WELCOME TO

Wireless Hacking and Defending Spoken Simply

For
Non-Techies

All Dekked Out
Information Security

ALL DEKKED OUT INFORMATION SECURITY LLC

Welcome – About Me

Patrick Cleary

- Been in the industry full-time since 1997
- Nearly half my life spent working in Security
- Every day I'm still picking up new and cool ways of doing things, often from folks who just started or are new to security themselves
- Love to innovate, collaborate, learn and mentor
- Founder of ADO & Salty Security – this presentation is my own
- Handles are for pots, military aviators, and cool kids –

I'm none of those, so please just call me Patrick

ALL DEKKED OUT

Course Content

CRAWL

Brief introduction to wireless and its terminology. The basics of what you should know as a non-techie.

RUN

”Show and tell” both wireless attacking and defending tools. Impart some ways to further protect.

WALK

Cursory knowledge of wireless protocols and security. Introduction to some of its challenges.

DEMO / Q&A

Run a few demos for anyone interested, and answer questions – not necessarily in that order

ALL DEKKED OUT

CRAWL

Wireless – What is it?

Their Answer: Wireless communication (or just **wireless**, when the context allows) is the transfer of information between two or more points that do not use an electrical conductor as a medium by which to perform the transfer. - source: Wikipedia

Spoken Simply: Wireless is a data exchange between two (usually) devices that does not **require** wires or cables. Wireless typically uses radio waves.

ALL DEKKED OUT

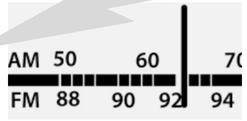
Wireless – How's it work?

AP

(Access Point)

SSID

(Service Set Identifier)



CH

(Channel)

STA

(Station)

*Images are sourced in hyperlinks – All rights and copyrights remain with image owner(s) – Images used under Fair Use Act and for educational purposes only.

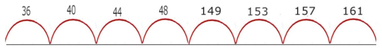
ALL DEKKED OUT

Wireless – How's it look in an IT context?

1. It Burns When IP
2. I'm Under Your Bed
3. Pretty Fly for a Wi-Fi
4. FBI Surveillance Van #119871
5. DEA Surveillance #4188A87
6. I'm In Your Closet
7. I'm Watching You Now
8. Skynet Global Defense Network
9. Let Me Out Of Your Router
10. Undercover Police Car #751
11. I'm Cheating on my WiFi
12. InterTubes
13. Mom - Click Here for Internet

CH

2.4Ghz Channels



5Ghz Channels

AP

SSID

STA

*Images are sourced in hyperlinks – All rights and copyrights remain with image owner(s) – Images used under Fair Use Act and for educational purposes only.

Wireless – Intro to Wireless Alphabet soup

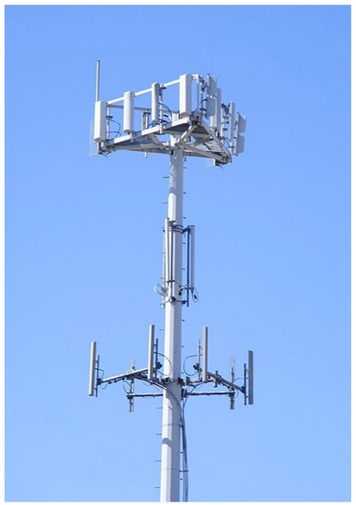
Mobile Broadband Generic term that refers to cellular wireless internet capabilities and their networks. 3G, 4G, 5G are simple terms for the generation (i.e., age) of the network. LTE is Long Term Evolution and is usually affiliated with 4G networks. 3G and parts of 4G are dated as of late 2021.

WiFi Stands for Wireless Fidelity. Basically, a shorter name for wireless. As with cell phones/mobile devices, there are different types or classifications like WiFi 5, WiFi 6. These basically follow the same "generational" model and represent advances in technology and arguably sometimes security. More later.

Bluetooth Generic term that refers short distance wireless. BLE stands for Bluetooth Low Energy. Bluetooth uses a pairing code to connect devices. More on this in the WALK section.

ALL DEKKED OUT

Wireless – How's it work in a cellular context?



BTS

(Base Transceiver Station or Cell Tower spoken simply)

SIM Card

(Service Set Identifier)

Phone

(GSM example)

*Images are sourced in hyperlinks – All rights and copyrights remain with image owner(s) – Images used under Fair Use Act and for educational purposes only.

MORE READING: https://www.clove-technology.com/pages/what-does-sim-free-mean

ALL DEKKED OUT

Wireless – More Alphabet soup (Mobile)

GSM (Global System for Mobile communications). Known more holistically as 3G/2G. The first GSM 3G network launched in the US in December 1995.

CDMA (Code Division Multiple Access). Known more commonly as 3G/2G. Along with GSM, CDMA is the main reason you can't use your AT&T phone on Verizon's network and vice versa.
Most carriers have already shut down 2G networks and have plans to retire 3G by late 2022.

HSPA (High Speed Packet Access). When used without LTE, this term generally refers to a 4G network. WIMAX is another common standard for 4G first utilized in South Korea.

MORE READING: https://www.usmobile.com/blog/lte-gsm-vs-cdma/

Wireless – Alphabet soup – Why we should care?

