

Hackers' Toolbox: Exploring the Gadgets of the Trade

Evgenios Anastasiadis

BRIDGEFEST II
SAT 31.05.25
12.00

BRIDGEFEST II

BATWORTHYWOMBAT (UK)

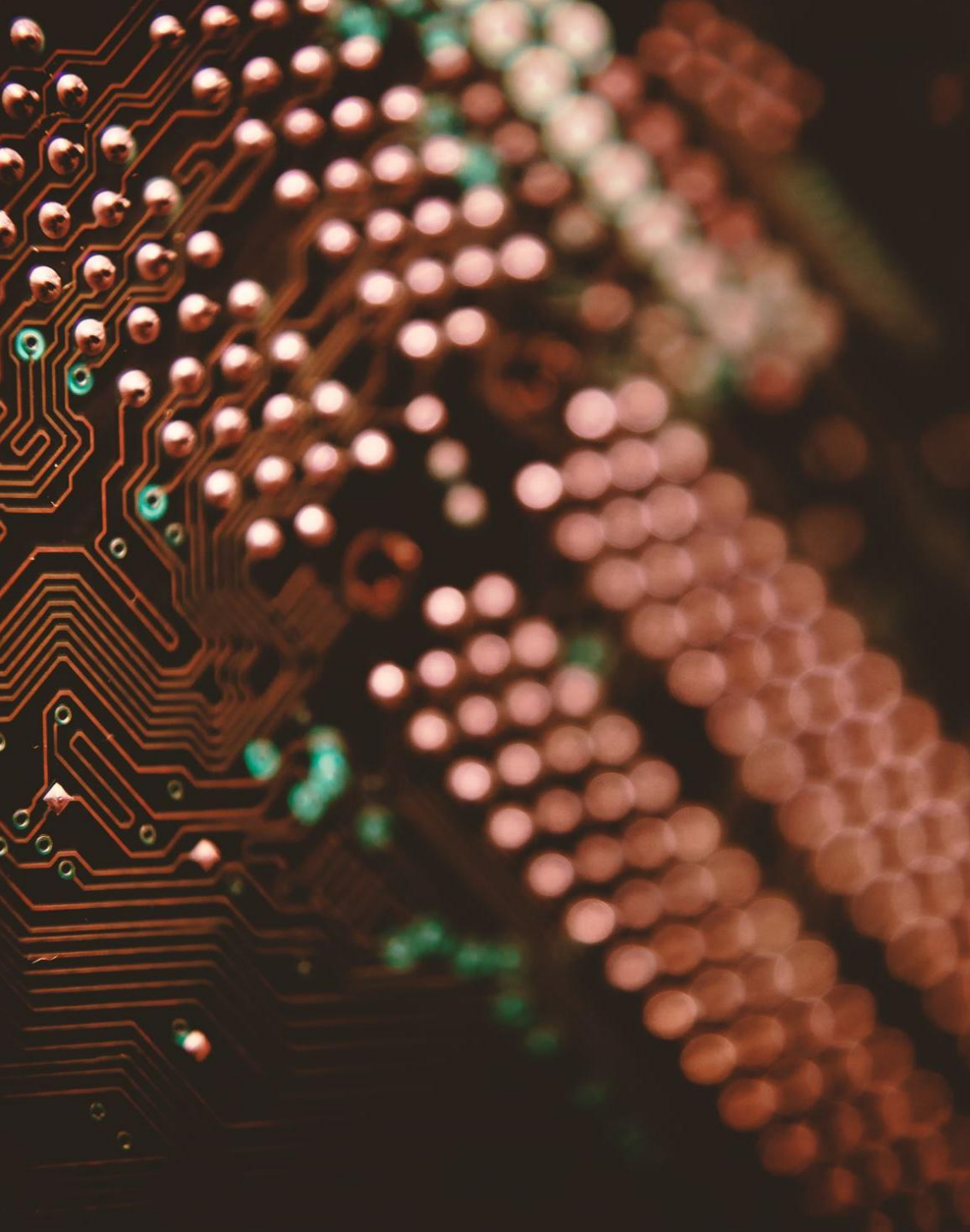
PHRS (GR)

(GR)

(R)

(GR)

(R)



Why are we here?

