OŠ Livada Velenje
Efenkova 60, 3320 Velenje

MLADI RAZISKOVALCI ZA RAZVOJ SAŠA REGIJE

RAZISKOVALNA NALOGA

Etično hekanje

Tematsko področje: elektrotehnika, elektronika in robotika

Avtor:
Taj Remenih, 8. razred

Mentorja:
Boris Bubik, prof.
Uroš Remenih, inž. inf.

Velenje, 2026

Raziskovalna naloga je bila opravljena na Osnovni šoli Livada Velenje.

Mentorja: Boris Bubik, prof.,

Uroš Remenih, inž. inf.

Datum predstavitve: marec 2026

KLJUČNA DOKUMENTACIJSKA INFORMACIJA

ŠD Osnovna šola Livada, šolsko leto 2025/2026

KG Flipper zero

AV REMENIH, Taj

SA BUBIK, Boris / REMENIH, Uroš

KZ 3320 Velenje, Efenkova cesta 60

ZA Osnovna Šola Livada Velenje

LI 2026

IN **Etično hekanje**

TD Raziskovalna naloga

OP X, 34 str., 1 pregl., 0 graf, 25 sl., 2 pril., 12 vir.

IJ SL

JI sl / en

AI Hekanje pomeni vdor ali poseganje v računalniške sisteme, omrežja in programe, največkrat z namenom dostopa do podatkov, spreminjanje delovanja sistema in odkrivanje njegovih slabosti. Toda je to dejanje nedovoljeno, v nekaterih primerih tudi kriminalno. Etično hekanje, ki sem ga jaz uporabil, je varnostno testiranje ranljivosti računalniškega sistema z dovoljenjem. V tej nalogi sem v ta namen uporabil naprava Flipper Zero, ki uporablja različne signale v namen pridobivanja podatkov različnih tehnologij in aparatov. S pomočjo različnih signalov sem preverjal, če je možno krmiliti naprave brez daljinskega upravljalnika, opravljati semafor in dobiti geslo Wi-Fi omrežja. Naloga mi je odgovorila na različna vprašanja na tem področju, ki sem jih že nekaj časa gledal na videoposnetkih in na socialnih omrežjih.

KEY WORDS DOCUMENTATION

ND Osnovna šola Livada, šolsko leto 2025/2026
CX Flipper zero
AU REMENIH, Taj
AA BUBIK, Boris / REMENIH, Uroš
PP 3320 Velenje, Efenkova cesta 60
PB Osnovna Šola Livada Velenje
PY 2026
TI **Ethical hacking**
DT Research work
NO X, 34 p., 1 tab., 0 graf, 25 fig., 2 ann., 12 ref.
LA SL
AL sl / en

AB Hacking means breaking into or interfering with computer systems, networks, and programs, usually to access data, change how a system works, or find its weaknesses. This behavior is often unauthorized and can be illegal. Ethical hacking, which I used in this project, means testing computer systems with permission to find security weaknesses. In this project, I used a device called Flipper Zero, which can use different signals to collect data from various devices and technologies. With these signals, I tested whether it is possible to control devices without a remote control, control traffic lights, and get a Wi-Fi password. This project helped me answer questions about this topic that I had been curious about from videos and social media.

KAZALO VSEBIN

1 UVOD 1

1.1 HIPOTEZE 1

2 PREGLED OBJAV 2

2.1 FLIPPER ZERO 2

2.1.1 OPIS NAPRAVE 2

2.1.2 TEHNIČNE LASNOSTI 3

2.2 OPIS UPORABLJENIH TEHNELOGIJ 4

2.2.1 RADIOFREKVENČNA IDENTIFIKACIJA (RFID) 4

2.2.2 NFC 4

2.2.3 SUB-1 GHZ 5

2.2.4 INFRARDEČA KOMUNIKACIJA (IR) 6

2.2.5 IBUTTON 6

2.2.6 WI-FI 6

2.2.7 PRIMERJAVA TEHNIČNIH LASTNOSTI 6

2.2.8 SEMAFORJI 7

3 MATERIAL IN METODE DELA 9

3.1 APLIKACIJA 9

3.2 OPIS DELA 11

3.2.1 WI-FI GESLO 11

3.2.2 KRMILJENJE NAPRAV 16

3.2.3 SEMAFORJI 19

4 REZULTATI 23

4.1 PRIDOBIVANJE WI-FI GESLA 23

4.1.1 TEŽAVE PRI PRIDOBIVANJU GESLA 24

4.2 IR DALJINEC 25

4.3 BARVE NA SEMAFORJIH 25

4.3.1 DELOVANJE KOMUNIKACIJE SEMAFORJEV ..... **NAPAKA! ZAZNAMEK NI DEFINIRAN.**

5 RAZPRAVA 27

6 POVZETEK 29

7 ZAKLJUČEK 30

8 ZAHVALA 31

9 PRILOGE ..... **NAPAKA! ZAZNAMEK NI DEFINIRAN.**

10 VIRI IN LITERATURA 34

KAZALO SLIK

Slika 1: Flipper Zero 2
Slika 2: Logo aplikacije 9
Slika 3: Prvi pogled aplikacije 9
Slika 4: Domači zaslon aplikacije 10
Slika 5: List tehničnih lastnosti 10
Slika 6: Možne posodobitve 10
Slika 7: Shranjeni programi 11
Slika 8: Upravljanje flipperja 11
Slika 9: Wi-Fi module 12
Slika 10: Gumb za skeniranje na Flipper zaslonu 12
Slika 11: Seznam omrežji 13
Slika 12: Izbira omrežja 13
Slika 13: Gumb za zbiranje podatkotkov omrežja 14
Slika 14: Preglednica brez gesla 14
Slika 15: Preglednica z najdenim geslom 15
Slika 16: Izbira aplikacije 16
Slika 17: Znotraj aplikacije 16
Slika 18: Notranje izbire 17
Slika 19: Možnost krmiljenja televizije 17
Slika 20: Prižig televizije 18
Slika 21: Elektro omarica 20
Slika 22: Deli elektro omarice 20
Slika 23: Moduli in releji ..... **Napaka! Zaznamek ni definiran.**
Slika 24: Stikalo za prižig/izklop ..... **Napaka! Zaznamek ni definiran.**
Slika 25: Onlinehashcrack.com 24

KAZALO PRILOG

PRILOGA 1: ZEMLJEVID SEMAFORIZIRANEGA KRIŽIŠČA..... 33

PRILOGA 2: GRAF INTERVALA PRIŽGANIH BARV NA SEMAFORJU**NAPAKA! ZAZNAMEK NI DEFINIRAN.**

SEZNAM OKRAJŠAV IN SIMBOLOV

angl. – angleško

GPIO – general purpose input/output

NFC – near-field communication (*slov.* komunikacija s sosednjim poljem)

USB – univerzalno serijsko vodilo (*angl*. universal serial bus)

HDMI – high-definition multimedia interface

ID – identifier

RFID – radiofrekvenčna identifikacija (*angl*. radio frequency identification)

IR – infrardeč signal

WI-FI – tehnologija za brezžični prenos podatkov (internet) med napravami.

WEP – wired equivalent privacy (zasebnost enakovredna žični povezavi)

WPA – Wi-Fi protected access (zaščiten dostop do Wi-Fi)

WPA2 – Wi-Fi protectet access 2 (zaščiten dostop do Wi-Fi (2. verzija))

WPA3 – Wi-Fi protected access 3 (zaščiten dostop do Wi-Fi (3. verzija))

1 UVOD

Ko sem na spletni strani YouTube, družbenem omrežju TikToku in drugih omrežjih večkrat videl napravo Flipper Zero (v nadaljevanju Flipper Zero), se mi je zdela zelo zanimiva. V videoposnetkih so govorili, da lahko z njo dobiš gesla za Wi-Fi, spreminjaš delovanje semaforja, upravljaš naprave na daljinski upravljalnik in celo vklapljaš ali izklapljaš kamere. Zato sem se začel spraševati, koliko od tega je sploh res in ali je ta naprava res tako zmogljiva, kot pravijo na internetu.

Potem sem dobil idejo, da bi bila to izvrstna tema za raziskovalno nalogo. O tem sem se pogovoril z mentorjema in skupaj smo se odločili, da jo naročim in preizkusim. Ko je naprava prispela, sem si najprej postavil nekaj hipotez o tem, kaj vse zmore. Nato sem jo predstavil še mentorjema in začel raziskovati njene funkcije. Tako sem se lotil dela in začel ugotavljati, kaj od tega, kar sem videl na internetu, dejansko drži in kaj ne.

1.1 HIPOTEZE

1. hipoteza: Flipper Zero lahko krmili napravo, ki deluje na daljinski upravljalnik.

2. hipoteza: Flipper Zero lahko spreminja barvo na semaforju.

3. hipoteza: Flipper Zero lahko dobi geslo Wi-Fi omrežja.

2 PREGLED OBJAV

2.1 FLIPPER ZERO

2.1.1 OPIS NAPRAVE

Flipper Zero je majhna elektronska naprava, ki lahko opravlja veliko različnih nalog. Uporabljamo jo preko majhnega zaslona in gumbov na napravi. Na njej je že nameščenih veliko aplikacij, ki omogočajo različne funkcije. Poleg tega lahko nanjo naložimo tudi dodatne programe in orodja, s katerimi lahko napravo še bolj prilagodimo in razširimo njene možnosti.