THERE WILL BE A TEST.

Just kidding. No one cares if you remember the verbiage or the differences right now. In short, it's a hot, convoluted technical mess even for the techies.

Spoken simply – the various numbers refer to increases in wireless transfer speeds, *sometimes* technology advances, and sometimes increased security. But as we'll see later on, there are some challenges and trade-offs still facing the mobile world.

ALL DEKKED OUT

Game Time – Wireless or Canadian?

ALL DEKKED OUT

Wireless – Game Time - IoT

*Images are sourced in hyperlinks – All rights and copyrights remain with image owner(s) – Images used under Fair Use Act and for educational purposes only.

ALL DEKKED OUT

Wireless – Game Time - RFID

*Images are sourced in hyperlinks – All rights and copyrights remain with image owner(s) – Images used under Fair Use Act and for educational purposes only.

ALL DEKKED OUT

Wireless – Game Time - Zigbee

*Images are sourced in hyperlinks – All rights and copyrights remain with image owner(s) – Images used under Fair Use Act and for educational purposes only.

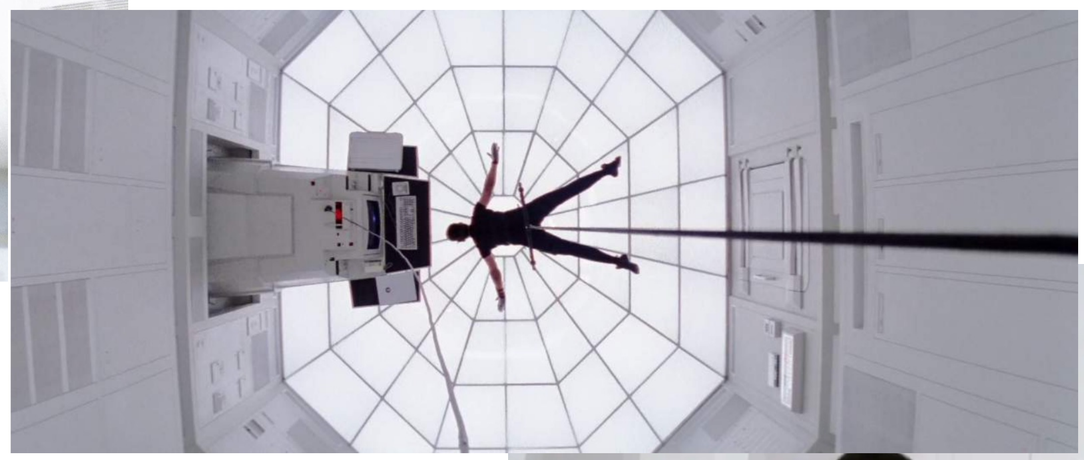
ALL DEKKED OUT

Wireless – Game Time - LoRa

*Images are sourced in hyperlinks – All rights and copyrights remain with image owner(s) – Images used under Fair Use Act and for educational purposes only.

ALL DEKKED OUT

Wireless – Game Time – Air Gapped



*Images are sourced in hyperlinks – All rights and copyrights remain with image owner(s) – Images used under Fair Use Act and for educational purposes only.

ALL DEKKED OUT

Game Time – Wireless or Canadian?

Wireless

IoT – internet of things – represe[illegible] devices and gadgets that weren't previously connected think appliances, mattresses, sex toys, et[illegible]

RFID – radio frequency identification – uti[illegible]ed heavily in retail and supply chain management – smart badges, credit cards, etc.

Zigbee – IEEE 802.15-4 – personal area networks with low-power digital radios

LoRa – long range – low power, wide area network modulation

Canadian

Air Gapped – why Canadian? Because it's isolated, lonely and wishes it could belong to/be us

Apologies – to all our friends and neighbors to the North. We realize the absolute juvenile nature of our cheap joke and take full responsibility.**

ALL DEKKED OUT

WALK

Wireless – A Visual Timeline – 802.11

2.4 Ghz

WIFI 1/2 (b) — 1999

WIFI 3 (g) — 2003

WIFI 5 (ac) — 2013

1999 2009 2021

5 Ghz

WIFI 1/2 (a) — 1999

WIFI 4 (n) — 2009

WIFI 6 (ax) — 2021

NO WIRELESS
ADAPTERS AVAILABLE
for HACKING

Wireless – Frequencies…

802.11 This is the technical specification assigned to wireless communications (e.g., networks and devices - WLAN). Depending upon the type of wireless device you buy, there is a number affiliated with the technology such as 802.11ac, 802.11g, 802.11a, 802.11b, 802.11n and so on. These letters correlate directly to what frequencies your wireless device offers and whether it has capabilities to support both frequencies or just one. These numbers will also tell you the general age of the device and will give clues as to what generation they are. Double letters like ac (Wifi 5) or ax (Wifi 6) indicate newer equipment.

2.4 GHz Provides coverage at a longer range but transmits data at slower speeds. Was introduced/available initially through 802.11b back in 1999. It has a top speed transmission rate of about 150 Mbps. This is also the frequency where most wireless hacking is targeted – more on that in a little bit.