- E: I think I should have a hardware hacking talk at **Bridgefest**, so I can feel good about myself for the money I spend
- G: Congrats, your talk was submitted
- S: TALK APPROVED

I also wanted to find the time to play more with them :)

DISCLAIMER

- This presentation is designed for educational and informational purposes only. The demonstrations and examples provided are intended to showcase the devices' functionalities and potential applications in a controlled and lawful manner.
- Use only your own hardware and networks.
- Misusing any device can lead to serious legal consequences.
- **All situations described are purely hypothetical and probably generated by some sort of AI.**





Dear Valued Guest,

Welcome, and thank you for choosing Resorts World Las Vegas. We are pleased that you have joined us, as you have chosen to stay with us for relaxation, fun, and excitement!

As you may or may not know, a well-known hacking convention will be held in Las Vegas during your stay.

We remain committed to our guests' safety and understand the utmost importance of cybersecurity, as well.

In an effort to increase the safety of our guests, we will be conducting scheduled, brief visual and non-intrusive room inspections daily beginning Monday, August 5.

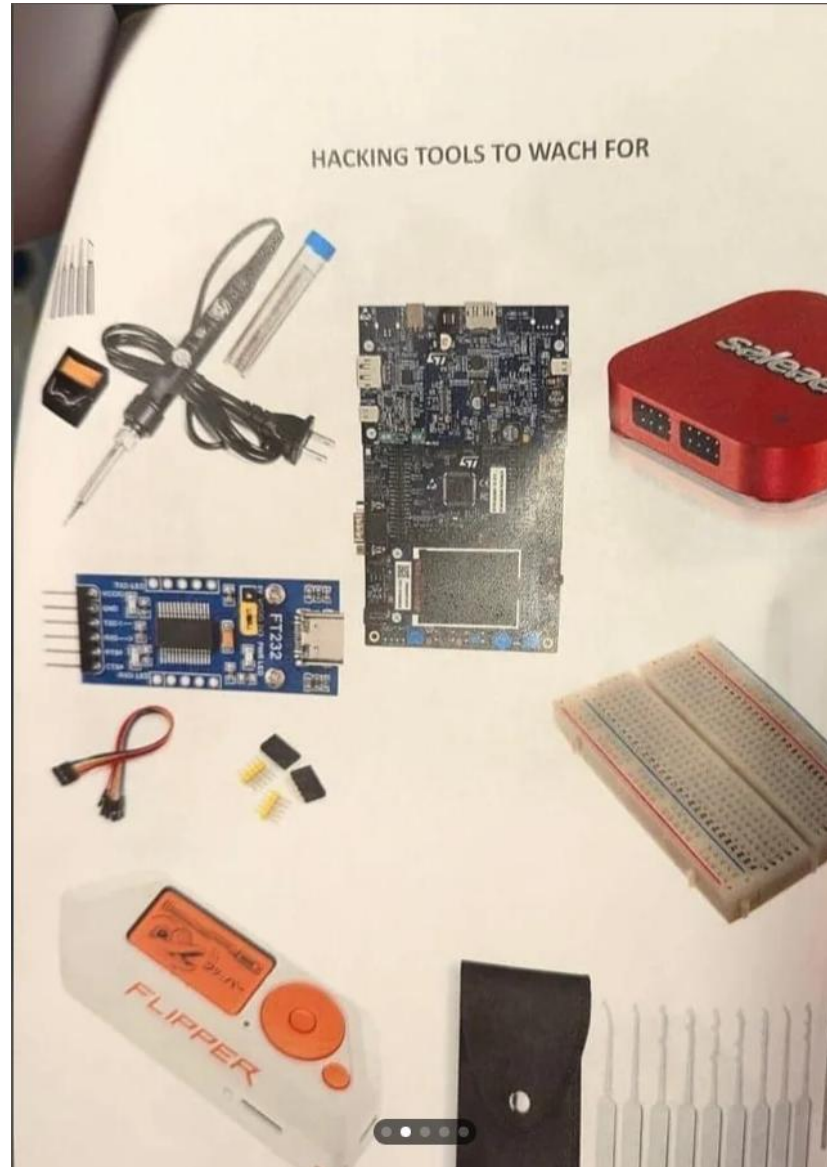
Rooms with a privacy sign will be included as part of the inspection process.