Slika 1: Flipper Zero

2.1.2 TEHNIČNE LASNOSTI

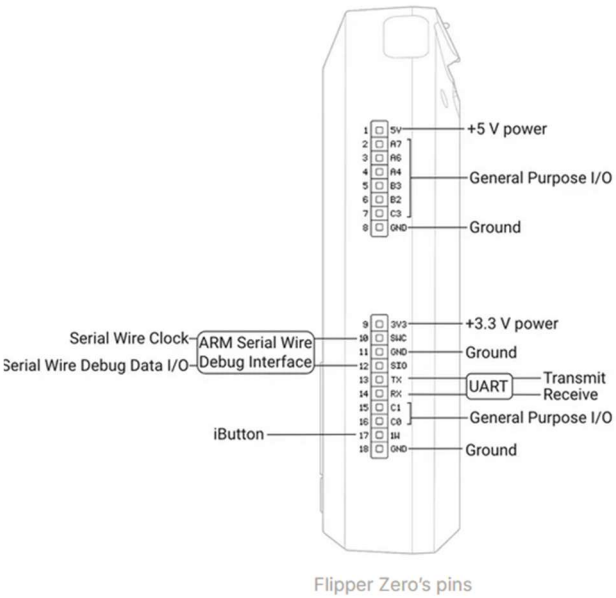
Velikost: naprava je visoka približno 4 cm in široka okoli 10 cm, tehta približno 102 g. Zaradi svoje velikosti je priročna za držanje v roki in prenašanje.

Ekran: ima zaslon velikosti približno 16 × 32 mm z ločljivostjo 128 × 64 pikslov. Gre za LED/LCD zaslon, ki omogoča prikaz menijev, podatkov in upravljanje naprave.

Mikrokrmilna enota: uporablja 32-bitni mikrokrmilnik ARM Cortex-M4. Podpira Bluetooth LE 5.4 in brezžične protokole ter ima približno 256 KB pomnilnika za delovanje in shranjevanje podatkov.

Flipper Zero podpira več različnih tehnologij in dodatkov, zato je zanimiv za raziskovanje elektronike. Omogoča SUB-1 GHz komunikacijo, NFC in RFID 125 kHz ter infrardeči signal (IR) za upravljanje nekaterih naprav. Z dodatnim modulom lahko uporablja tudi Wi-Fi.

Ima tudi GPIO vtič za priklop dodatnih modulov in lahko bere iButton podatke. Zaradi teh funkcij je uporaben za učenje o tehnologiji in delovanju različnih elektronskih naprav.



Slika 2: Predstavitev GPIO vtičev

Flipper Zero za shranjevanje podatkov potrebuje Micro SD kartico. Za polnjenje in povezavo z računalnikom uporablja USB-C priključek. Naprava ima vgrajena tudi zvočnik in vibracijski motor, ki uporabnika obveščata o delovanju in različnih dogodkih.

Flipper Zero ima veliko dodatkov, ki jih lahko priklopimo nanj. Eden izmed njih je Wi-Fi modul, ki sem ga uporabil tudi v svoji raziskovalni nalogi. Obstajajo pa še drugi dodatki, ki napravo še bolj razširijo.

Wi-Fi moduli omogočajo, da se Flipper Zero poveže z brezžičnim omrežjem. Sam Flipper Zero nima vgrajenega Wi-Fi-ja, zato se uporablja zunanji modul, ki se priklopi preko GPIO priključka ali USB-ja. Najpogosteje temeljijo na ESP8266 ali ESP32 mikrokontrolerjih in omogočajo povezavo z internetom, posodabljanje naprave ter različne omrežne raziskave.

Glavni namen Wi-Fi modulov je razširiti funkcionalnost naprave. Z njimi lahko Flipper Zero povežemo z računalnikom ali telefonom, ga upravljamo na daljavo in se učimo, kako delujejo Wi-Fi omrežja in brezžične povezave. Uporabljajo se predvsem v izobraževalne in raziskovalne namene ter za razumevanje delovanja sodobnih tehnologij.

2.2 OPIS UPORABLJENIH TEHNOLOGIJ

2.2.1 RADIOFREKVENČNA IDENTIFIKACIJA (RFID)

RFID je tehnologija, ki deluje s pomočjo radijskih valov. Uporablja se za prepoznavanje in sledenje predmetom ali oseb brez neposrednega stika. To pomeni, da kartice ali obeska ni treba vstaviti v napravo, ampak ga samo približamo čitalniku.

RFID kartica vsebuje majhen čip, ki oddaja posebno kodo. Vsaka kartica ima svojo edinstveno kodo, po kateri jo sistem prepozna. Čitalnik to kodo prebere in nato dovoli ali zavrne dostop. RFID se pogosto uporablja za vstop v stavbe, v šolae, hotelske sobe ali za odpiranje vrat.

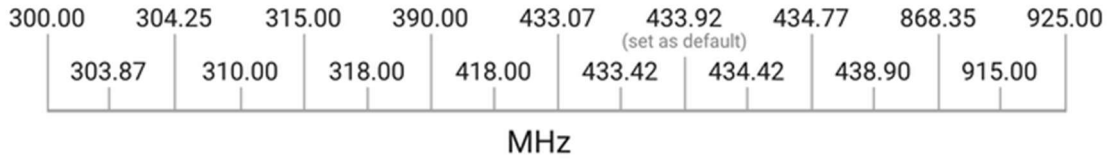
2.2.2 NFC

NFC pomeni komunikacijo bližnjega polja (Near Field Communication). To je tehnologija, ki omogoča, da telefoni, tablice in druge naprave brezžično izmenjujejo podatke na zelo kratki razdalji. Da deluje, morata biti napravi zelo blizu skupaj, navadno le nekaj centimetrov.

NFC se je razvil iz tehnologije RFID, ki jo uporabljamo pri karticah za odpiranje vrat, evidenci delovnega časa in brezstičnih plačilnih karticah. NFC je nadgradnja te tehnologije, ker ne omogoča samo branja podatkov, ampak tudi dvosmerno komunikacijo med napravami. To pomeni, da lahko z njim plačujemo s telefonom ali hitro prenašamo podatke med napravami.

2.2.3 SUB-1 GHZ

SUB-1 GHz pomeni radijske frekvence pod 1 GHz. Flipper Zero uporablja frekvence približno med 300 in 925 MHz. Te frekvence se uporabljajo za brezžično komunikacijo med različnimi napravami, na primer daljinci za garažna vrata, brezžična stikala, vremenski senzorji in drugi pametni senzorji.



Slika 3: Frekvenčni razpon

Glavna prednost SUB-1 GHz je dolg doseg signala. Na odprtem prostoru lahko signal doseže tudi več kilometrov. Ti signali se dobro širijo skozi ovire, kot so stavbe, drevesa in tla, zato so primerni za uporabo na večjih razdaljah. Poleg tega porabijo malo energije, kar pomeni, da ima naprava dolgo dobo delovanja na baterijo.

2.2.4 INFRARDEČA KOMUNIKACIJA (IR)

Infrardeči signal uporablja elektromagnetno sevanje v infrardečem spektru, ki je tik pod vidno svetlobo. S prostim očesom ga ne vidimo, vendar ga naprave lahko zaznajo.

Ta tehnologija se najpogosteje uporablja v daljinskih upravljalnikih za televizijo, klimatske naprave, projektorje in druge naprave, ki jih upravljamo na daljavo. Z infrardečim signalom lahko pošiljamo ukaze napravam, na primer za vklop, izklop ali spreminjanje nastavitev.

2.2.5 IBUTTON

iButton je posebna tehnologija za identifikacijo, ki se uporablja za shranjevanje osebnih ali tehničnih podatkov. Najpogosteje se uporablja za odpiranje vrat, nadzor dostopa ali evidenco delovnega časa v podjetjih in šolah.

Deluje tako, da se iButton dotakne čitalnika in ta prebere njegovo edinstveno kodo. Uporablja protokol 1-Wire, kar pomeni, da za prenos podatkov in napajanje potrebuje samo eno podatkovno linijo in maso. Nekateri iButtoni se napajajo kar preko čitalnika, drugi pa imajo vgrajeno tudi majhno baterijo.

2.2.6 WI-FI

Wi-Fi je brezžična tehnologija, ki omogoča povezavo naprav v omrežje brez kablov. Uporabljamo ga za dostop do interneta ter povezovanje računalnikov, telefonov in drugih pametnih naprav. Deluje po standardih IEEE 802.11 in omogoča hiter prenos podatkov.

Wi-Fi deluje na frekvencah 2,4 GHz, 5 GHz in 6 GHz. Frekvenca 2,4 GHz ima večji doseg, vendar nižjo hitrost, medtem ko frekvenca 5 GHz omogoča večje hitrosti na krajši razdalji. 6 GHz je novejša tehnologija z zelo visokimi hitrostmi in manj motnjami.

Za zaščito Wi-Fi omrežij se uporabljajo različni načini varnosti, kot so WEP, WPA, WPA2 in WPA3. V šolah in podjetjih se pogosto uporabljajo tudi naprednejše zaščite z uporabniškim imenom, geslom ali posebnimi certifikati, kar omogoča večjo varnost in nadzor nad omrežjem.

