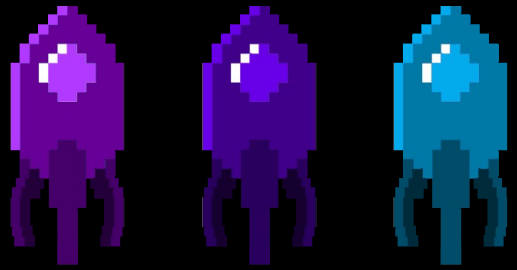
ETHERIFY

Bringing the ether back to ethernet

Jacek Lipkowski
SQ5BPF



RC3 Conference 2020

~$ whoami

Jacek Lipkowski <sq5bpf@lipkowski.org>

hobby: amateur radio operator (since 1993), callsign SQ5BPF

electronics (since forever)

making/breaking networks, unix/linux stuff, security (20+ years)

https://github.com/sq5bpf

work: at Pekao Financial Services, Poland

all opinions stated here are mine, not my employer’s

Agenda

- What is (Soft) TEMPEST
- A few words about Ethernet
- Etherify :)
- Demos :)
- Some other stuff

TEMPEST is often treated as magic

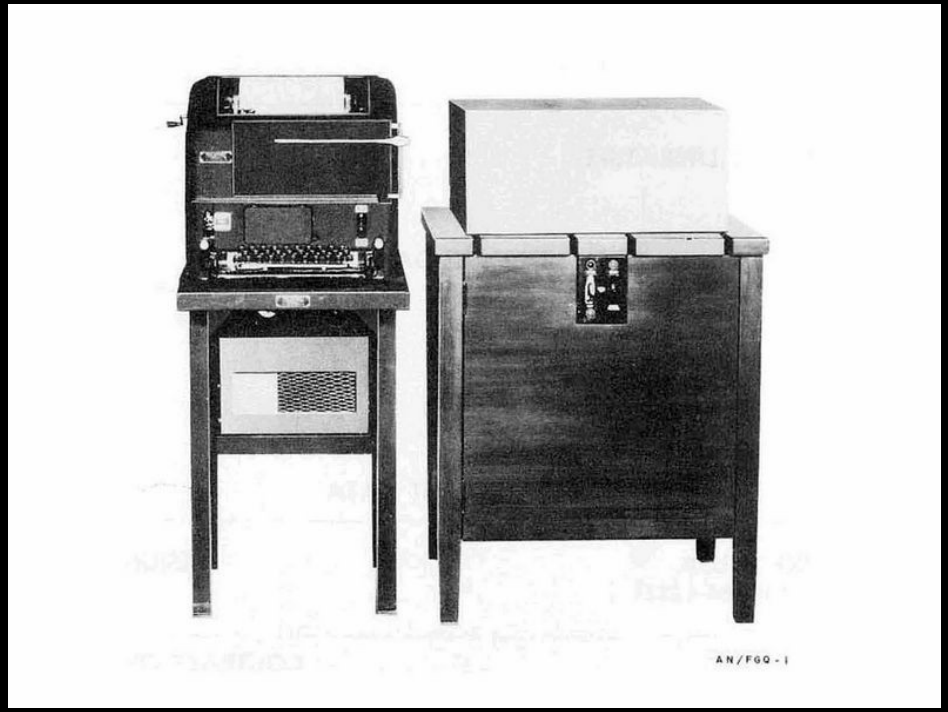
But maybe we can have a peek behind the curtain.

TEMPEST

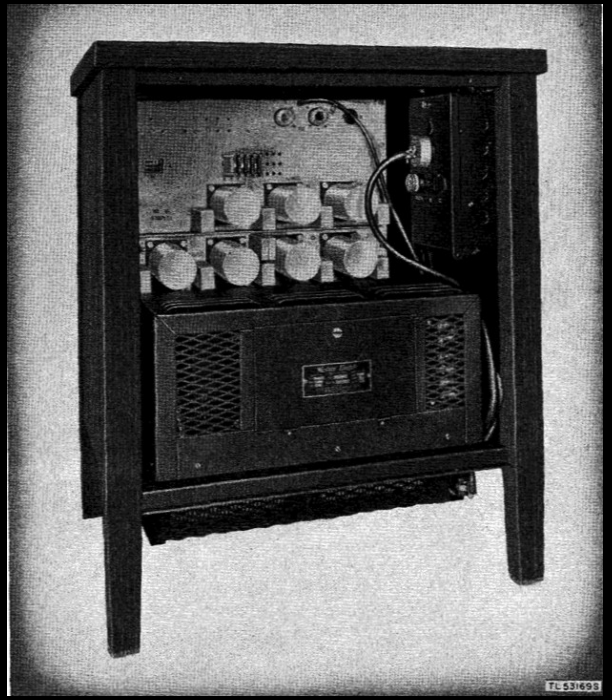
First documented discovery in 1943: a Bell AN/FGQ-1 teletype with 131-B2 mixer (XOR in a box) causes electromagnetic interference. [1]

Nothing spectacular, most electric/electronic devices cause some radio interference.