If you have any questions or concerns during your visit, please contact the Hotel Operator by pressing "0" on your guestroom phone.

We appreciate your understanding and cooperation.

Sincerely,

Prescott Yee
Director of Hotel Operations





BRIDGEFEST II



SECURITY

- No later than 9:00 AM each day, Housekeeping Assistant Director+ will run and print rooming list for all hotel guests reserved through the DEF CON group block.
- Security will be responsible for conducting visual inspections on these rooms, all in Hilton.
 - 8/5 – 8/12 between the hours of 9a-5p.
 - Upwards of 1,000 rooms on peak.

HOUSEKEEPING

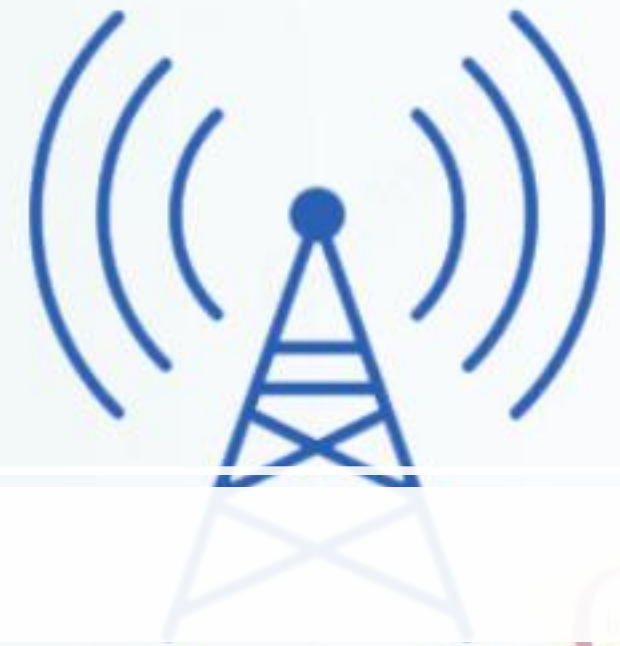
- At 2:00 PM each day, Housek



The Hacker's Toolbox

(some of them)

**Radio operates by
transmitting and receiving
electromagnetic waves**



What is Radio?



SDR vs HDR

- Software Defined Radio - uses software modules and processors operating on a hardware platform to digitally recreate radio signal transmissions and receptions.
- Hardware Defined Radio - Antennas, dials and knobs, receivers, and the like, that transmit and receive signals via radio waves.

HackRF

A software-defined radio (SDR) that can transmit and receive signals from 1 MHz to 6 GHz.

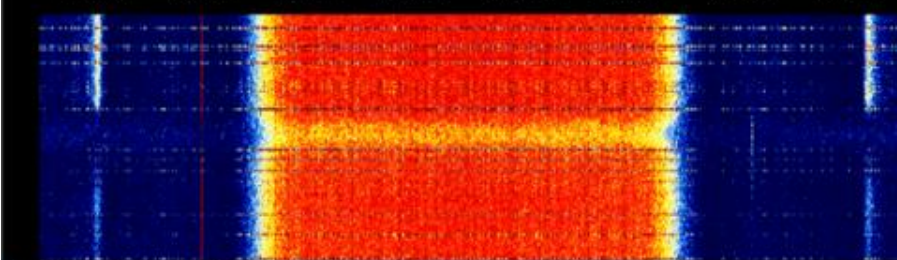
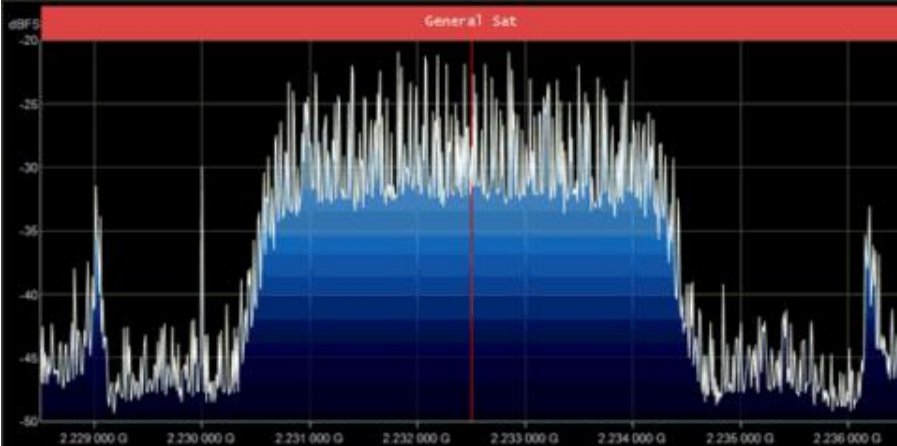
Key Features:

- Open-source hardware
- Supports signal analysis and transmission
- Operates on USB power

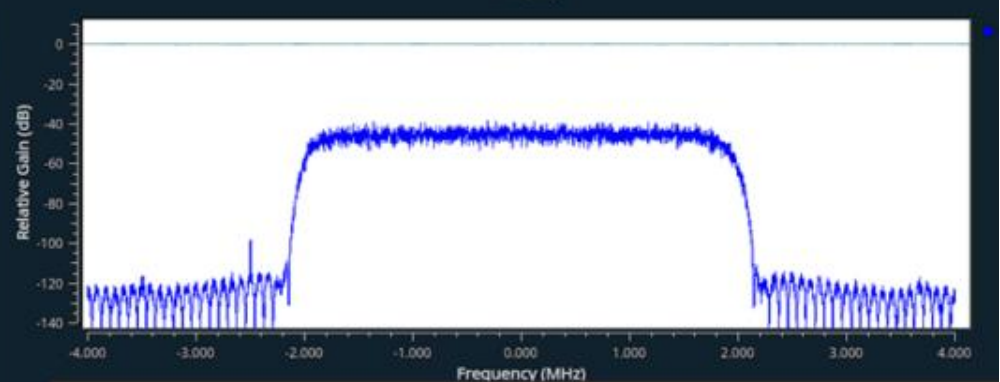
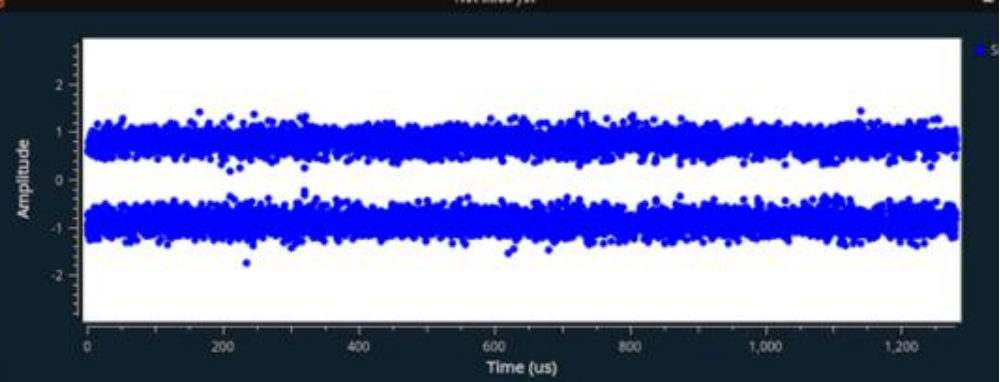
Use Cases:

- Wireless signal reverse engineering
- GSM, LTE, Bluetooth, satellite signals





```
3041902000450> solution x/y/z: 4327407.9 1812900.1 4628573.8 PDOP=1.6 n_sats=10
d solution tow:377441.5122801500, wn:2147
1298883042380882495> 5 PLL stress
1298883042787485199> 5 low C/N0 too long, dropping (@ 185881226597800000.000)
1298883043286481741> GPS L1CA 8 Nav phase flip - half cycle slip detected, but not corrected
Mar 4 08:50:25 stmib system_slate_sharer: 185700.001191: mark: 2021-03-04 08:50:25.780092000
~Mar 4 08:50:26 stmib system_housekeeping_monitor: 185700.001369: mark: 2021-03-04 08:50:26.258105000
Mar 4 08:50:26 stmib system_slate_sharer: 185700.000044: mark: 2021-03-04 08:50:26.280315000
Mar 4 08:50:26 stmib system_housekeeping_monitor: 185700.000223: mark: 2021-03-04 08:50:26.709828000
j1298883049266914235> New ephemeris(valid: 1) for GPS L1CA 13, fi:14400
meris(valid: 1) for GPS L1CA 14, fi:14400
1298883049269650063> New ephemeris(valid: 1) for GPS L1CA
1298883049271424312> New ephemeris(valid: 1) for GPS L1CA 15, fi:14400
635> New ephemeris(valid: 1) for GPS L1CA 30, fi:14400
1298883049277253807> New ephemeris(valid: 1) j8
esMar 4 08:50:32 stmib system_slate_sharer: 185700.001211: mark: 2021-03-04 08:50:32.033380000
1298883049279423719> New ephemeris(valid: 1) for GPS L1CA 24, fi:14400
Mar 4 08:50:32 stmib system_housekeeping_monitor: 185700.000593: mark: 2021-03-04 08:50:32.245662000
q8883049281410525> New ephemeris(valid: 1) for GPS L1CA 19, fi:14400
1298883049281641048> New ephemer
is(valid: 1) for GPS L1CA 20, fi:14400
1298883049281703765> New ephemeris(valid: 1) for GPS L1CA 23,
1298883049289429535> New ephemeris(valid: 1) for GPS L1CA 12, fi:14400
> New ephemeris(valid: 1) for GPS L1CA 10, fi:14400
1298883049290431077> New ephemeris(valid: 1) for
052102160747> solution x/y/z: 4330545.8 1883044.9 4598476.6 PDOP=1.6 n_sats=10
olution tow:377451.7121195335, wn:2147
1298883059715777061> 7 PLL stress
1298883061286346973> GPS L1CA 8 Nav phase flip - half cycle slip detected, but not corrected
r1298883061391728998> 7 PLL stress
61027721820> 7 PLL stress
1298883062302130884> solution x/y/z: 4333150.5 1952832.6 4567708.4 PDOP=2.
1298883062302217340> solution tow:377461.9121034250, wn:2147
1298883063632983297> 5 PLL stress
1298883064448153900> Tracking! PRN:22
1298883065717002000> 15 PLL stress
mar 4 08:50:48 sfic system_housekeeping_monktr: 185820.000131: mark: 2021-03-04 08:50:48.664341000
71298883066704991519> 22 no sync, dropping
1298883066705107566> 7 low C/N0 too long, dropping (@ 18582
6rsubag
1298883070234921610> 5 PLL stress
1298883070739080500> 15 PLL stress
1P11117009> 15 PLL stress
```





Aircraft Tracking

HackRF



Flipper Zero

- Portable
- Multi-use
- Open Source
- Extensible
- Dolphin





Car Keyfob Replay

Beware!!

Newer cars have rolling codes / changing frequency.

Bluetooth Spam Attacks

Works for Android & iOS



Video from @Securiosity

BRIDGEFEST II







BRIDGEFEST II





RFID FIELD DETECTOR

- Usage: Access Control Reconnaissance
- Detects and displays the presence of **Low Frequency** (125KHz) and **High Frequency** (13.56MHz) fields.
- Doesn't tell you exact which card technology

The device requires no batteries. When in the presence of an RFID field, an LED indicates the frequency of the field.

