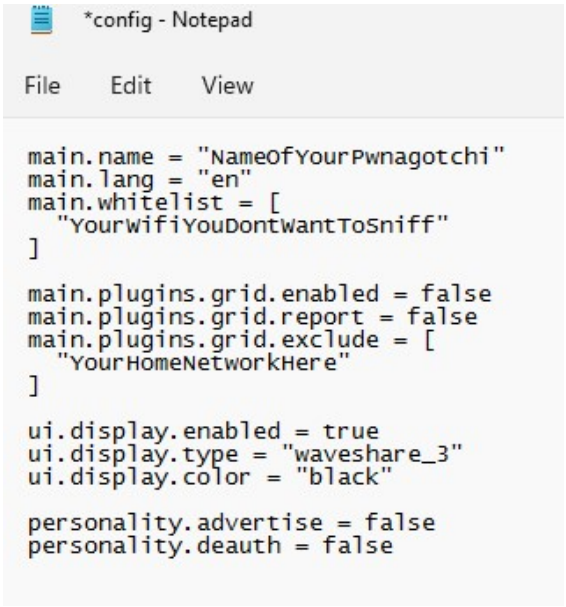
Kljub pravilni konfiguraciji testnega okolja pričakovani ARP paket ni bil zaznan, zato nadaljnjih faz testiranja ni bilo mogoče izvesti. Posledično je bil dosežen operativni zastoj, pri katerem ni bilo mogoče zanesljivo določiti ali je bil vzrok v konfiguraciji okolja v omejitvah uporabljene strojne ali programske opreme, oziroma v nezadostnem prometu v omrežju. Zaradi časovnih omejitev projekta nadaljnja optimizacija testnega okolja in ponovitev meritev nista bili izvedeni, zato eksperimentalnega dela v tem segmentu ni bilo mogoče dokončati.

4.4.5.2 WPA2

Eden izmed znanih napadov na omrežja WPA2 je napad z grobo silo (brute-force), pri katerem napadalec preizkuša veliko število možnih gesel, dokler ne najde pravilnega.

Napad, ki sem ga izvedel, se imenuje napad z grobo silo z uporabo seznama gesel (wordlist), pri katerem se namesto naključnega generiranja kombinacij uporablja vnaprej pripravljen seznam možnih gesel (wordlist), kar lahko bistveno pospeši proces ugibanja pravilnega gesla.

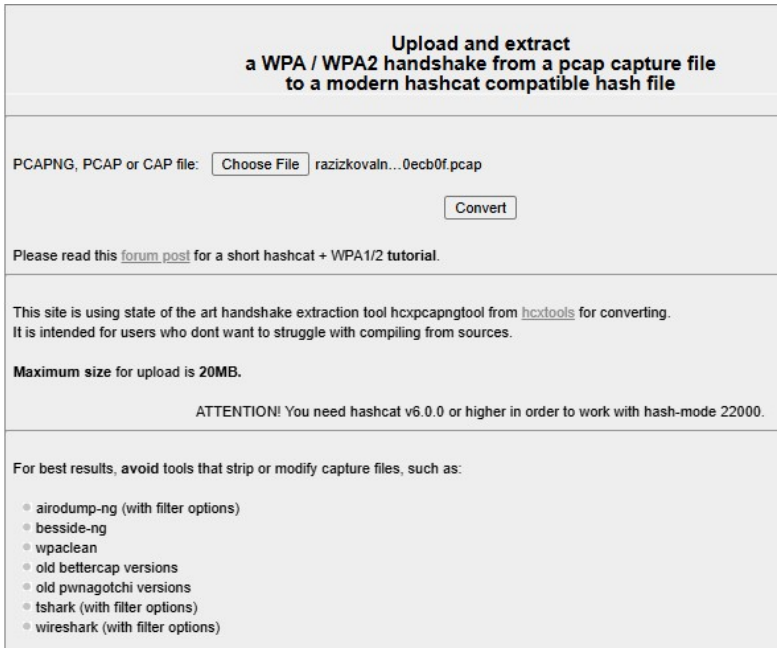
Za zajem rokovanja je bil uporabljen program Pwnagotchi, ki sem ga konfiguriral tako, da sem na seznam dovoljenih omrežij (main.whitelist) dodal tista omrežja, ki jih nisem želel opazovati oziroma napadati.