5 GHz Provides less coverage but transmits data at faster speeds. Coverage at this frequency provides speeds up to 1300 Mbps. Wireless attacks at this frequency are less frequent (no pun intended) than at 2.4 GHz BUT not impossible.

Wireless – Channels…

Channels In North America, the FCC governs the regulation of wireless frequencies and determines the number of available wireless channels permitted. Wireless channels help to isolate wireless traffic from other wireless traffic within the same frequency or band, which can be ideal when there is a large overlap of wireless signals, providers, services, or networks within a given geographical location. This directly reduces the amount of "noise" and chaos one might receive if all devices operated only at a preset, dedicated channel.

2.4 GHz For wireless devices in this frequency range, there are ~~fourteen~~ eleven (11) channels to select from/use in the US. However, it is extremely common to see **channels 1, 6, and 11** from a prevalence standpoint. Most wireless networks operating at this frequency will employ one of these three channels or all of them.

5 GHz For wireless devices in this frequency range, there are 24 non-overlapping channels to choose from/use. Better to use in high-congestion, higher device use cases/situations. BUT…doesn't penetrate well.

Wireless – Security…

Wireless Security is generally misunderstood, ignored, or both. For most non-technical folks, wireless access and availability is both convenient and an absolute necessity in today's hectic, on-the-go, ever-on/ever-connected lifestyle.

How many of us actually stop to question whether connecting to wireless is safe or secure? Heck, don't we just want to watch cat videos, play Candy Crush, or download the menu from the new Mexican restaurant that just opened up down the street rather than ask who FBI_Surveillance_Van222 is? After all, their network's open!

Most computing devices were built with this in mind and make it "automatic" by connecting your device to any wireless network in range, or any wireless network your device remembers by name (i.e., SSID). Is this starting to scare you yet?

SSID This is the only piece of information a wireless network uses to identify or distinguish itself. There is no point to MAC (media access control) address allow listing/filtering as wireless couldn't care less about MAC addresses. Don't be fool into a false sense of security. Speaking of which…

Wireless – …Oh My!

Wireless Security Protocol / Method	Totally Unabashed Assessment
WEP (Wired Equivalency Protocol)	
WPA (Wi-Fi Protected Access) & WPS (Wi-Fi Protected Setup)	
WPA2-PSK (Pre-Shared Key)	
WPA2-Enterprise	
WPA3 (first changes in 14 years!!!)	

ALL DEKKED OUT

RUN

Wireless – Hacking and Defending

READY?

Wireless – Some General Truths/Common Sense

- WEP, WPA, and WPS are all broken – do not use them.
- There are hundreds if not more free wireless hacking programs. Easy to find, step-by-step instructions. New tools/software released regularly.
- Hacking tools available for Windows, *nix, and Mac platforms.
- Sub-groups of hackers and enthusiasts exist dedicated solely to wireless.
- Wireless hacking hardware is almost as prevalent as software. Arguably this makes it a great (better?) place to start!
- Aircrack-ng is NOT the only tool to use. ~~*Try harder.*~~ **BE BRIGHT** instead.
- Be wary of anyone offering/selling wireless guarantees, “God boxes”, panaceas, or do-it-this-way solutions.

Offense – Wireless Hacking Platform Options

Ready-Made Hacking Platforms remove a lot of the guesswork and frustration from setting up or building a wireless hacking arsenal/platform. There are multiple options available, including:

- KALI Linux – this platform is widely popular with new and experienced hackers/testers alike. It's packed with a lot of bells and whistles, but in our opinion, shows signs of commercialism that often accompanies mass adoption.

- Backbox – another Linux platform dedicated to penetration testing and security assessment. Comes with quite a few wireless assessment and testing tools pre-installed.

- Parrot OS – by the folks from Parrot Security comes yet another – surprise – Linux platform. It is Debian based likely Kali but has a lot less "bloat" to it.

- BlackArch – is an Arch-based Linux platform that comes with over 2700+ tools installed. If you're not keen on Debian-based implementations, you might want to try this one out!

Offense – Wireless Hacking Basics

Wireless Hacking relies on two (2) primary requirements for the attacker to be successful:

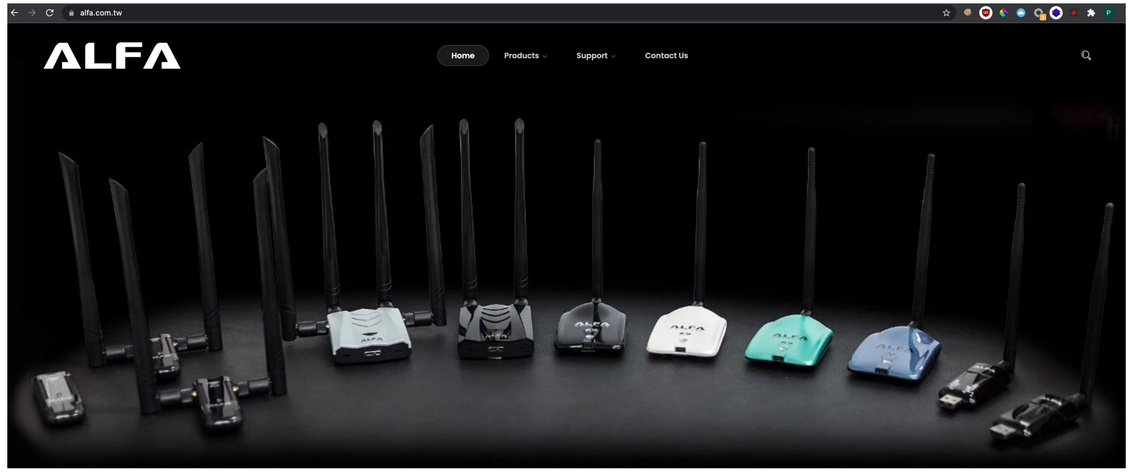
1. Monitor Mode – this mode places a wireless adapter or wireless card into a constant monitoring state, sometimes (incorrectly) referred to as promiscuous mode. Given what that word implies, one is generally up to no good when in promiscuous mode. When in Monitor Mode, you're in essence looking at EVERYONE's data versus just your own.