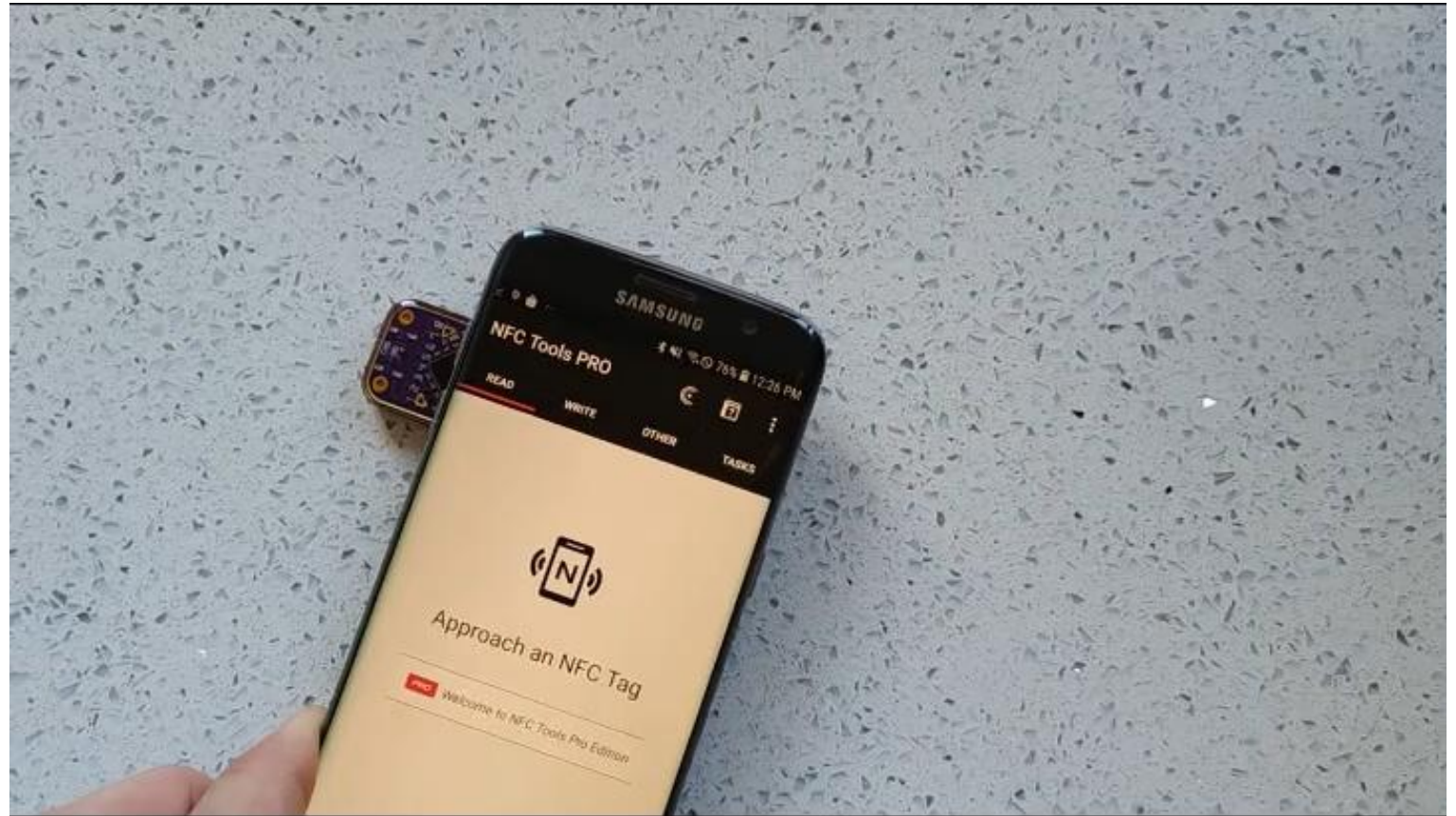


Chameleon

- Key-chain sized, fully open-sourced device
- Low and high-frequency emulation, full read & write capabilities