Slika 18: Primer konfiguracije programa

Pri tem sem naletel na omejitev: ker Pwnagotchi deluje na napravi Raspberry Pi Zero, ne podpira zaznavanja 5-GHz omrežij, temveč samo 2,4-GHz omrežja. Usmerjevalnik je zato moral biti nastavljen na način b/g/n, saj standardi a/ac/ax niso podprti. To predstavlja pogost problem pri uporabi nizkocenovnih omrežnih kartic.

Po ustrezni konfiguraciji (b/g/n) sem zagnal Pwnagotchi, ki se je samodejno preklopil v način poslušanja omrežnega prometa. Naprava je uspešno zajela rokovanje (handshake), ki sem ga kasneje prek protokola za prenos datotek FTP (File Transfer Protocol) prenesel na računalnik ter pretvoril v obliko, ki jo program Hashcat lahko bere in obdeluje.



Slika 19: Pretvornik datotek na uradni strani Hashcat

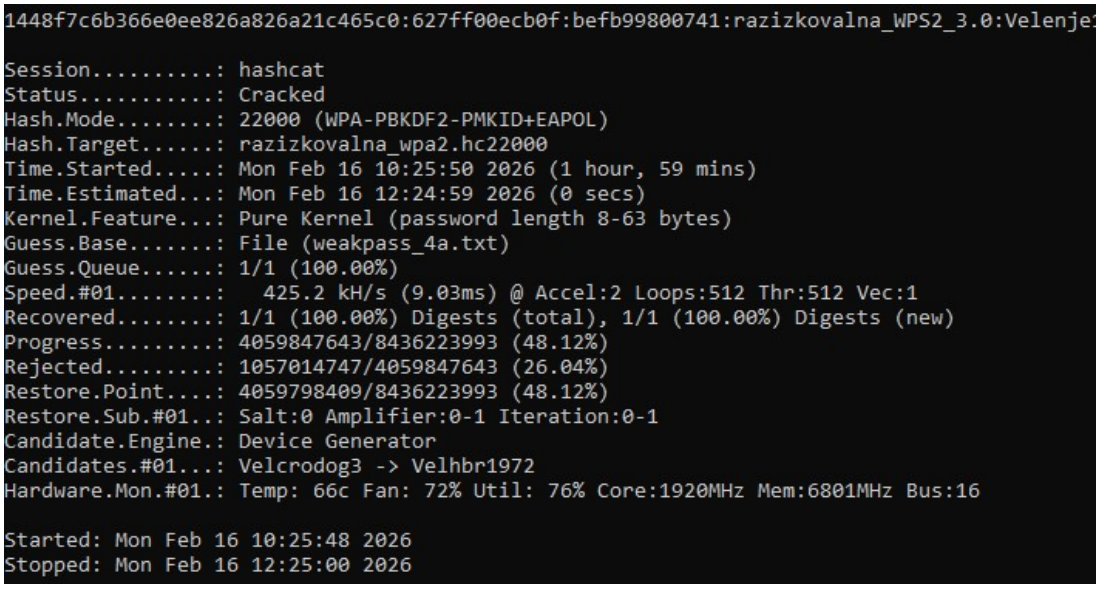
Po konverziji sem datoteko uvozil v program Hashcat, ki deluje v okolju Windows Terminal.

Za začetek napada sem uporabil naslednji ukaz:

```
hashcat -m 22000 razizkovalna_wpa2.hc22000 weakpass_4a.txt
```

Parameter `-m` v programu hashcat določa način oziroma tip hasha, ki ga program napada. Koda `22000` označuje WPA/WPA2 Wi-Fi zajeme, pretvorjene v format `.hc22000`. Datoteka `raziskovalna_wpa2.hc22000` vsebuje zajete podatke omrežja, medtem ko je `weakpass_4a.txt` izbrani wordlist, ki ga hashcat uporablja za preverjanje možnih gesel.