2.2.7 PRIMERJAVA TEHNIČNIH LASTNOSTI

Tehnologija	Hitrost	Doseg	Poraba energije
IR	nizka	zelo kratek	zelo nizka
iButton	zelo nizka	dotik	minimalna
Sub-1 GHz	nizka	zelo dolg	zelo nizka
Wi-Fi	zelo visoka	srednja	visoka

Tabela 1: Primerjava tehničnih lastnosti

2.2.8 SEMAFORJI

Semaforji so naprave v prometu, ki z lučmi uravnavajo promet. Uporabljajo tri osnovne barve: rdečo, rumeno in zeleno. Njihov glavni namen je, da povečajo varnost na cesti, omogočijo bolj tekoč promet in preprečijo prometne nesreče.

Delujejo na elektriko in danes večinoma uporabljajo LED luči, ki imajo življenjsko dobo tudi do 50.000 ur. Dobro so vidni podnevi in ponoči ter veljajo za zelo zanesljive prometne naprave.

Semafor je del večjega prometnega sistema. Sestavljajo ga luči, krmilnik (nekakšen majhen računalnik), senzorji in povezave z drugimi semaforji. Krmilnik določa, kdaj se katera luč prižge in koliko časa sveti.

Poznamo več vrst semaforjev: za avtomobile, za pešce z gumbi, pametne semaforje, ki se prilagajajo prometu, ter semaforje za avtobuse ali vlake. Promet zaznavajo s senzorji v cesti, kamerami, radarji ali gumbi za pešce.

2.2.9 GPIO VTIČ

GPIO vtič na napravi Flipper Zero omogoča povezovanje z drugimi elektronskimi napravami in moduli. GPIO pomeni »General Purpose Input/Output«, kar pomeni splošni vhodno-izhodni priključek. Preko tega vtiča lahko napravo povežemo z različnimi senzorji, moduli ali drugimi elektronskimi komponentami.

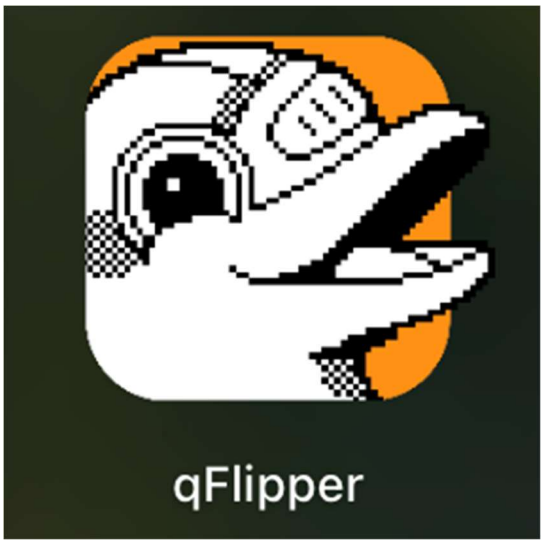
Z uporabo GPIO vtiča lahko na Flipper Zero priklopimo dodatke, kot so Wi-Fi moduli, LED lučke, tipke, senzorji ali druge razvojne plošče. To omogoča, da napravo uporabljamo tudi za učenje elektronike in programiranja.

GPIO vtič je zelo uporaben pri raziskovanju, saj lahko z njim preizkušamo delovanje različnih elektronskih vezij in naprav. Zaradi tega je Flipper Zero primeren za izobraževanje in spoznavanje delovanja sodobne tehnologije.

3 MATERIAL IN METODE DELA

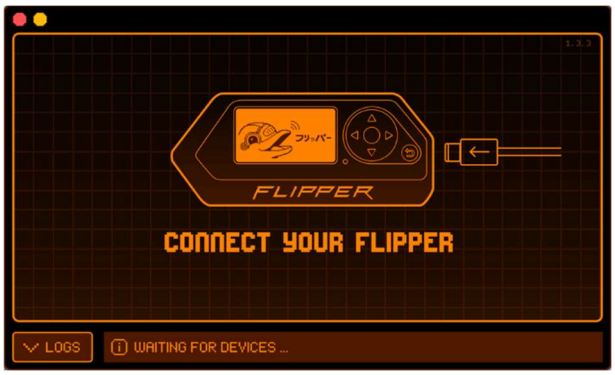
3.1 APLIKACIJA

Uporabil sem izvirno aplikacijo s Flipper Zero spletne strani. Imenuje se qFlipper.



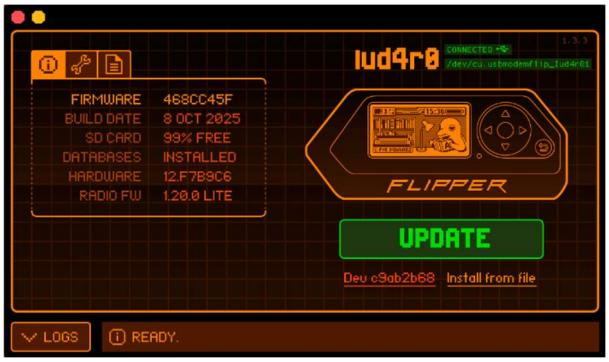
Slika 4: Logo aplikacije

Ko odpreš aplikacijo, se ti pokaže okence, na katerem piše, da moraš priklopiti svoj Flipper s kablom na računalnik.



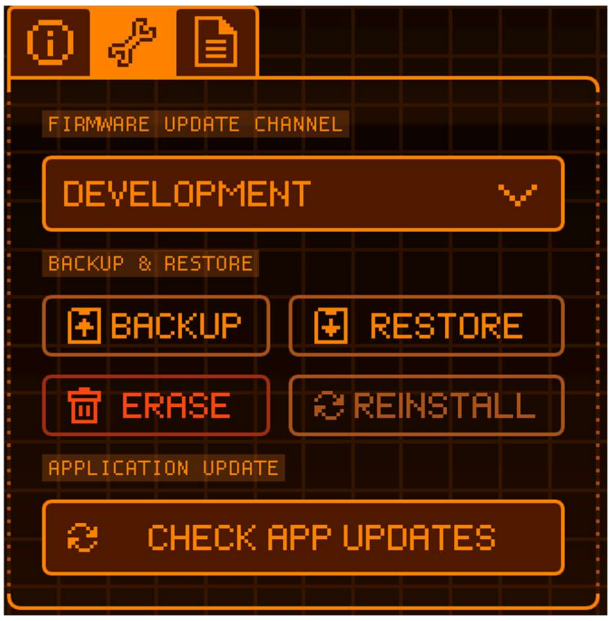
Slika 5: Prvi pogled aplikacije

Ko se računalnik in Flipper Zero povežeta, dobimo dostop do aplikacije, kjer lahko vidimo tehnične lastnosti naprave, preverimo posodobitve in upravljamo shranjene programe. V aplikaciji lahko dodajamo tudi nove programe, brišemo stare ter spremljamo delovanje naprave.



Slika 6: Domači zaslon aplikacije

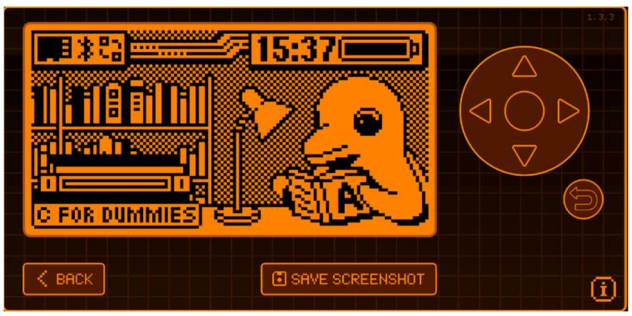
Slika 7: List tehničnih lastnosti



Slika 8: Možne posodobitve

Slika 9: Pomnilniki, ki so na voljo

Preko aplikacije na računalniku lahko spremljamo zaslon naprave Flipper Zero in jo tudi upravljamo na daljavo. To omogoča lažje delo, saj lahko vse funkcije vidimo neposredno na računalniku in napravo upravljamo brez uporabe gumbov na njej.

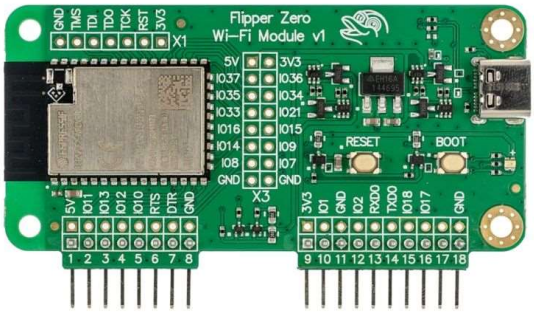


Slika 10: Upravljanje flipperja

3.2 OPIS DELA

3.2.1 WI-FI GESLO

Začel sem raziskovati. Ves čas mi je bilo zelo zanimivo in zabavno, saj me elektronika zelo zanima. Poleg naprave Flipper Zero sem naročil še Wi-Fi devboard modul, saj brez njega ne bi mogel uporabljati vseh funkcij, povezanih z Wi-Fi omrežji. Ta dodatek omogoča, da naprava zaznava in analizira brezžična omrežja ter izvaja dodatne funkcije, povezane z Wi-Fi komunikacijo.