BUT: plaintext could be recovered from this interference, with the radio receiver at a large distance.



AN/FGQ-1 Teletype
Serial terminal with printer



131-B2 Mixer
XOR with key on
paper tape

TEMPEST

Problem rediscovered by CIA in 1951 (on the same equipment), got codeword TEMPEST.

Soon other channels were found (acoustic, optical etc).

The problem of electromagentic interference isn’t new, maybe someone else discovered it (Who? When? How many times?) [2]

TEMPEST

TEMPEST is a CIA codeword, but often used as a single word to describe the phenomenon (instead of “compromising emanations”).

Officially declassified in 2007 (64 years after 1943 :)

Defence: lowering emissions, masking and air-gap (controlled perimeter around the device)

Civilian TEMPEST

In 1984 Win van Eck showed that it is possible to eavesdrop remotely on CRT monitors.

See Oona's video for a modern-day implementation [6]

Today sidechannels get a lot of love: recovering keys from cryptographic devices by monitoring radio interference or power consumption etc (same as TEMPEST but at 0.5mm distance).

TEMPEST

Sidechannels:

- Electromagentic [1]
- Acoustic[1] [10]
- Optical [7]
- Thermal [8]
- Power supply [9]
- Other :) [11]

Soft TEMPEST

Modifing TEMPEST properties by software:

Turning sidechannels into covert channels for exfiltrafion (software is placed to INTENTIONALLY LEAK SECRETS).

As a countermeasure by lowering/masking emissions to make sidechannels less usable [13]

What do I care?

Exfiltration from your devices not connected to the internet:

- Keys from a HSM?
- Dedicated workstation used as a poor man's CA? :)
- Air-gapped high-risk facilities

Defence:

- Make it harder for interceptors (TEMPEST fonts in Tails) [13]
- As a fun experiment! If I can receive at 20m distance, "THEY" can do it at least 10x further

Academia

If you are to read only one article, read this:

“The Air-Gap Jumpers” Black Hat US 2018

Mordechai Guri, PhD The Head of R&D, Cyber-Security Research CenterBen-Gurion, University of the Negev, Israel

https://i.blackhat.com/us-18/Wed-August-8/us-18-Guri-AirGap.pdf

Example of academic research

„GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies”

https://www.usenix.org/system/files/sec15-paper-guri-update_v2.pdf

- Malware on a PC, receiver in GSM phone baseband software
- No source code, no raw data
- Grants ($$$), access to expensive equipment, herds of professors etc

Not something we can easily reproduce :(

(don’t get me wrong, it’s great that these guys published this in an unclassified journal).

Counter example

"Screaming Channels" Giovanni Camurati and Aurélien Francillon and François-Xavier Standaert [15]

- Source code published!
- Raw data published!
- HOWTO reproduce published!

Done right, this is how it should look like.

Unfortunately this is a rare exception, not the norm.

Military research

We know almost nothing.

- Sometimes old papers are declassified (but still redacted)
- Sometimes we get a leak or two :)

- Probably unbelievable amount of money, equipment inaccessible to mere mortals, batalions of professors, UFO technology etc

https://www.433aw.afrc.af.mil/News/Photos/igphoto/2000835639/

Amateurs

- No funds
- No expensive equipment
- We don’t know what we’re doing

- We don’t know something can’t be done
- We have cheap SDRs, zip ties, silver tape
- So let’s do a few simple Soft TEMPEST demos, to see what can be achieved.