Proces preizkušanja gesel je trajal približno 4 ure, dokler program ni našel ustreznega gesla Velenje1, ki predstavlja primer gesla, značilnega za lokalno okolje in zato realističnega za testne scenarije. Enako geslo sem uporabljal skozi vse konfiguracije in testiranja, da so bili rezultati primerljivi.



Slika 20: Zaključen program vrne poizvedbo

Za testiranje sem uporabil datoteko (weakpass_4a.txt)10 velikosti 81,37 GB, ki je vsebovala približno 8.440.000.000 možnih gesel. Čas izvajanja je bil neposredno odvisen od velikosti wordlista, zmogljivosti strojne opreme ter kompleksnosti ciljnega gesla, zato se lahko pri večjih seznamih ali zahtevnejših geslih čas obdelave bistveno podaljša.

V nekaterih primerih se je pojavil tudi rezultat »exhausted«, kar pomeni, da je program preizkusil vse vnose v uporabljenem wordlistu, vendar pravilnega gesla ni našel. Takšne situacije so se pojavile predvsem pri manjših wordlistih ter pri daljših geslih, ki so obsegala približno 10 ali več znakov, saj ta pogosto niso vključena v omejene sezname pogostih gesel.

[10] Weakpass. Weakpass_4a – Wordlist znanih gesel: https://weakpass.com/wordlists?name=weakpass_4a

5. REZULTATI

Na podlagi večkratnega skeniranja območja Velenja je bilo zaznanih 889 brezžičnih omrežij na 40 lokacijah, kar omogoča reprezentativen vpogled v dejansko stanje uporabe varnostnih protokolov v Šaleški dolini. Kljub velikim številkam celotno Velenje ni bilo vključeno v raziskavo.

Varnostni protokol	Število omrežij	Delež (%)	Varnostna ocena
Open	63	7 %	zelo nizka
WEP	0	<1 %	neuporabna
WPA	3	<1 %	nizka
WPA2	722	81 %	srednja–visoka
WPA3	49	6 %	zelo visoka
Enterprise (802.1X)	52	6 %	zelo visoka

Tabela 1: Po lestvici razporeditev varnih vrst zaščit

Ta tabela prikazuje dejansko razporeditev uporabljenih zaščitnih tehnologij med zaznanimi brezžičnimi omrežji ter omogoča neposredno primerjavo stopnje razširjenosti posameznih varnostnih standardov na analiziranem območju.

Pri odprtih omrežjih (open network), kjer ne uporabljajo nobenega mehanizma avtentikacije ali šifriranja, je nepooblaščen dostop tehnično trivialen, kar pomeni, da se lahko katerakoli naprava v dosegu brez omejitev poveže v omrežje in prestreza promet.

Protokol WEP v skeniranem okolju praktično ni bil zaznan (Tabela 1), kar kaže na njegovo postopno opuščanje. Laboratorijsko testiranje pa je potrdilo, da je zaščito WEP mogoče razbiti v nekaj minutah z analizo zajetega prometa, zato ta protokol ne predstavlja več uporabne varnostne rešitve. Kar predstavlja dobro stran je, da se v Velenju ne uporablja tega protokola.

Rezultati analize so pokazali, da je bil protokol WPA zasnovan predvsem kot nadgradnja protokola WEP in ne kot popolnoma nov varnostni sistem. Zaradi potrebe po združljivosti s starejšo strojno opremo je WPA ohranil šifrirni algoritem RC4, hkrati pa uvedel mehanizem TKIP, ki je izboljšal zaščito integritete podatkov. Za preverjanje integritete paketov je bil uveden MIC ključ (Michael). Sistem je sproti preverjal integriteto paketov; v primeru nepravilnega ICV je bil paket zavržen, ob večkratnih napakah MIC pa je bila komunikacija

začasno prekinjena, kar je ključna informacija za iskanje zadnjih 12 bajtov. Kljub uvedenim izboljšavam je analiza pokazala, da zaščita ni popolnoma odporna na napade. Mehanizme zaščite je bilo mogoče obiti z uporabo različnih QoS kanalov, kjer se je TKIP sequence counter lahko ponovno začel od začetne vrednosti.