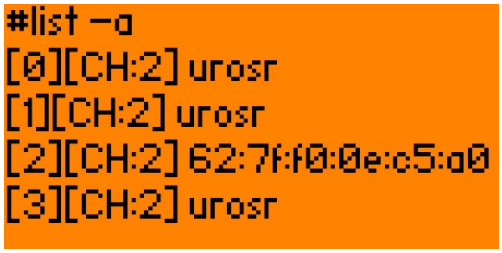
Slika 11: Wi-Fi modul

Wi-Fi modul sem priklopil na GPIO vtič na vrhu naprave Flipper Zero. Na vrhu naprave je priključek z več majhnimi luknjicami, kamor se vstavi Wi-Fi devboard. Ko je modul pravilno priklopljen, omogoča uporabo dodatnih funkcij, povezanih z Wi-Fi omrežji.

Aplikacije za Wi-Fi še nisem imel nameščene, zato sem odprl spletno stran lab.flipper.net (Flipper Lab), kjer lahko na napravo naložimo različne aplikacije in dodatke. Ko sem aplikacijo uspešno namestil, sem priključil Wi-Fi modul in začel raziskovati njegovo delovanje.

V aplikaciji sem najprej izbral možnost »SCAN ALL«, ki omogoča skeniranje Wi-Fi omrežij v okolici. Na zaslonu so se prikazala zaznana omrežja in IP naslov. Skeniranje sem pustil delovati približno pet minut, da je naprava zaznala čim več omrežij v bližini.

Slika 12: Gumb za skeniranje na Flipper zaslonu



Slika 13: Seznam omrežij

Za raziskovanje sem uporabil naše domače Wi-Fi omrežje. Ko je naprava končala skeniranje, je bil seznam zelo dolg, saj je zaznala približno 50 različnih omrežij. To pomeni, da lahko zazna omrežja tudi širše v okolici in ne samo v bližini.

Na zaslonu so se ob vsakem zaznanem omrežju pojavile številke. Te številke so pomenile zaporedno številko omrežja na seznamu. Zapomniti sem si moral številko našega omrežja, ker sem jo potreboval v naslednjem koraku, kjer sem izbral omrežje, ki sem ga želel podrobneje raziskati.

Slika 14: Izbira omrežja

V aplikaciji sem lahko izbiral med različnimi orodji, ki jih ponuja Wi-Fi modul. Med njimi so bila na primer »Join«, »Attack«, »Wardrive«, »Evil portal« in »Beacon spam«. Jaz sem izbral orodje z imenom »SNIFF«, ker omogoča branje in zbiranje podatkov o izbranem Wi-Fi omrežju.

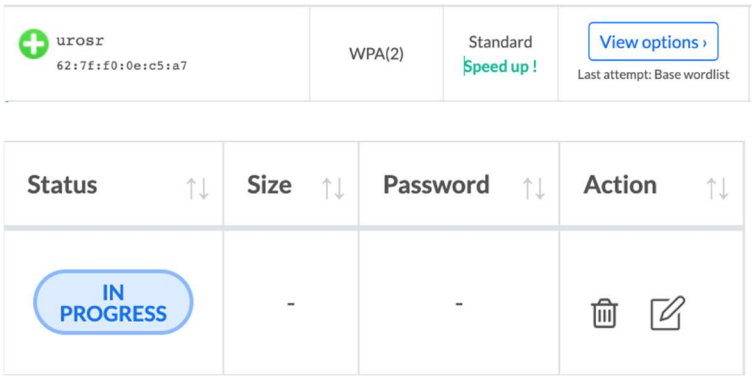
V tem načinu je bilo na voljo še več različnih možnosti, kot so »Beacon«, »Deauth«, »Probe«, »Raw«, »BT«, »Airtag« in druge. Za svojo raziskavo sem izbral možnost »PMKID«, saj omogoča zbiranje osnovnih podatkov o omrežju, ki se uporabljajo za nadaljnjo analizo in razumevanje delovanja Wi-Fi povezave.

Slika 15: Gumb za zbiranje podatkotkov omrežja

Podatke je naprava zbirala kar dolgo časa. Medtem ko sem čakal, sem si ogledal nekaj videoposnetkov na internetu, ker nisem točno vedel, kako nadaljevati. Tam sem izvedel, kako lahko iz shranjene datoteke preberem podatke o omrežju. To sem poskusil narediti na spletni strani onlinehashcrack.com.

OnlineHashCrack je spletna stran, ki omogoča analizo hash vrednosti gesel. Uporabnik lahko naloži datoteko z zbranimi podatki, stran pa poskuša s pomočjo velikih baz gesel in zmogljivih strežnikov ugotoviti izvirno geslo. Takšne strani se pogosto uporabljajo za varnostno testiranje in učenje o zaščiti omrežij.

Najprej sem več tednov poskušal naložiti datoteko, vendar mi je vedno napisalo, da je napačna. Ko sem poskusil ponovno, sem opazil drugo okno za oddajo datoteke in ga preizkusil. Takrat je končno pisalo »IN PROGRESS«, kar je pomenilo, da se je analiza začela. Nato se je prikazala razpredelnica z rezultati, ki jo prikazuje spodnja slika.

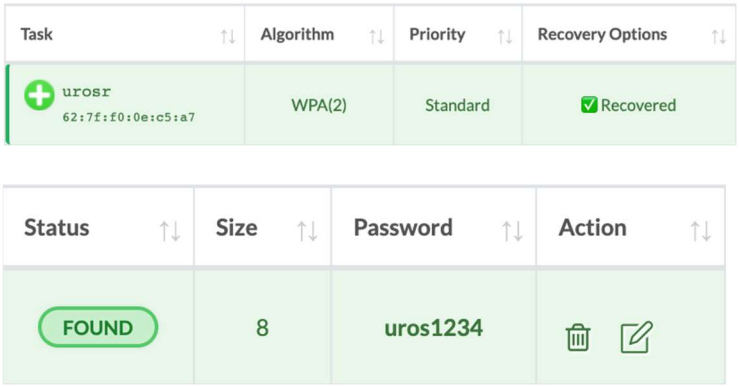


Slika 16: Preglednica brez gesla

Pisalo je, da bo za iskanje kode potrebovalo približno 1–2 dni. Po približno 20 urah čakanja sem ponovno odprl računalnik in preveril, kako napreduje postopek. In res je delovalo.

V razpredelnici se je pojavil stolpec z napisom »Password«, kjer je bilo zapisano geslo našega domačega Wi-Fi omrežja, to geslo smo predhodno nastavili na usmerjevalniku,

tako da smo takoj vedeli, če ga je aplikacija prepoznala. Tako sem ugotovil, da je bila analiza uspešna in da je naprava pravilno zbrala podatke za raziskavo.



Slika 17: Preglednica z najdenim geslom

Bil sem zelo vesel in hkrati presenečen, da je to res mogoče. Zato sem si želel še bolj podrobno pogledati postopek oz. delovanje, da ga lahko razumem in razložim. Ugotovil sem, da PCAP datoteka, ki sem jo uporabil, ne vsebuje gesla. To je moje zanimanje, kako sistem kljub temu pride do pravega rezultata, še poglobilo.

Postopek deluje tako, da iz PCAP datoteke prebere ime omrežja (SSID), MAC naslov dostopne točke, MAC naslov naprave ter tako imenovani WPA handshake. WPA handshake je zapis, ki nastane, ko se naprava poskuša povezati v Wi-Fi omrežje. Sam po sebi ne vsebuje gesla, ampak je dokaz, da je do povezovanja prišlo.

Ko se naprave ponovno povezujejo v omrežje, se ustvari ta handshake, ki ga lahko naprava zajame in shrani. V datoteki so nato shranjeni podatki o omrežju, ki se lahko uporabijo za analizo varnosti in delovanja Wi-Fi omrežij v raziskovalne in izobraževalne namene.

Sistem nato uporablja hash vrednosti. Hash je posebna kriptografska vrednost, ki nastane iz gesla. Če je geslo pravilno, se izračunani hash ujema s tistim iz datoteke. Program poskuša različna možna gesla in izračuna njihove hash vrednosti. Ko se hash ujema s shranjenim hashom, to pomeni, da je bilo geslo pravilno. Na ta način je mogoče preveriti geslo, ne da bi bilo neposredno zapisano v datoteki.

3.2.2 KRMILJENJE NAPRAV

Tukaj sem preizkušal upravljanje naprav, ki delujejo preko IR (infrardečega) daljinskega upravljalnika. Pri tem nisem potreboval nobenih dodatnih modulov, kot sem jih pri raziskovanju Wi-Fi omrežij. Odločil sem se, da bom najprej preizkusil televizor.

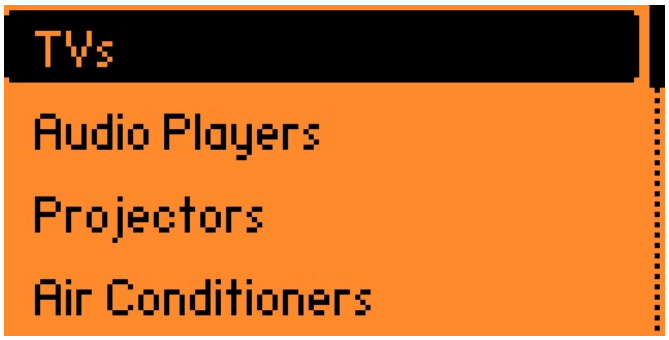
Flipper Zero sem priklopil na računalnik in v programu qFlipper preveril, kaj vse naprava že omogoča in ali potrebujem kakšno dodatno aplikacijo. Ugotovil sem, da ima Flipper Zero že nameščeno aplikacijo INFRARED. Ta aplikacija omogoča, da napravo uporabljamo kot univerzalni daljinski upravljalnik za različne naprave, ki delujejo z infrardečim signalom.