2. Packet Injection – packets make up the building blocks of wireless communications, and without getting overly technical they carry the data and the specifics about the data (called metadata) with them when two parties communicate. A wireless adapter using packet injection can insert itself into that communication flow and modify data or metadata by injecting other data the attacker wants into the packet. This is often referred to as man-in-the-middle (MitM) or denial of service (DoS) attacks.

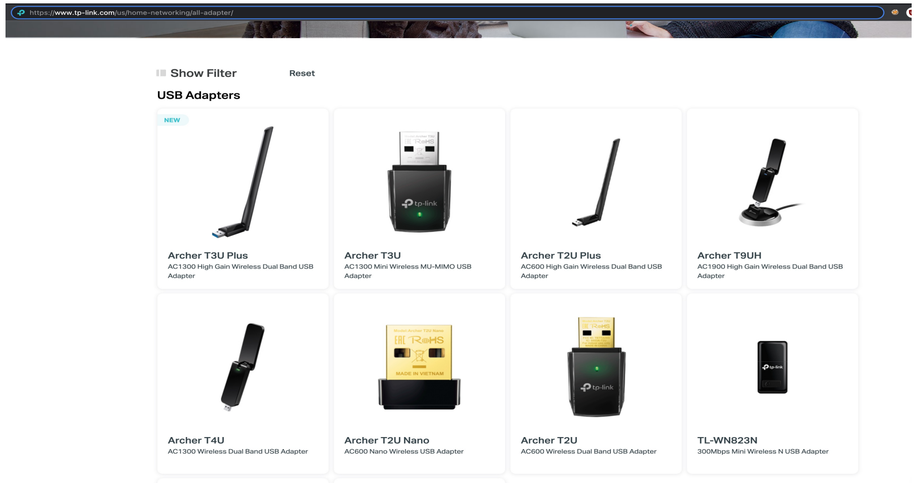
In general, most on-board or "on computer"/built in wireless radios in computers and laptops cannot support packet injection, so specialized wireless adapters must be purchased to allow for hacking.

ALL DEKKED OUT

Offense – Wireless Hacking Adapters



- Reliable
- Collectible**
- AWUS036xx
- Often imitated – watch out
  https://alfa.com.tw



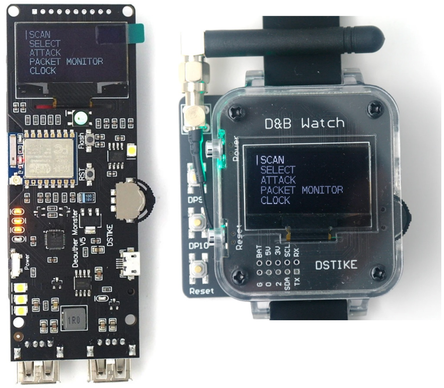
- Strong Performers
- Nano form factors
- Be sure to select right adapter
  https://www.tp-link.com

Chipsets:

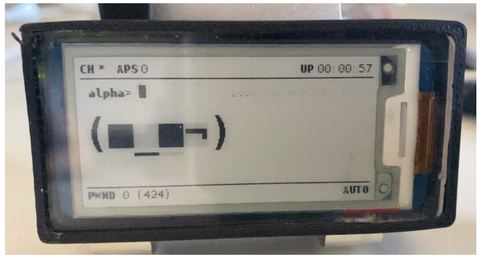
- ❖ Atheros
- ❖ Realtek

Offense – Bring on the Hardware…

WIFI Pineapple



DSTIKE Deauther
Monster & Watch



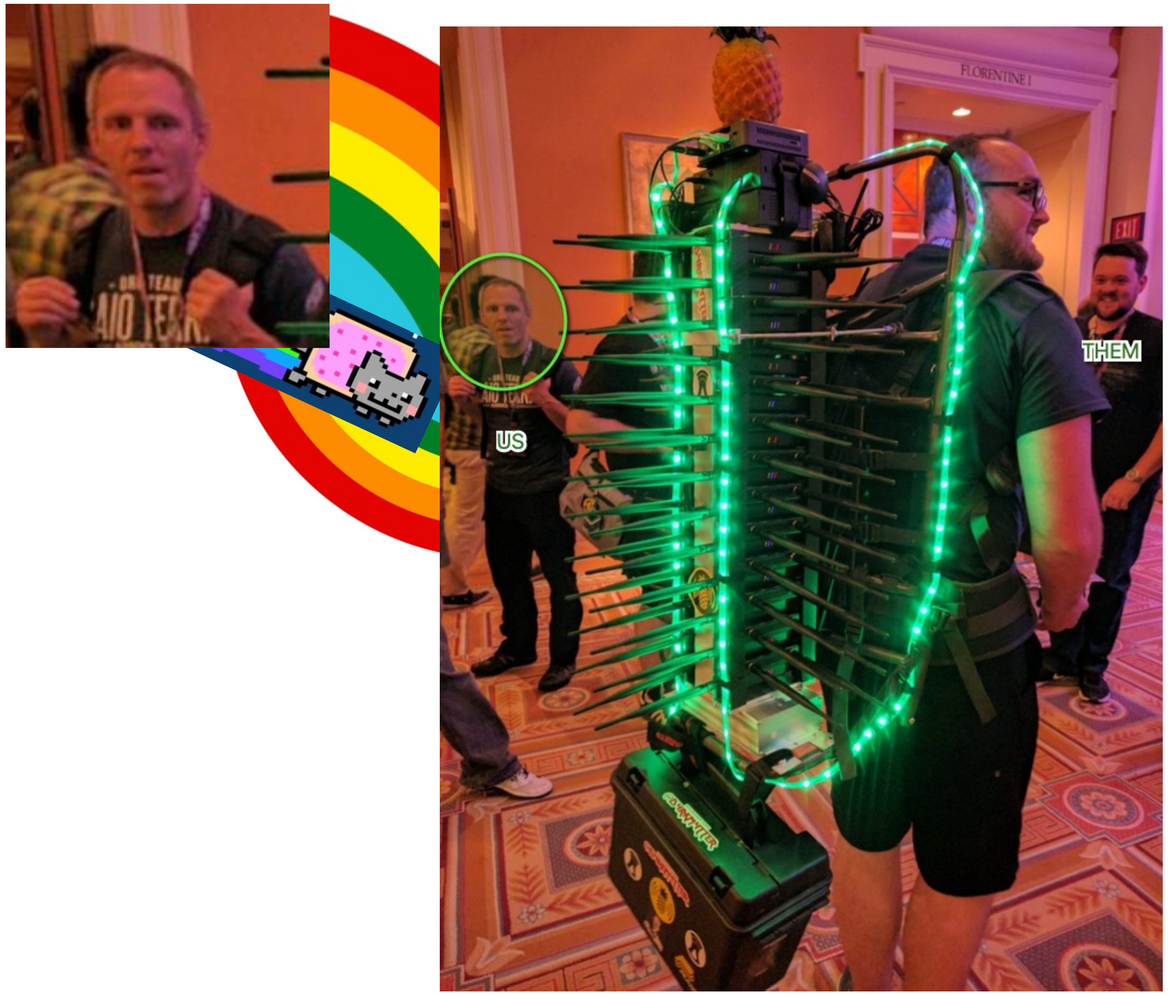
Pwnagotchi

Keysy RFID Cloner

NFC Kill Professional

Alfa AWUS036AC

Offense – But Wait, There's More?



Offense – The Hardware Keeps Going

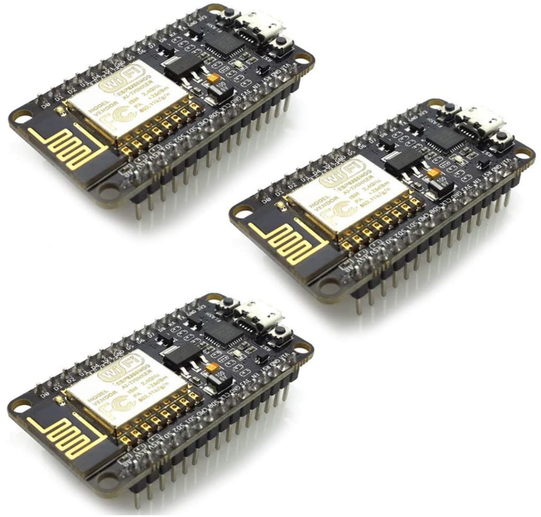
WIFI HID Injector

HackRF One

Ubertooth One

Comidox Zigbee Sniffer

Raspberry Pi (any wireless model)



HiLetGo ESP8266 or other development boards

Defense – Wireless Must Do's

- Change Default Passwords (Immediately).
- Update Router, Switch Firmware (Monthly).
- Use Wired First (Daily).
- Shut Off Bluetooth on Your Phone when You Leave Home (Daily).
- Turn Off Wireless on Your Phone when You Leave Home (Daily).
- Use a VPN (Whenever Possible).
- Don't use Your Partner/Spouse, Important Dates, Kids, Pets, Sports teams, "Password" or "1234" for a Password/PIN (Immediately).
- Choose 5GHz Before 2.4 GHz (Whenever Possible).
- Don't just ***DON'T*** use Open Public Wi-Fi.