Ugotovitve potrjujejo, da WPA predstavlja pomembno izboljšavo v primerjavi z WEP, vendar zaradi konstrukcijskih omejitev in zastarele kriptografije ne zagotavlja več zadostne ravni zaščite in se danes obravnava kot zastarel varnostni standard.

WPA2 predstavlja prevladujoč standard v Šaleški dolini. V laboratorijskem testnem okolju je bilo mogoče po zajemu handshake podatkov izvesti napad z uporabo wordlista, pri čemer je bila uspešnost napada odvisna od kompleksnosti gesla ter uporabe dobre strojne opreme. Pri kompleksnejših geslih napad ni bil uspešen, kar potrjuje, da je WPA2 ob pravilni konfiguraciji še vedno relativno varen, vendar potencialno ranljiv na slovarske in brute-force napade.

Pri omrežjih WPA3 praktičnega napada v okviru raziskave ni bilo mogoče izvesti zaradi časovnih omejitev projekta. Na podlagi pregleda literature in stanja tehnike velja WPA3 za trenutno najvarnejši Wi-Fi standard, saj uporablja napredno avtentikacijo SAE, ki bistveno otežuje napade z ugibanjem gesel in onemogoča klasično analizo handshake podatkov. Zaradi teh lastnosti se WPA3 v praksi pogosto obravnava kot praktično neizvedljivo razbijanje z uporabo tradicionalnih metod.

Pri Enterprise omrežjih je bilo ugotovljeno, da se povezava izvaja preko centralnega strežnika (RADIUS), kjer vsak uporabnik prejme lastniško uporabniško ime in geslo. Zaradi individualne avtentikacije in uporabe protokola 802.1X ni mogoče pridobiti uporabnih podatkov iz klasičnega handshake zajema, kar bistveno zmanjšuje možnost napadov na gesla in povečuje celotno varnost sistema.

Analiza je pokazala, da konfiguracije dostopnih točk v združljivostnih načinih, kot sta WPA/WPA2 (mixed mode) in WPA2/WPA3 (transition mode), lahko predstavljajo dodatno varnostno tveganje.

V primeru konfiguracije WPA/WPA2 lahko napadalec poskuša doseči, da se povezava vzpostavi prek protokola WPA, ki uporablja starejše kriptografske mehanizme in je bolj ranljiv za napade. Podobno lahko pri konfiguraciji WPA2/WPA3 napadalec povzroči, da se povezava vzpostavi z uporabo WPA2 namesto WPA3, s čimer postanejo ponovno uporabne napadalne metode, ki pri WPA3 niso več učinkovite.

Takšne konfiguracije sicer izboljšujejo združljivost naprav, vendar lahko zmanjšujejo dejansko raven varnosti omrežja. Zaradi tega se v sodobnih okoljih, kjer je to mogoče, priporoča uporaba izključno WPA2 ali WPA3 brez omogočenih združljivostnih načinov, saj s tem bistveno zmanjšamo možnost izrabe starejših varnostnih mehanizmov.

Pri interpretaciji rezultatov je treba upoštevati omejitve uporabljene strojne opreme. Uporabljena naprava Pwnagotchi na platformi Raspberry Pi Zero ter uporabljena USB antena podpirata zajem prometa predvsem v frekvenčnem pasu 2,4 GHz, medtem ko zajem podatkov iz dela omrežij, ki delujejo izključno v pasu 5 GHz, ni bil mogoč. Posledično praktični del testiranja napadov na WPA/WPA2 omrežja predstavlja predvsem stanje omrežij v pasu 2,4 GHz, kjer se pogosteje pojavljajo starejše ali kompatibilnostne konfiguracije.

Ta omejitev ne vpliva na statistični del analize razširjenosti varnostnih protokolov, lahko pa vpliva na obseg praktičnega testiranja odpornosti sodobnejših omrežij, ki uporabljajo novejše standarde brezžične komunikacije.

6. RAZPRAVA

6.1 Hipoteza 1: Omrežja, ki uporabljajo zastarele protokole (WEP, WPA), so bistveno bolj ranljiva za napade kot omrežja z WPA2 ali WPA3.