LOW & HIGH FREQUENCY EMULATION





Proxmark3

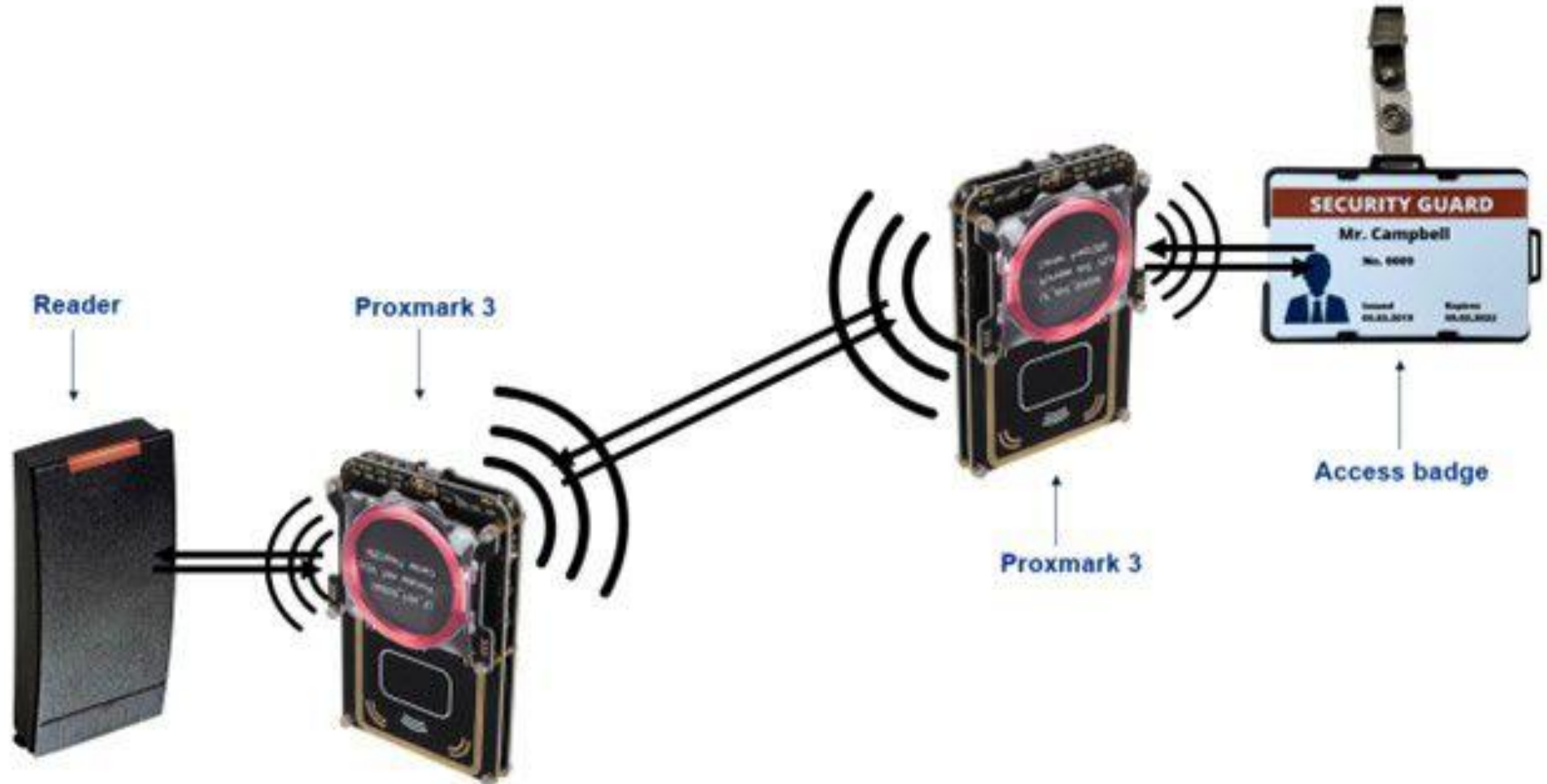
An advanced RFID/NFC sniffing, reading, and emulation tool.

Often referred to as the Swiss army knife of RFID research.

125 kHz LF

13.56 MHz HF

Relay Attacks !



Honorable Mentions



MININO



RUBBER DUCKY



ICOPY XS



WIFI PINEAPPLE

Thank you

BRIDGEFEST II

SAT 31.05.25