ALL DEKKED OUT

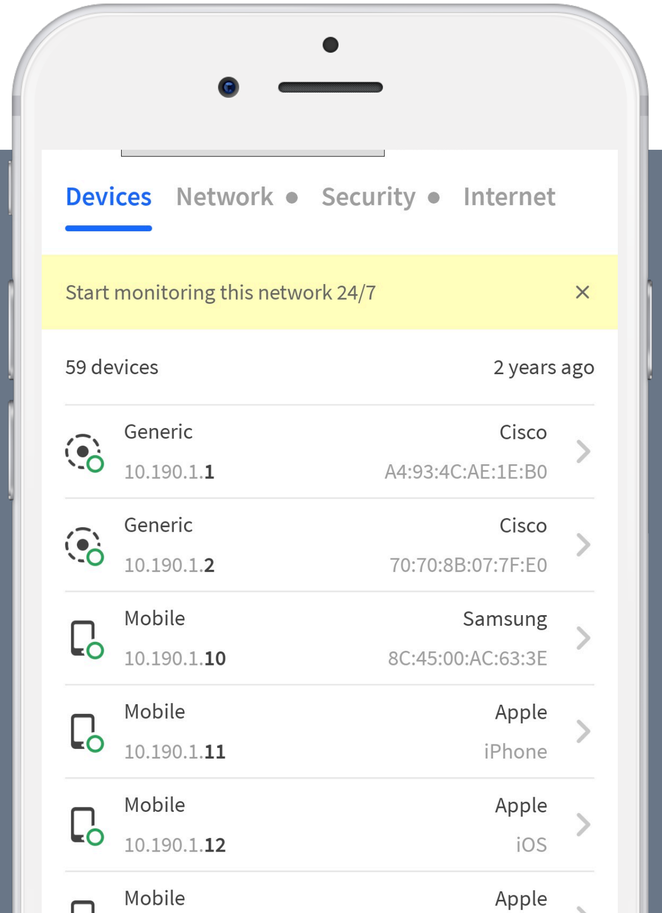
Defense – Fing Mobile App

Fing is an excellent complimentary app for providing a quick peek into devices connected to your wireless network, or for assessing wireless networks you're in range of, or are considering joining

"Free" to Use

Fing encourages payment through/by unlocking additional features, but it's still free to use.

Can scan for devices on the wireless network you're connected to, as well as provides a speed check, and updates on internet outages in 26 countries.



Limited Security Assessment

Premium (i.e., pay for) services start at $6.99 per month, or $4.92 a month if purchased on an annual basis, and offer such things as router vulnerability assessment and finding hidden cameras.

Offers open port scan without premium service.

ALL DEKKED OUT

Defense – Fingbox

Fingbox is a home market targeted appliance that provides all the functionality of the Fing app along with some additional controls, such as namely providing notification and interactive acceptance or refusal of wireless devices/clients attempting to access the network.

https://www.fing.com/products/fingbox

More Robust

Fingbox provides additional capabilities that are not possible with the Fing app.

- Schedule internet downtime or pause internet access
- Analysis bandwidth and identify choke points or data greedy devices

Security Features

- Can be configured to automatically block unknown devices.
- Monitors the network, even while you are aware with “Digital Presence”
- Same open port analysis as the app

Device is currently $99 USD

ALL DEKKED OUT

Defense – RF Shielding Paint

Fing is an excellent complimentary app for providing a quick peek into devices connected to your wireless network, or for assessing wireless networks you're in range of, or are considering joining

Effectiveness

Pros:

- Can provide great coverage and reduction especially for multi-tenant situations like apartment buildings
- Great at blocking Bluetooth and lower energy, lower power signals
- Effective for WiFi and reduces LTE

Counterpoints

Cons:

- Expensive, particularly if a lot of area to cover
- Timely to "install" properly
- Does not block 100% of wireless signals
- Likely requires an electrician

ALL DEKKED OUT

Defense – WiFi Deauth Detector

A low-cost, and low-tech from an end-user perspective for identifying and alerting on the presence of WiFi deauthentication attacks. Works by shifting LED colors and playing music. Runs off any (well, mostly any) USB power source.