Rezultati laboratorijskega testiranja so pokazali, da je bilo mogoče zaščito WEP razbiti v nekaj minutah z analizo zajetega prometa, kar potrjuje njegovo popolno neustreznost za sodobno uporabo. Prav tako je analiza protokola WPA pokazala, da zaradi zastarelih kriptografskih mehanizmov in ranljivosti TKIP ne zagotavlja več zadostne ravni zaščite. Nasprotno pa je bilo pri WPA2 uspešno izvajanje napada odvisno predvsem od kompleksnosti gesla, medtem ko pri WPA3 klasični napadi na handshake podatke niso več učinkoviti.

HIPOTEZA POTRJENA

6.2 Hipoteza 2: Uporaba sodobnih usmerjevalnikov zmanjšuje varnostne ranljivosti Wi-Fi omrežij.

Kot je razvidno iz rezultatov praktičnega testiranja, so sodobnejši usmerjevalniki, ki delujejo tudi v frekvenčnem pasu 5 GHz, predstavljali dodatno oviro pri izvedbi napadov, saj uporabljena merilna oprema (Pwnagotchi in uporabljena antena) ni omogočala zajema handshake podatkov iz dela takšnih omrežij. To pomeni, da novejše konfiguracije omrežij in uporaba sodobnih naprav lahko povečajo odpornost omrežja že na ravni fizičnega in tehnološkega sloja, saj omejujejo možnosti prestrezanja prometa z osnovno ali nizkocenovno opremo.

To kaže, da sodobna strojna oprema in uporaba novejših standardov brezžične komunikacije zmanjšujeta praktično izvedljivost določenih napadov.

HIPOTEZA POTRJENA

6.3 Hipoteza 3: Večina analiziranih Wi-Fi omrežij uporablja neoptimalne varnostne nastavitve.

Kot je razvidno iz rezultatov (Tabela 1), velika večina analiziranih omrežij uporablja protokol WPA2, ki ob pravilni konfiguraciji in uporabi dovolj kompleksnega gesla še vedno predstavlja ustrezno raven zaščite. Zastareli protokoli, kot sta WEP in WPA, so bili zaznani le v zanemarljivem deležu ali pa sploh ne, kar kaže na postopno opuščanje neustreznih varnostnih nastavitev.

Čeprav je bilo zaznanih nekaj odprtih omrežij in konfiguracij v združljivostnih načinih, njihov delež ne predstavlja večine analiziranega okolja. Kot je razvidno iz rezultatov, večina omrežij uporablja protokol WPA2, dodatni delež pa tudi naprednejše zaščite, kot so WPA3 in Enterprise avtentikacija, ki zagotavljajo visoko raven zaščite. Na podlagi teh ugotovitev lahko ocenimo, da analizirano območje Velenja glede uporabe varnostnih nastavitev brezžičnih omrežij dosega razmeroma dobro oziroma optimalno raven osnovne varnosti.

HIPOTEZA ZAVRNJENA

7. NADALJNJE DELO IN IZBOLJŠAVE

7.1 POTENCIALNI RAZVOJ IN IZBOLJŠAVE

V nadaljnjem raziskovalnem delu bi bilo smiselno razširiti testiranje na širše geografsko območje ter vključiti več merilnih točk, kar bi omogočilo še natančnejšo analizo dejanskega stanja varnosti brezžičnih omrežij. Smiselna nadgradnja raziskave bi bila tudi uporaba naprednejše merilne opreme, ki podpira zajem prometa v frekvenčnem pasu 5 GHz in novejših standardih Wi-Fi (802.11ac/ax), saj bi s tem odpravili omejitve, zaznane pri praktičnem testiranju.

Dodatno bi bilo mogoče raziskavo razširiti z analizo vpliva različnih konfiguracij dostopnih točk, kot so izklop združljivostnih načinov (WPA/WPA2 ali WPA2/WPA3), uporaba ločenih omrežij za goste ter vpliv dolžine in kompleksnosti gesel na odpornost omrežja proti napadom. Nadaljnje delo bi lahko vključevalo tudi avtomatizirano dolgoročno spremljanje omrežij, kar bi omogočilo opazovanje sprememb varnostnih nastavitev skozi čas.