Slika 18: Izbira aplikacije

Znotraj aplikacije je bilo na voljo veliko različnih okenc, v katerih sem imel možnost že shranjenih signalov, možnost prebrati in shraniti lasten signal ter tudi nastavitve, na katerih lahko spreminjamo lastnosti signalov.

Slika 19: Znotraj aplikacije

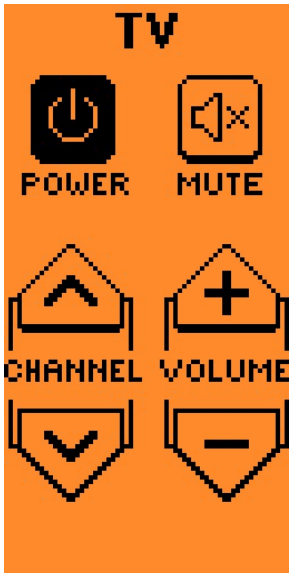
Za začetek sem izbral že shranjene signale in raziskoval, kaj lahko z njimi storim. V tem okencu so bili shranjeni daljinski upravljalniki za televizor, radio, projektor in klimo. Kliknil sem na signale televizorja.



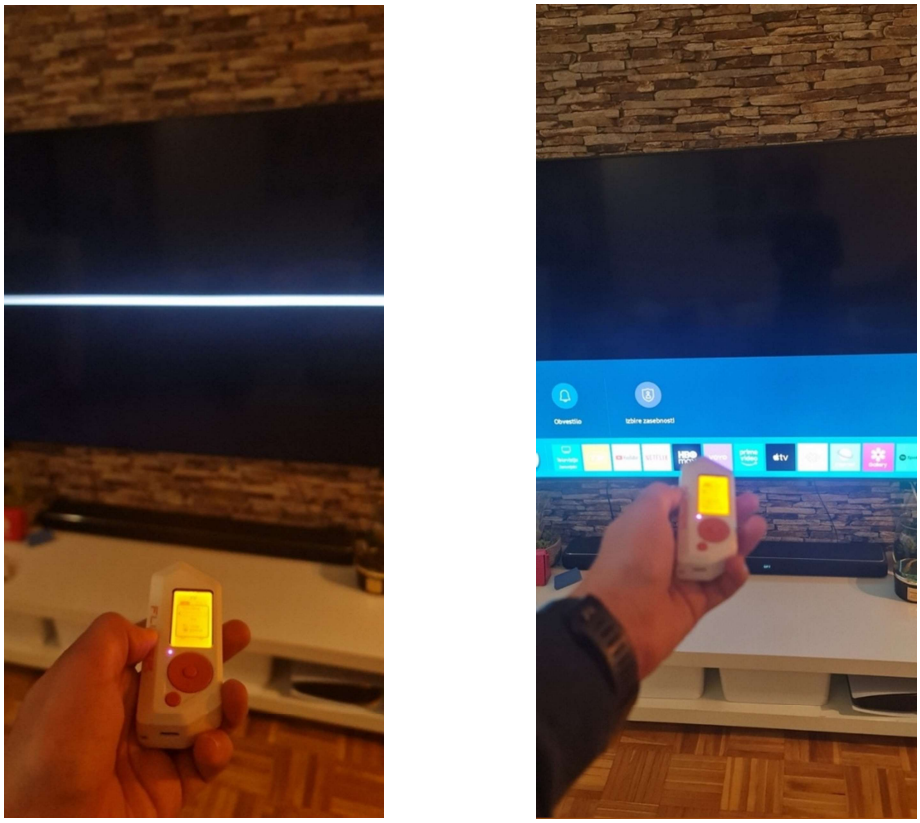
Slika 20: Notranje izbire

Naprava je potrebovala nekaj časa, da je naložila obliko daljinca na zaslon Flipper Zero. Ko se je prikazal daljinec, sem imel na zaslonu več možnosti: vklop in izklop televizije, povečanje in zmanjšanje glasnosti, izklop zvoka ter menjavo kanalov.

Za začetek sem preizkusil samo vklop televizije in opazoval, kaj se bo zgodilo. Po približno petih sekundah se je televizija res prižgala. Bil sem zelo presenečen in hkrati zelo vesel, da je naprava dejansko delovala in uspela prižgati televizor.



Slika 21: Možnost krmiljenja televizije



Slika 22: Vklop televizije

Nekaj časa sem se igral s televizorjem, nato pa sem poskusil prebrati še lasten IR signal, in sicer gumb za OK na daljincu. Naprava je signal uspešno prebrala in mi ponudila možnost, da ga uporabim ali shranim. Najprej sem signal shranil v pomnilnik naprave, nato pa sem ga lahko tudi ponovno predvajal.

Na Flipper Zero se to naredi tako, da v meniju izberemo možnost za infrardeče signale (Infrared) in nato izberemo učenje novega signala. Daljinec usmerimo proti napravi in pritisnemo gumb, ki ga želimo kopirati. Flipper Zero signal zazna, ga prebere in shrani v svojo knjižnico.

Ko je signal shranjen, ga lahko kasneje izberemo s seznama shranjenih signalov in ponovno pošljemo. Tako lahko naprava posnema delovanje pravega daljinca. Ko sem preizkusil shranjeni signal, je deloval brezhibno. Nato sem preizkusil še nekaj drugih daljincev, na primer za klimatsko napravo in projektor, in tudi pri teh je Flipper Zero uspešno prebral in ponovno oddal signal.

Ugotovil sem, da IR signali niso nič zelo posebnega, saj jih uporabljamo vsak dan pri daljincih za televizijo, klimo ali druge naprave. Danes jih je tudi precej enostavno kopirati in uporabiti, saj ima Flipper Zero že veliko bazo različnih signalov.

3.2.3 SEMAFORJI

Barvo semaforja sem poskušal spreminjati na varnem območju, kjer ni bilo veliko prometa, da s poskusom ne bi ogrožal varnosti. S seboj sem imel napravo Flipper Zero in Wi-Fi modul.

Najprej sem pomislil, da semaforji morda delujejo preko brezžičnega signala. Zato sem najprej poskusil z Wi-Fi skeniranjem. Na Flipper Zero sem priklopil Wi-Fi modul in približno deset minut skeniral omrežja v bližini semaforja. Naprava je zaznala veliko Wi-Fi omrežij iz bližnjih hiš in stavb, vendar nobeno ni pripadalo semaforju.

Ker nisem našel ničesar, sem začel raziskovati naprej. Na internetu sem pogledal več videoposnetkov in člankov, kjer so razlagali, ali lahko Flipper Zero spreminja semaforje. Večina je pisala, da to ni mogoče in da so videi na internetu pogosto prirejeni. Kljub temu sem želel preveriti še sam.

Naslednji dan sem se vrnil do istega semaforja in poskusil še s skeniranjem SUB-1 GHz signalov. To so signali, ki jih uporabljajo nekatere naprave za brezžično komunikacijo. Tudi po daljšem skeniranju Flipper Zero ni zaznal nobenega signala, ki bi pripadal semaforju. Zato sem začel sumiti, da semafor sploh ne uporablja brezžične komunikacije.

Čez približno teden dni sem opazil, da so semafor popravljali delavci, zato sem jih vprašal, kako deluje. Povedali so mi, da večina semaforjev v Velenju ne deluje preko Wi-Fi ali drugih brezžičnih signalov, ampak so povezani s kabli pod cesto. Ti kabli so povezani z glavnim sistemom za upravljanje prometa, ki nadzoruje delovanje semaforjev.

Izvedel sem tudi, da se barve na semaforju ne spreminjajo naključno, ampak po vnaprej nastavljenem programu. Semaforji so usklajeni med seboj in delujejo glede na čas ali prometne senzorje v cesti. Do sistema za upravljanje imajo dostop samo pooblaščene osebe.

Na koncu sem ugotovil, da Flipper Zero ne more spreminjati barve semaforjev v Velenju, ker ti niso povezani brezžično. Ta del raziskave mi je pomagal bolje razumeti, kako delujejo prometni sistemi in zakaj vseh naprav ni mogoče upravljati z brezžičnimi signali.

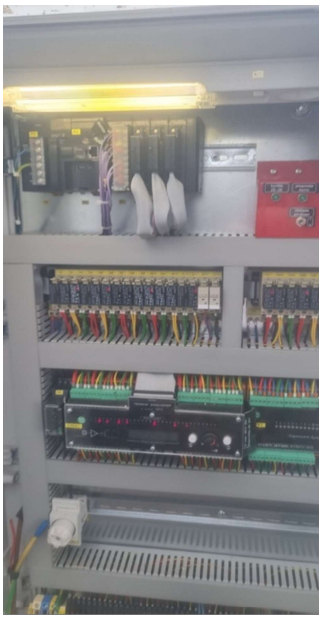
3.2.3.1 »PAMET« SEMAFORJA

Ker me je še vedno zanimalo delovanje semaforja, mi je mentor pomagal in dobil sem kontakt glavnega vzdrževalca semaforjev v Velenju, gospoda Vinka Meže. Zaposlen je pri Komunalnem podjetju Velenje in skrbi za upravljanje ter vzdrževanje semaforjev v Velenju in okolici.