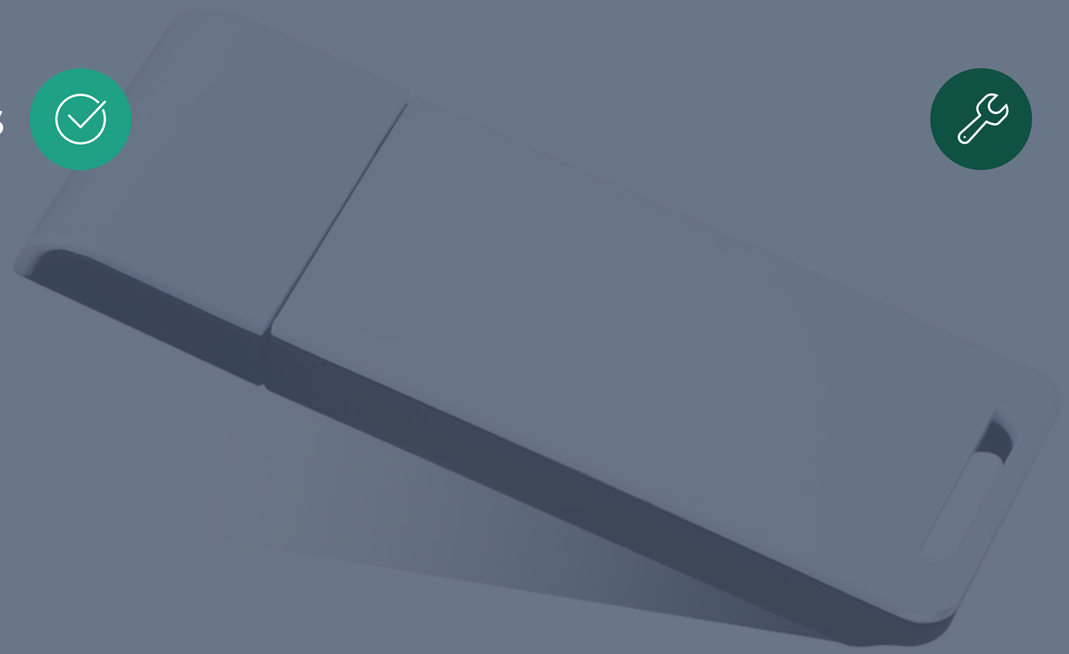
https://dstike.com

Benefits

Simple “plug it in” and forget about it design.

Moves from Green to Red LED when a deauthentication attack is detected. Plays some catchy music as well

Code is available online at Github or comes pre-flashed.



Counter

It’s limited to 2.4 GHz and cannot detect attacks against 5 GHz bands

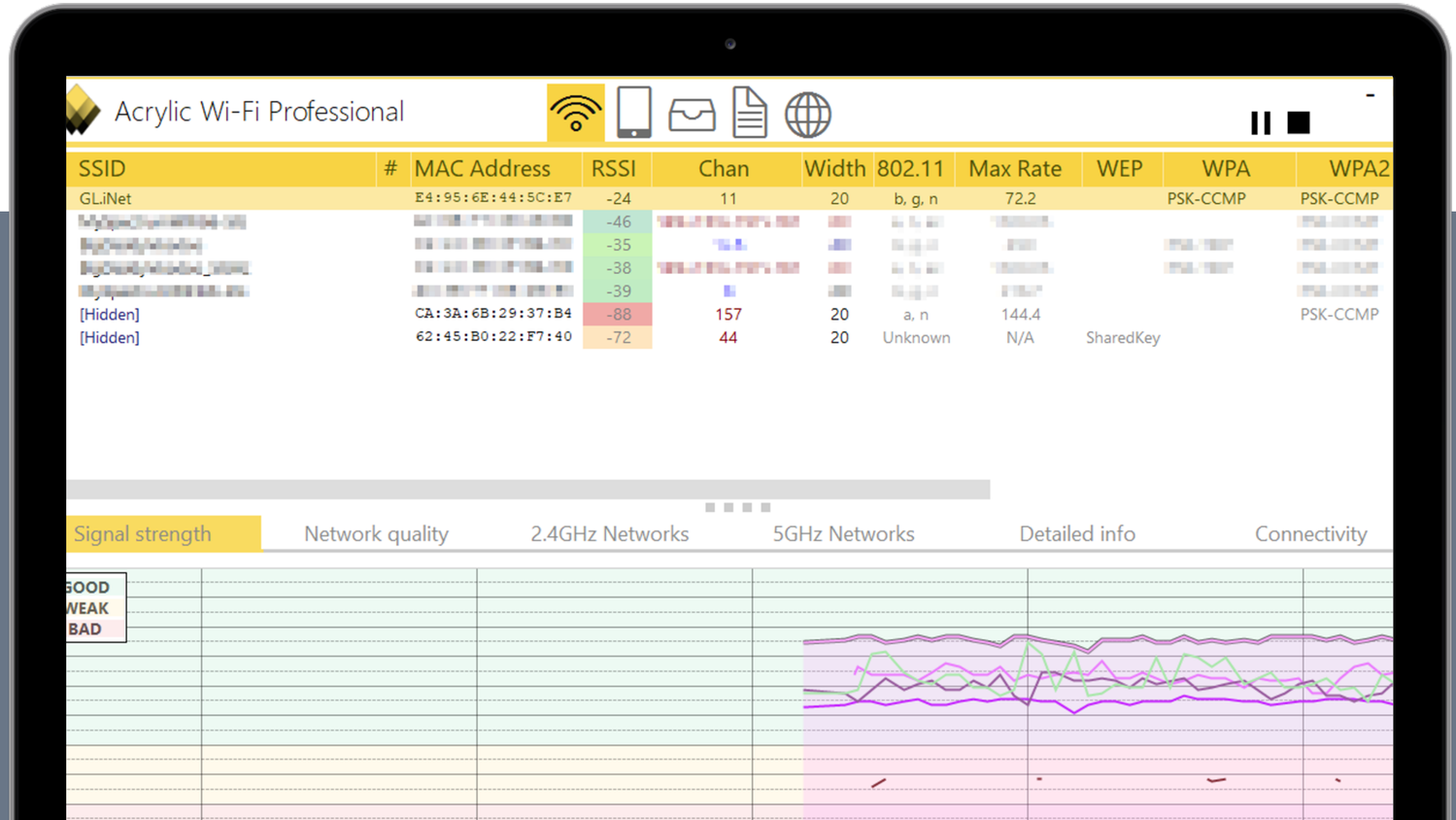
Catchy “music” can be grating/become incessant when under full deauth attack by one or more pwnagotchi – right, Doug?