Pri prihodnjih meritvah bi bilo smiselno v merilni sistem vključiti tudi GPS modul, ki bi omogočal natančno beleženje lokacij zaznanih omrežij. Tak pristop bi omogočil kartografski prikaz razporeditve omrežij in njihove ravni zaščite ter s tem boljšo prostorsko ponazoritev varnosti brezžičnih omrežij na obravnavanem območju.

7.2 SMERNICE ZA PRAKTIČNO UPORABO

Na podlagi rezultatov raziskave je mogoče podati več priporočil za izboljšanje varnosti brezžičnih omrežij. Priporočljiva je uporaba sodobnih varnostnih protokolov, predvsem WPA2 ali WPA3 ter izklop zastarelih protokolov in združljivostnih načinov, ki lahko zmanjšajo dejansko raven zaščite omrežja. Pomembna je tudi uporaba dovolj kompleksnih gesel, ki bistveno zmanjšajo možnost uspešnih slovarskih ali brute-force napadov.

Organizacijam in posameznikom se priporoča redno posodabljanje programske opreme usmerjevalnikov, spremljanje povezanih naprav ter uporaba ločenih omrežij za goste, saj ti ukrepi dodatno zmanjšujejo možnost nepooblaščenega dostopa. V okoljih z večjim številom uporabnikov je priporočljiva tudi uporaba Enterprise rešitev z avtentikacijo preko centralnih strežnikov (npr. RADIUS), kar omogoča boljši nadzor dostopov in večjo varnost omrežja. S kombinacijo ustrezne konfiguracije, sodobne opreme in rednega nadzora je mogoče bistveno izboljšati splošno raven varnosti brezžičnih omrežij v lokalnem okolju.

8. ZAKLJUČEK

Raziskava je pokazala, da je splošna raven varnosti brezžičnih omrežij v analiziranem območju Šaleške doline razmeroma dobra, saj večina omrežij uporablja sodobne varnostne protokole, predvsem WPA2, medtem ko je uporaba zastarelih protokolov, kot sta WEP in WPA, skoraj popolnoma opuščena. Praktično testiranje je potrdilo, da so omrežja z zastarelimi protokoli bistveno bolj ranljiva, saj je bilo zaščito WEP mogoče razbiti v zelo kratkem času, medtem ko je bila uspešnost napadov na WPA2 odvisna predvsem od kompleksnosti gesla.

Rezultati so pokazali tudi, da uporaba sodobne strojne opreme in novejših standardov brezžične komunikacije zmanjšuje praktično izvedljivost določenih napadov, saj del novejših omrežij deluje v frekvenčnem pasu 5 GHz in uporablja naprednejše varnostne mehanizme. Kljub temu analiza konfiguracij kaže, da lahko nepravilne nastavitve, kot so združljivi načini ali uporaba šibkih gesel, še vedno predstavljajo pomemben dejavnik ranljivosti.

Treba je poudariti, da predstavljeni rezultati zajemajo le del možnih varnostnih preverjanj, saj obstaja še vrsta drugih potencialnih ranljivosti, povezanih z napačno konfiguracijo usmerjevalnikov, zastarelo programsko opremo, napadi na avtentikacijske mehanizme, socialnim inženiringom ter drugimi metodami testiranja, ki v tej raziskavi niso bile podrobneje obravnavane.

Stanje varnosti brezžičnih omrežij se postopno izboljšuje, vendar je dejanska raven zaščite še vedno močno odvisna od pravilne konfiguracije omrežij ter uporabe sodobnih protokolov.

9. POVZETEK

Danes se ljudje vse bolj zanašajo na brezžična omrežja, ki so pogosto tarča napadov in zlorab. Moja raziskovalna naloga se osredotoča na analizo varnosti Wi-Fi sistemov v Velenju, preučevanje njihovih ranljivosti, pogostih napadov ter učinkovitih zaščitnih mehanizmov. Pri raziskavi izvajam varnostne teste in simulacije napadov z namenom odkrivanja pomanjkljivosti v brezžičnih omrežjih. Cilj naloge je izboljšati razumevanje varnostnih tveganj Wi-Fi omrežij ter prispevati k večji kibernetski varnosti v Šaleški dolini.