Poklical sem ga in se z njim dogovoril za kratek sestanek pri enem izmed križišč. Tam mi je pokazal notranjost semaforja. Odprl je elektro omarico, mi podrobno razložil, kako deluje, in odgovoril na vsa moja vprašanja. To mi je zelo pomagalo pri razumevanju delovanja semaforjev.

Elektro omarica semaforja je kovinska omara, ki stoji ob križišču. V njej je vsa glavna oprema za delovanje semaforjev. Notri so naprave, ki nadzorujejo menjavanje barve luči in skrbijo za pravilno delovanje semaforja. Ta omarica je zelo pomembna, saj omogoča varno in urejeno vodenje prometa v križišču.

Slika 23: Elektro omarica



Slika 24: Moduli in varovalke

Slika 25: Gumbi za osvetlitev

V desnem delu elektro omarice so bili nameščeni releji, ki imajo pomembno vlogo pri delovanju semaforja. Releji so električne komponente, ki delujejo kot stikala. Omogočajo vklapljanje in izklapljanje različnih tokokrogov. Preko njih krmilna enota upravlja, katera barva luči na semaforju se bo prižgala. Ko krmilnik pošlje signal, rele preklopi tok in prižge rdečo, rumeno ali zeleno luč. Releji so nameščeni pregledno, da jih lahko vzdrževalci hitro preverijo ali v primeru okvare zamenjajo.

Na spodnjem delu elektro omarice so nameščene varovalke. Njihova naloga je zaščita električnega sistema pred preobremenitvijo ali kratkim stikom. Če pride do previsokega toka, varovalka prekine tokokrog in s tem zaščiti naprave in kable. Tako prepreči poškodbe krmilnika, napajalnikov in luči na semaforju. Varovalke so razporejene po posameznih delih sistema, zato lahko vzdrževalci hitro ugotovijo, kje je napaka in jo varno odpravijo.

V levem delu elektro omarice so nameščeni gumbi in drugi upravljalni elementi. Ti gumbi omogočajo ročni vklop, izklop ali testiranje posameznih luči na semaforju. Uporabljajo jih predvsem vzdrževalci, ki z njihovo pomočjo preverjajo, ali vse luči delujejo pravilno, ter po potrebi opravijo popravila ali nastavitve.

Gumbi so povezani s krmilnim sistemom semaforja in omogočajo neposreden nadzor nad delovanjem luči. Tako lahko vzdrževalci preverijo vsako luč posebej, jo začasno izklopijo ali testirajo. To omogoča hitrejše in varnejše vzdrževanje celotnega sistema.

V omarici se nahaja tudi krmilnik semaforja, ki deluje kot majhen računalnik. Ta računalnik določa zaporedje luči in čas, koliko časa sveti posamezna barva. Program semaforja je nastavljen glede na promet in čas dneva, lahko pa se po potrebi tudi spremeni. Krmilnik skrbi, da se luči ne prižigajo hkrati in da promet skozi križišče poteka varno.

Če pride do napake ali spremembe prometa, lahko program semaforja prilagodijo tudi na daljavo. Komunikacija med semaforjem in nadzornim centrom poteka po kablih ali optični povezavi. Takšna povezava je bolj zanesljiva kot brezžična, zato se uporablja za upravljanje semaforjev. Tako lahko nadzorni center spremlja delovanje in po potrebi spremeni nastavitve.

Kot zanimivost sem izvedel, da imajo nekateri semaforji v elektro omarici posebno stikalo, s katerim lahko delavci podaljšajo zeleno luč, če nastane večji zastoj. V določenih primerih lahko semafor preklopijo tudi na rumeno utripajočo luč, na primer ob delih na cesti ali izrednih dogodkih. Če je križišče blizu železnice, se lahko ob prihodu vlaka semafor samodejno preklopi na rumeno utripajočo luč, da dodatno opozori voznike.

V elektro omarici so nameščene tudi varovalke in zaščitni sistemi, ki skrbijo za varno delovanje. Če pride do okvare, na primer da ena luč ne deluje ali pride do električne napake, varovalke preprečijo nadaljnje težave. Takrat se lahko semafor samodejno preklopi v varnostni način, kjer vse smeri utripajo rumeno. To voznike opozori, da semafor ne deluje normalno in morajo voziti bolj previdno.

Če pride do okvare, lahko vzdrževalci uporabijo tudi posebno stikalo v omarici, s katerim začasno preverijo delovanje sistema. Tako lažje ugotovijo napako in poskrbijo, da semafor čim prej ponovno deluje pravilno in varno.

Na ta način lahko vzdrževalci opazujejo, katera luč ne deluje pravilno ali kateri del sistema povzroča težavo. Ko napako odkrijejo, lahko okvaro popravijo ali nedelujoči del zamenjajo. Takšna stikala so namenjena predvsem servisiranju in jih uporabljajo le usposobljeni strokovnjaki, saj omogočajo natančen pregled delovanja semaforja.

Semaforji so lahko med seboj povezani tudi v tako imenovani zeleni val. To pomeni, da so semaforji časovno usklajeni. Če se voznik pelje z dovoljeno hitrostjo, lahko na določenih cestah zapored prevozi več križišč brez ustavljanja, ker se mu prižiga zelena luč. Takšen primer je na primer na Mariborski cesti v Celju, kjer je promet zaradi tega bolj tekoč.

V nekaterih državah, predvsem v ZDA, imajo semaforji tudi naprednejše sisteme. Ti lahko zaznajo intervencijska vozila, kot so reševalci, gasilci ali policija. Ko se takšno vozilo približuje križišču, semafor samodejno spremeni signal in omogoči hitrejši prehod. Nekateri sistemi omogočajo tudi daljinsko upravljanje semaforjev, vendar takšnih sistemov v tej raziskavi nisem mogel preizkusiti, saj se uporabljajo predvsem v tujini.

4 REZULTATI

4.1 PRIDOBIVANJE WI-FI GESLA

Na podlagi raziskovanja sem ugotovil, da je mogoče iz zajetih podatkov brezžičnega omrežja analizirati varnost gesla in preveriti, kako močno je. PCAP datoteka sama po sebi ne vsebuje pravega gesla, ampak vsebuje podatke o omrežju, kot so ime omrežja (SSID), MAC naslovi in WPA handshake. Ta handshake je zapis, ki nastane ob povezovanju naprave z omrežjem in omogoča nadaljnjo analizo varnosti.

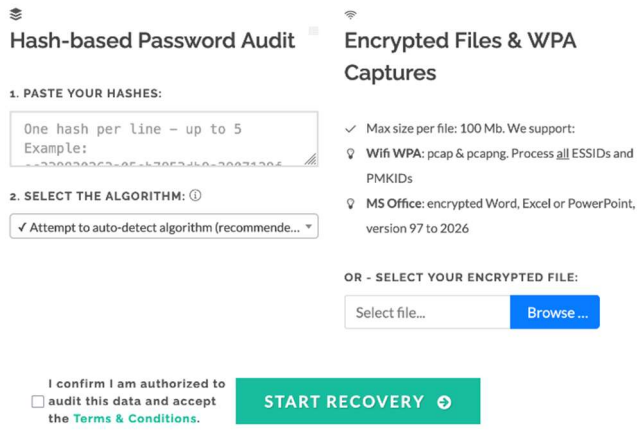
Ugotovil sem, da lahko posebni programi iz tega WPA handshaka preverjajo različna možna gesla in jih primerjajo s shranjenimi podatki. Tak postopek lahko traja zelo dolgo, saj mora program preveriti veliko možnih kombinacij. Koliko časa traja, je odvisno predvsem od dolžine in zahtevnosti gesla. Daljše in bolj zapleteno geslo pomeni večjo varnost.

Rezultati so pokazali, da je varnost Wi-Fi omrežja zelo odvisna od kakovosti gesla. Kratka in enostavna gesla je mogoče uganiti hitreje, medtem ko so daljša in bolj zapletena gesla veliko bolj varna. Če v geslo dodamo posebne znake, kot so klicaj ali vprašaj, zvezdica itd., bo geslo ugotavljalo lahko tudi več let. S tem sem spoznal, kako pomembno je uporabljati močna gesla in dobre varnostne nastavitve za zaščito brezžičnega omrežja.

4.1.1 TEŽAVE PRI PRIDOBIVANJU GESLA

Na začetku sem imel nekaj težav pri uporabi spletne strani OnlineHashCrack, saj ima stran dva različna stolpca za nalaganje podatkov. Sprva nisem izbral pravilnega načina za oddajo datoteke, zato postopek ni deloval in nisem dobil rezultatov. Po več poskusih sem ugotovil, da moram izbrati pravilen stolpec za nalaganje datoteke, ki je namenjen analizi Wi-Fi omrežij.