ALL DEKKED OUT

Defense – Acrylic WiFi

A Windows-Only WiFi scanning and monitoring tool. Works amazingly well and takes a GPS receiver for stronger correlation and mapping. Best part - $40 USD for a lifetime license!

https://acrylicwifi.com



ALL DEKKED OUT

Defense – 2FA/U2F Authentication

There are many, many two-factor (2FA) authenticator applications available for your mobile device from Microsoft Authenticator to Duo to Google Authenticator, and so on. Try out a couple and pick one you like.

For added security, consider stepping up to U2F which provides a tangible hardware solution. Some devices available include YubiKey, Google Titan, and SoloKey.

Benefits

Requires a second form of authentication in order to access your device or data.

Works well with mobile devices and laptops alike.

Has an enterprise component in some cases like Yubico where integration is easier.

Counter

May be overkill for daily use.

Can be difficult to set up, configure or integrate if you're not particularly technical.

Assumes a level of knowledge or experience you may not have.

ALL DEKKED OUT

Defense – Password Vault/Manager

If you aren't using one of these already – kick yourself!

Password managers are great, often easy to use, and provide some relative peace of mind when used properly. But like all things, choosing the right password manager for how you work and play is essential. Check out Mooltipass.

Benefits

It has interchangeable and insertable cards for each member of the family. No more remembering your spouse, kids, or siblings passwords!

It's portable and fun-sized.

It's a cool tip to The Fifth Element!!

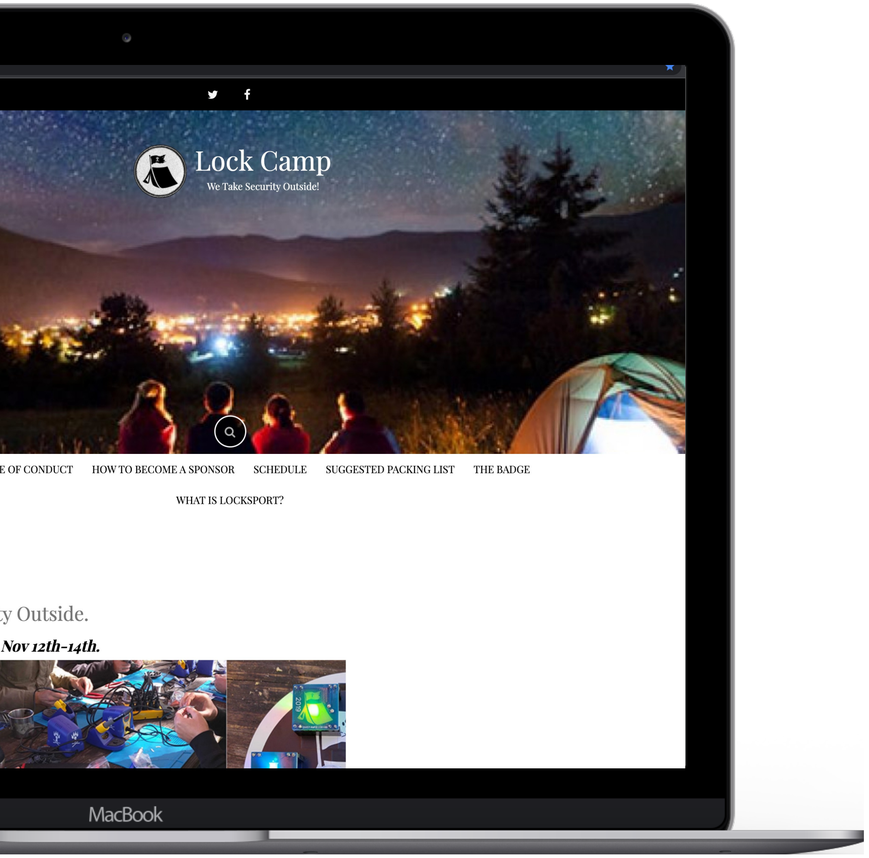
Counter

The lifespan of the turn wheel has yet to be determined.

It collects dust easily. Cleaning it with a dry cloth is fine, but wish it was easier to keep clean.

Can slow down the login process. Requires an app install.

Defense – Leveling Up



Learn to/Improve Self-Research

It may sound “cheesy” but learning to research online is a great skill to have and to continue to develop. A great place to start is searching for keywords like “wireless hacking hardware” or “how to protect my wifi”

Join a Local Group

Check this one off your list; you’re here at Lock Camp 2021! Don’t be shy – ask as many questions as you want. Guaranteed someone can and will help, or if they can’t, they can likely refer you.

READ

Get your hands on as much content as possible. Hacking conferences and other industry meet-ups are a great and free resource. They often offer slides, whitepapers, tutorials, and videos free to download. If you’re uncertain, ask around or buddy up with someone.

ALL DEKKED OUT

Q&A

Demo

ALL DEKKED OUT

Wireless – What Next?

Got Slides? Send an email to info@alldekkedout.com
Or pick up online at https://how2pentest.com/lock_camp2021
after the conference (Monday)

ALL DEKKED OUT

Thank You!