10. ZAHVALA

Vesel sem, da sem z raziskovalno nalogo dosegel, večino stvari, ki sem si zadal. Najprej bi se rad zahvalil mentorjema Urošu Remenihu in Samu Železniku za vso pomoč, usmerjanje in podporo pri delu. Zahvaljujem se tudi bližnjim in družini za podporo skozi celoten proces raziskovalnega dela. Posebno zahvalo izražam učiteljici dr. Nataši Meh Peer za lektoriranje te raziskovalne naloge.

11. VIRI IN LITERATURA

[1] Huawei Technologies Co., Ltd., "WiFi Encyclopedia," [Elektronski]. Dostopno na: https://info.support.huawei.com/info-finder/encyclopedia/en/WiFi.html

[2] One World Rental, "History of WiFi – timeline of all WiFi generations," [Elektronski]. Dostopno na: https://oneworldrental.com/blog/history-of-wifi-timeline-of-all-wifi-generations-with-specs-details/

[3] TechTarget, "Wireless security & encryption basics: Understanding WEP, WPA and WPA2," [Elektronski]. Dostopno na: https://www.techtarget.com/searchnetworking/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2

[4] Cloudi-Fi, "WPA2/WPA3 Enterprise (802.1X)," [Elektronski]. Dostopno na: https://www.cloudi-fi.com/blog/wpa2-enterprise-802-1x

[5] SecureW2, "WPA3 vs WPA2," [Elektronski]. Dostopno na: https://www.securew2.com/blog/wpa3-vs-wpa2

[6] Alibaba, "RT5370 USB Wireless Network Card," [Elektronski]. Dostopno na: https://www.alibaba.com/product-detail/RT5370-USB-Wireless-Network-Card-Song_1601603758191.html

[7] Raspberry Pi Foundation, "Raspberry Pi Zero," [Elektronski]. Dostopno na: https://www.raspberrypi.com/products/raspberry-pi-zero/

[8] Mimovrste, "Linksys WRT54GL router," [Elektronski]. Dostopno na: https://www.mimovrste.com/usmerjevalniki-routerji/linksys-brezzicni-router-linksys-wrt54gl

[9] Mlacom, "TP-Link BE230 Wi-Fi 7 router," [Elektronski]. Dostopno na: https://www.mlacom.si/mrezna-oprema/usmerjevalniki/i_2986280_tp-link-be230-be3600-wi-fi-7-brezzicni-2-4-5ghz-usmerjevalnik-router-

dostopna-tocka

[10] NilTechEdu, "Python programming logo," [Elektronski]. Dostopno na: https://niltechedu.com/blog/shop/courses/corporate-python/

[11] Aircrack-ng Project, "Aircrack-ng Documentation," [Elektronski]. Dostopno na: https://www.aircrack-ng.org/

[12] Pwnagotchi Project, "Pwnagotchi Documentation," [Elektronski]. Dostopno na: https://pwnagotchi.ai/

[13] Hashcat, "Hashcat Password Recovery Tool," [Elektronski]. Dostopno na: https://hashcat.net/hashcat/

[14] Wireshark Foundation, "Wireshark," [Elektronski]. Dostopno na: https://www.wireshark.org

[15] Mawgoud, M., "Wireshark 101 – finding credentials in traffic," [Elektronski]. Dostopno na: https://mawgoud.medium.com/wireshark-101-finding-passwords-credentials-in-plain-text-traffic-0ec04ab0e014

[16] Beck, M., Tews, E., "Practical attacks against WEP and WPA," [Elektronski]. Dostopno na: https://www.researchgate.net/publication/220332983_Practical_attacks_against_WEP_and_WPA

[17] Hashcat, "cap2hashcat converter," [Elektronski]. Dostopno na: https://hashcat.net/cap2hashcat/

[18] Weakpass, “weakpass_4a wordlist,” [Elektronski]. Dostopno na: https://weakpass.com/wordlists?name=weakpass_4a

[19] Kristan test page (heatmap visualization), [Elektronski]. Dostopno na: http://kristantest.wuaze.com/?i=1

Priloga 1

Izjava avtorja naloge

Podpisan(a)_____Krsitan Blaž_____, maturant(ka) Elektro in računalniške šole Šolskega centra Velenje, programa____4.tra_____, izjavljam, da sem nalogo pripravil(a) samostojno pod vodstvom mentorja na šoli ter po virih, ki so navedeni v bibliografiji naloge.