Ugotovil sem, da je levi stolpec na strani namenjen predvsem vnosu hash vrednosti gesel, kjer uporabnik vnese samo hash. Desni stolpec pa je namenjen nalaganju datotek, kot so PCAP datoteke z zajetimi podatki omrežja. Ko sem izbral pravilen način nalaganja, je sistem datoteko uspešno prepoznal in začel z analizo.



Slika 26: Onlinehashcrack.com

Pri iskanju gesla program uporablja več različnih načinov. Med njimi so preverjanje pogostih gesel iz slovarja, preizkušanje različnih kombinacij ter primerjanje izračunanih vrednosti z zajetim hashom iz datoteke. Program tako postopoma preverja veliko možnih gesel.

Takšen postopek lahko traja precej dolgo, saj mora sistem preizkusiti veliko kombinacij. Koliko časa traja, je odvisno predvsem od tega, kako dolgo in zapleteno je geslo. Po daljšem času je program našel pravilno geslo in ga prikazal na zaslonu.

4.2 IR DALJINEC

Kot sem že omenil, so IR signali med najbolj pogostimi in tudi najlažji za uporabo, saj je veliko signalov že shranjenih v različnih bazah. V raziskavi sem preverjal, ali lahko Flipper Zero upravlja naprave, ki delujejo na IR signal.

Pri testiranju sem ugotovil, da Flipper Zero lahko upravlja nekatere naprave, kot so televizije in druge naprave z daljinskim upravljalnikom. Deluje tako, da pošlje enak signal kot pravi daljinec. Če je signal pravilen, naprava reagira enako kot na originalni daljinski upravljalnik.

Opazil sem, da je delovanje najboljše pri televizijah, ker imajo te naprave zelo pogoste IR signale, ki jih je lahko najti v bazi. Pri nekaterih drugih napravah pa ni delovalo vedno, ker signal ni bil shranjen v bazi ali pa je bil drugačen.

Ugotovil sem tudi, da IR signal ne deluje skozi stene in mora biti naprava dovolj blizu. Če si predaleč ali je med napravama ovira, signal ne pride do naprave. Na koncu lahko rečem, da Flipper Zero lahko upravlja veliko naprav, ki delujejo na IR signal, vendar ne vseh. Odvisno je od vrste naprave, razdalje in tega, ali ima naprava znan signal.

4.3 BARVE NA SEMAFORJIH

Na podlagi pogovora z vzdrževalcem semaforjev in ogleda elektro omarice sem ugotovil, da sodobni semaforji delujejo drugače, kot sem sprva mislil. Na začetku me je zanimalo, ali bi lahko na delovanje semaforjev vplivali z napravami, ki delujejo na brezžične signale. Po raziskovanju sem ugotovil, da semaforji ne uporabljajo takšne brezžične komunikacije, ki bi jo lahko zaznale podobne naprave.

Vzdrževalec mi je razložil, da semaforji delujejo s pomočjo krmilnika v elektro omarici, ki je povezan z lučmi in drugimi deli sistema prek kablov. Vsa komunikacija med semaforji in nadzornim centrom poteka po žičnih ali optičnih povezavah. Tak način povezave je bolj zanesljiv in varen, saj ni občutljiv na motnje in ga ni mogoče enostavno prestreči.

Ugotovil sem tudi, da semaforji nimajo Wi-Fi povezave ali drugih radijskih signalov, ki bi jih lahko zaznal Flipper Zero. Prav tako ne uporabljajo SUB-1 GHz signalov za upravljanje luči. Delujejo preko notranjih električnih povezav, relejev in krmilnika, ki natančno določa čas delovanja posamezne luči.

Po več poskusih sem ugotovil, da Flipper Zero ne more zaznati nobenega signala, s katerim bi lahko upravljal semafor. Kasneje sem izvedel, da semaforji v Velenju delujejo preko kablov in posebnega nadzornega sistema.

Semaforji v Velenju delujejo s pomočjo krmilne enote v elektro omarici ob križišču. Ta krmilnik deluje kot majhen računalnik, ki upravlja zaporedje luči in določa, koliko časa sveti posamezna barva. Program delovanja je nastavljen glede na promet, čas dneva in potrebe križišča.

Vsi deli semaforja, kot so luči, tipke za pešce in senzorji, so s krmilnikom povezani preko električnih kablov. Sistem je narejen tako, da deluje varno in zanesljivo. Do nastavitev in nadzora lahko dostopajo samo pooblaščene osebe s posebno opremo. Zato sem ugotovil, da semaforjev ni mogoče upravljati z navadnimi brezžičnimi napravami, kot je Flipper Zero.

5 RAZPRAVA

Hipoteze so bile sledeče:

1. hipoteza: Flipper Zero lahko krmili napravo, ki deluje na daljinski upravljalnik.

V raziskavi sem ugotovil, da lahko naprava Flipper Zero tudi brez dodatnih modulov upravlja naprave, ki uporabljajo infrardeči (IR) daljinski upravljalnik. Naprava ima že vgrajen infrardeči oddajnik in sprejemnik, zato lahko bere, shrani in ponovno oddaja IR signale.

Rezultati so pokazali, da lahko Flipper Zero uspešno posnema delovanje različnih daljinskih upravljalnikov, na primer za televizor, klimatsko napravo in projektor. Naprava lahko uporablja že shranjene signale iz baze ali pa signal prebere neposredno z daljinca in ga shrani za kasnejšo uporabo.

Na podlagi raziskave sem ugotovil, da je upravljanje naprav z infrardečimi signali s Flipperjem Zero preprosto in učinkovito. Naprava lahko zanesljivo posnema IR signale in tako deluje kot univerzalni daljinski upravljalnik. ***Hipotezo ena tako lahko potrdim.***

2. hipoteza: Flipper Zero lahko spreminja barvo na semaforju.

V raziskavi sem ugotovil, da z napravo Flipper Zero ni mogoče spreminjati barve semaforjev. Ko sem bil v bližini semaforjev, naprava ni zaznala nobenih brezžičnih signalov, kot so Wi-Fi ali SUB-1 GHz, ki bi bili povezani z njihovim delovanjem.

Rezultati so pokazali, da semaforji delujejo s pomočjo krmilnika in električnih povezav v elektro omarici. Delovanje luči je določeno z vnaprej nastavljenim programom, ki skrbi za pravilno zaporedje rdeče, rumene in zelene luči. Dostop do nastavitev imajo samo pooblaščene osebe s posebno opremo, zato jih navadni ljudje ne morejo upravljati.

Ugotovil sem tudi, da sodobni semaforji ne uporabljajo radijskih ali infrardečih signalov, ampak delujejo preko kablov ali centralnega nadzornega sistema. Ker komunikacija poteka po žici ali optičnem kablu, je naprava Flipper Zero ne more zaznati ali posnemati.

Na koncu raziskave lahko zaključim, da Flipper Zero ne more vplivati na delovanje semaforjev ali spreminjati njihovih barv. ***Hipotezo dve zavračam.***

3. hipoteza: Flipper Zero lahko dobi geslo Wi-Fi omrežja.

V raziskavi sem ugotovil, da lahko naprava Flipper Zero z dodatnim Wi-Fi modulom zazna in skenira Wi-Fi omrežja v okolici. Pri izbranem omrežju lahko zbere podatke o povezavi, kot so ime omrežja, MAC naslov in WPA handshake oziroma PMKID. Med raziskovanjem sem zajel podatke našega domačega omrežja in jih shranil v posebno datoteko.

Ugotovil sem, da ta datoteka sama ne vsebuje gesla, ampak omogoča nadaljnjo analizo. S pomočjo spletne strani za analizo hashov sem datoteko naložil v sistem, ki je začel preverjati različna možna gesla. Po določenem času je program našel pravilno geslo omrežja.

Na podlagi raziskave sem ugotovil, da Flipper Zero lahko pomaga pri ugotavljanju varnosti Wi-Fi omrežja, vendar ne neposredno. Naprava zbere potrebne podatke, iz katerih je nato mogoče s posebnimi programi preverjati gesla, če ta niso dovolj močna. ***Ta hipoteza je v tem delu potrjena.***

6 POVZETEK

V raziskovalni nalogi sem raziskoval delovanje naprave Flipper Zero in njene možnosti uporabe v vsakdanjem življenju. Zanimalo me je predvsem, ali lahko naprava pridobi geslo Wi-Fi omrežja, upravlja naprave z daljinskim upravljalnikom in spreminja barvo semaforjev.

Pri raziskovanju sem ugotovil, da lahko Flipper Zero s pomočjo dodatnega Wi-Fi modula zajame podatke o omrežju. Iz teh podatkov je nato mogoče s posebnimi programi preverjati gesla, če ta niso dovolj zapletena. Ugotovil sem tudi, da lahko naprava brez dodatnih modulov upravlja različne naprave, ki delujejo na infrardeči daljinski upravljalnik, kot so televizor, klima in projektor. Poskusi so pokazali, da Flipper Zero lahko prebere in posnema IR signale ter deluje kot univerzalni daljinski upravljalnik.

Pri raziskovanju delovanja semaforjev sem ugotovil, da Flipper Zero ne more spreminjati barve luči na semaforju. Semaforji niso povezani z brezžičnimi signali, ampak delujejo preko kablov in centralnega sistema za upravljanje prometa. Barve na semaforjih se spreminjajo po vnaprej določenem programu in jih lahko upravljajo samo pooblaščene osebe.