Velenje, dne_____28.1.2026_____ Podpis:_____Kristan_____

Priloga 2

```
import subprocess
import json
import time
from datetime import datetime

SCAN_INTERVAL = 5
OUTPUT_FILE = "wifi_city_scan.json"

all_networks = {}

def scan_wifi():
    output = subprocess.check_output(
        ["netsh", "wlan", "show", "networks", "mode=bssid"],
        text=True,
        encoding="utf-8",
        errors="ignore"
    )

    ssid = auth = bssid = None

    for line in output.splitlines():
        line = line.strip()

        if line.startswith("SSID"):
            ssid = line.split(":", 1)[1].strip()

        elif line.startswith("Authentication"):
            auth = line.split(":", 1)[1].strip()

        elif line.startswith("BSSID"):
            bssid = line.split(":", 1)[1].strip()

        elif line.startswith("Signal"):
            signal = int(line.split(":", 1)[1].replace("%", "").strip())

            if not bssid:
                continue

            if bssid not in all_networks:
                all_networks[bssid] = {
                    "ssid": ssid,
                    "bssid": bssid,
                    "best_signal": signal,
                    "security": auth,
                    "first_seen": datetime.now().isoformat(),
                    "last_seen": datetime.now().isoformat()
```

```
                }
            else:
                all_networks[bssid]["last_seen"] = datetime.now().isoformat()
                if signal > all_networks[bssid]["best_signal"]:
                    all_networks[bssid]["best_signal"] = signal
                    all_networks[bssid]["ssid"] = ssid
                    all_networks[bssid]["security"] = auth

def save():
    data = {
        "last_update": datetime.now().isoformat(),
        "network_count": len(all_networks),
        "networks": sorted(
            all_networks.values(),
            key=lambda x: x["best_signal"],
            reverse=True
        )
    }

    with open(OUTPUT_FILE, "w", encoding="utf-8") as f:
        json.dump(data, f, indent=2, ensure_ascii=False)

    print(f"[OK] Updated {OUTPUT_FILE} | total: {len(all_networks)}")


if __name__ == "__main__":
    print("[*] Continuous city-wide Wi-Fi scan started")
    print("[*] Stop with PyCharm STOP button")

    while True:
        scan_wifi()
        save()
        time.sleep(SCAN_INTERVAL)
```

Priloga 3

```
import json
from collections import Counter

INPUT_FILE = "wifi_city_scan.json"
OUTPUT_FILE = "output_simplified.json"

with open(INPUT_FILE, "r", encoding="utf-8") as f:
    data = json.load(f)

networks = data.get("networks", [])
total_networks = len(networks)

security_counter = Counter()

for net in networks:
    sec = net.get("security", "UNKNOWN")
    security_counter[sec] += 1

security_stats = {}
for sec, count in security_counter.items():
    security_stats[sec] = {
        "count": count,
        "ratio": f"{count}/{total_networks}"
    }

simplified_networks = []

for net in networks:
    observations = net.get("observations", [])
    if not observations:
        continue

    max_signal = max(obs["signal"] for obs in observations)
    best_obs = next(obs for obs in observations if obs["signal"] ==
max_signal)

    simplified_networks.append({
        "ssid": net.get("ssid"),
        "bssid": net.get("bssid"),
        "security": net.get("security"),
        "signal": best_obs["signal"],
        "lat": best_obs["lat"],
        "lon": best_obs["lon"],
        "time": best_obs["time"]
    })
```

```
output = {
    "last_update": data.get("last_update"),
    "total_networks": total_networks,
    "security_statistics": security_stats,
    "networks": simplified_networks
}

with open(OUTPUT_FILE, "w", encoding="utf-8") as f:
    json.dump(output, f, indent=2)

print("Končano.")
print("Statistika omrežij:")
for sec, info in security_stats.items():
    print(f"  {sec}: {info['ratio']}")
```

Priloga 4

http://kristantest.wuaze.com/