Raziskava mi je pomagala bolje razumeti delovanje sodobnih elektronskih naprav, brezžične komunikacije in prometnih sistemov. Ugotovil sem, da ima Flipper Zero veliko zanimivih funkcij in je zelo uporaben za učenje o tehnologiji, vendar ima tudi svoje omejitve.

7 ZAKLJUČEK

V prvem delu raziskovanja sem se osredotočil na pregled tehničnih lastnosti in delovanje naprave Flipper Zero. Spoznal sem, kako naprava deluje, katere funkcije ima in za kaj se lahko uporablja.

V drugem delu raziskovanja sem raziskoval delovanje Wi-Fi omrežij in naprave Flipper Zero. Preverjal sem, ali lahko naprava zazna omrežja in zbere podatke, iz katerih je mogoče ugotoviti geslo. Uporabil sem dodatni Wi-Fi modul, s katerim sem skeniral omrežja in zajel potrebne podatke. Nato sem raziskal, kako se ti podatki analizirajo in kako je mogoče preverjati varnost gesla, če to ni dovolj zapleteno.

V tretjem delu raziskovanja sem preizkušal delovanje infrardečih (IR) naprav. Ugotavljal sem, ali lahko Flipper Zero deluje kot univerzalni daljinski upravljalnik. S pomočjo že nameščene INFRARED aplikacije sem preizkusil upravljanje televizorja, klime in projektorja. Naprava je uspešno prebrala in posnemala IR signale ter omogočila upravljanje naprav brez dodatne opreme.

V četrtem delu raziskovanja sem se osredotočil na semaforje in možnost njihovega upravljanja. Preveril sem, ali semaforji uporabljajo brezžične signale, ki bi jih Flipper Zero lahko zaznal. Skeniral sem Wi-Fi in SUB-1 GHz signale v bližini semaforja, vendar nisem zaznal nobenega uporabnega signala. Po dodatnem raziskovanju in pogovoru s strokovnjaki sem ugotovil, da semaforji delujejo preko kablov in notranjih krmilnih sistemov, zato jih z napravo Flipper Zero ni mogoče upravljati.

Med raziskovanjem sem spoznal tudi, da ne smemo verjeti vsem informacijam na družbenih omrežjih, kot sta YouTube in TikTok. Tam je veliko videoposnetkov, ki pretiravajo ali prikazujejo neresnične stvari, saj so pogosto narejeni predvsem za zabavo in oglede, ne pa za resničen prikaz delovanja tehnologije.

8 ZAHVALA

Z raziskovalno nalogo sem dosegel cilj, ki sem si ga zadal na začetku. Pri tem bi se najprej rad zahvalil mentorjema Borisu Bubiku in Urošu Remenihu za vso pomoč, nasvete in podporo pri izdelavi raziskovalne naloge.

Posebna zahvala gre tudi gospodu Vinku Meži iz Komunalnega podjetja Velenje, ki mi je podrobno razložil delovanje semaforjev in mi s tem omogočil boljše razumevanje sistema. S pridobljenimi informacijami sem lahko uspešno raziskal to področje in dokončal raziskovalno nalogo.

Zahvaljujem se tudi staršema, ki sta mi omogočila nakup potrebne opreme in me pri raziskovanju ves čas spodbujala ter podpirala.

9 IZJAVA

Izjavljam, da sem raziskovalno nalogo z naslovom » Etično hekanje « izdelal samostojno. Pri delu sem uporabljal navedene vire, literaturo in pomoč mentorjev.

Vsa uporabljena literatura in viri so ustrezno navedeni v seznamu virov. Raziskovalna naloga je rezultat mojega lastnega dela in je še nisem oddal drugje.

Izjavljam, da sem pri pripravi raziskovalne naloge upošteval načela in smernice v skladu z veljavnimi akti raziskovalnega področja

Kraj in datum: Velenje, 11. 2. 2026

Avtor: Taj Remenih

Podpis avtorja: 

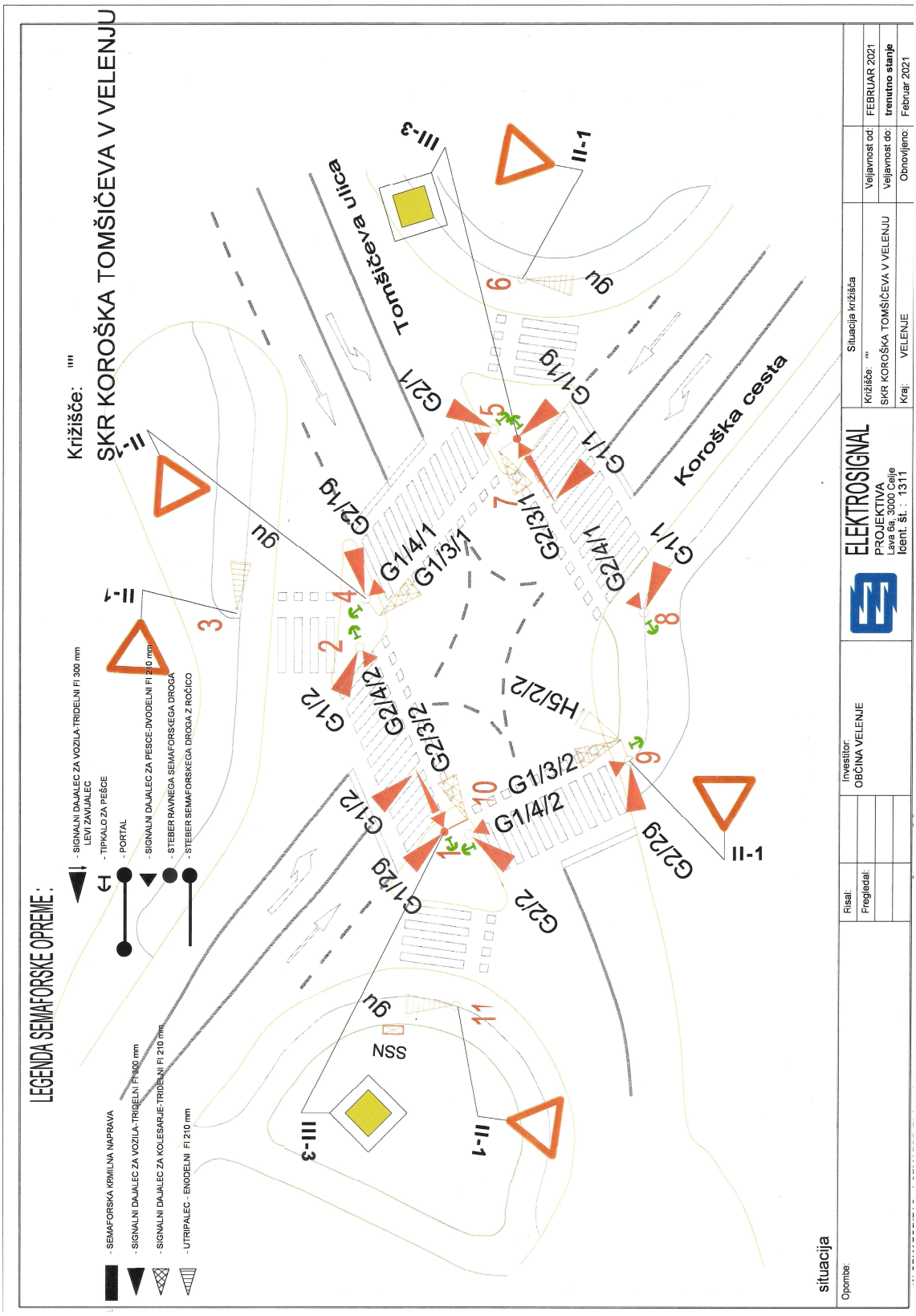
Mentor: Uroš Remenih

Podpis mentorja: Uroš Remenih Digitally signed by Uroš Remenih Date: 2026.02.20 09:27:28 +01'00'

Mentor: Boris Bubik

Podpis mentorja: BORIS BUBIK Digitalno podpisal BORIS BUBIK Datum: 2026.02.19 20:50:09 +01'00'

9 PRILOGE



Priloga 1: Zemljevid semaforiziranega križišča

Priloga 2: Graf intervala prižganih barv na semaforju

11 VIRI IN LITERATURA

Spletni viri

Flipper Zero. https://flipperzero.one (30. 9. 2025).

Flipper dokumentacija. https://docs.flipperzero.one (7. 10. 2025).

Flipper Lab. https://lab.flipper.net (7. 10. 2025).

Cisco: What is Wi-Fi. https://www.cisco.com (15. 12. 2025)

OnlineHashCrack. https://www.onlinehashcrack.com (30. 12. 2025).

Kaspersky: Wi-Fi security. https://www.kaspersky.com (22. 1. 2026).

RFID tehnologija. https://www.techtarget.com (14. 12. 2025).

NFC Forum. https://nfc-forum.org (14. 12. 2025).

Traffic light (Wikipedia). https://en.wikipedia.org/wiki/Traffic_light (15. 1. 2026).

Swarco. https://www.swarco.com (13. 1. 2026).

Siemens Mobility. https://www.mobility.siemens.com (14. 1. 2026).

Ustni viri

Meža, Vinko – Komunalno podjetje Velenje, razlaga delovanja semaforjev in ogled elektro omarice, februar 2026