Deluxe amateur TEMPEST receiver:

< 20 euro DVB-T dongle used as SDR
Laptop
Antenna
Chair :)

This technology is avaliable to everyone

HOWTO

- Pick a BUS with clocks in the MHz range
- Modulate it (turn it on/off, change frequency, whatever)
- See it you can receive it (at clock frequency and harmonics)
- Use a 20 euro rtl-sdr dongle and laptop as the receiver

Not that easy:

- Often clocks are spread-spectrum modulated
- Equipment has to be shielded for compliance reasons

Ethernet

UTP – unshielded twisted pair (4 balanced 100ohm lines)

STP – same as UTP, but shielded
(less radio leaks out, but more expensive)

10base-T 10Mbit/s , 20MHz clock, Manchester encoding

100base-T 100Mbit/s , 125MHz clock, 4B5B and NRZI

1000base-T 1Gb/s , 125MHz clock, 4D-PAM5

Just simple stuff: didn’t mention ethernet over fiber, coax

Ethernet MII

MII – Media Independent Interface

A standard way to connect the MAC to the PHY (physical interface)

1Gbit/s MIIs (different pin counts):

- GMII TXCLK 2.5MHz (10Mb) 25MHz (100Mb), GTXCLK 125MHz
- RGMII TXC 2.5MHz (10Mb) 25MHz (100Mb), 125MHz (1Gb)
- SGMII always 625MHz clock

Raspberry PI 4B uses RGMII.

Etherify 1

Simplest modulation: change speed via ethtool

1 is 100Mbit/s, 0 is 10Mbit/s

Use morse code, because it's easy to judge S/N by ear (and additional hack value, and amateur radio pleasure)

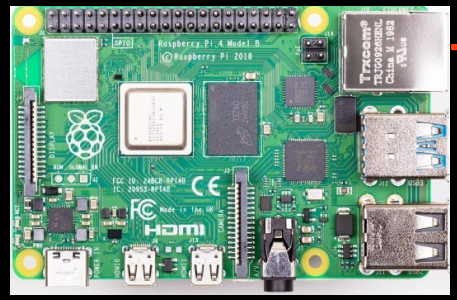
Reproductability: use two RPI 4B (yes, rpitx works too :)

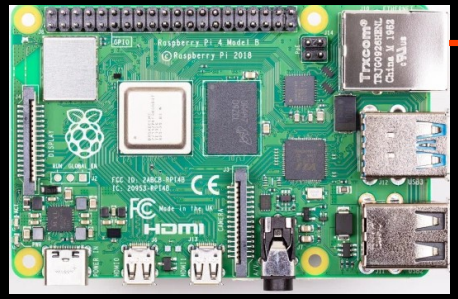
Primitive implementation etherify1.sh https://lipkowski.com/etherify

Receive at harmonics of RGMII clock (demo at 125MHz).

Result: reception at 100m distance, with 2 RPI 4B

Etherify 1 DEMO





Etherify 2

Simplest modulation: leave interface at 1Gb/s, flood it with data (via ping -f)

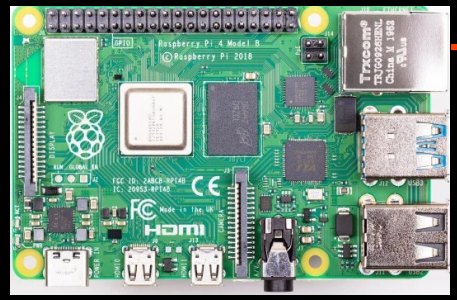
Use morse code, because it’s easy to judge S/N by ear (and additional hack value, and amateur radio pleasure)

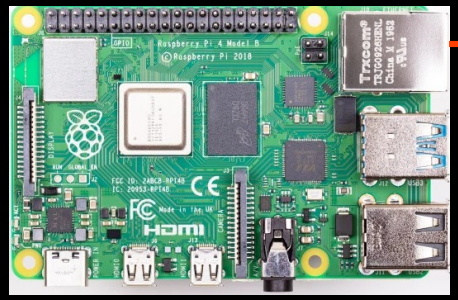
Primitive implementation etherify2.sh https://lipkowski.com/etherify

Receive at harmonics of RGMII clock (demo at 125MHz , 500MHz).

Result: reception at 30m distance, with 2 RPI 4B

Etherify 2 DEMO





Etherify 3

Didn’t connect the ethernet cable by accident (oops)

Turns out I’m still able to receive the RPI 4B at 50m

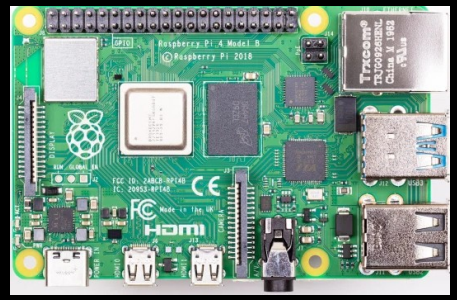
https://lipkowski.com/etherify3

The Rpi 4B generates a lot of interference

At least the two that I have, will test one from another batch some day.

This does make Etherify 1&2 less spectacular (oops again).

Etherify 3 DEMO



Etherify 4

Let’s Etherify 1 try on different hardware: Dell Laptops

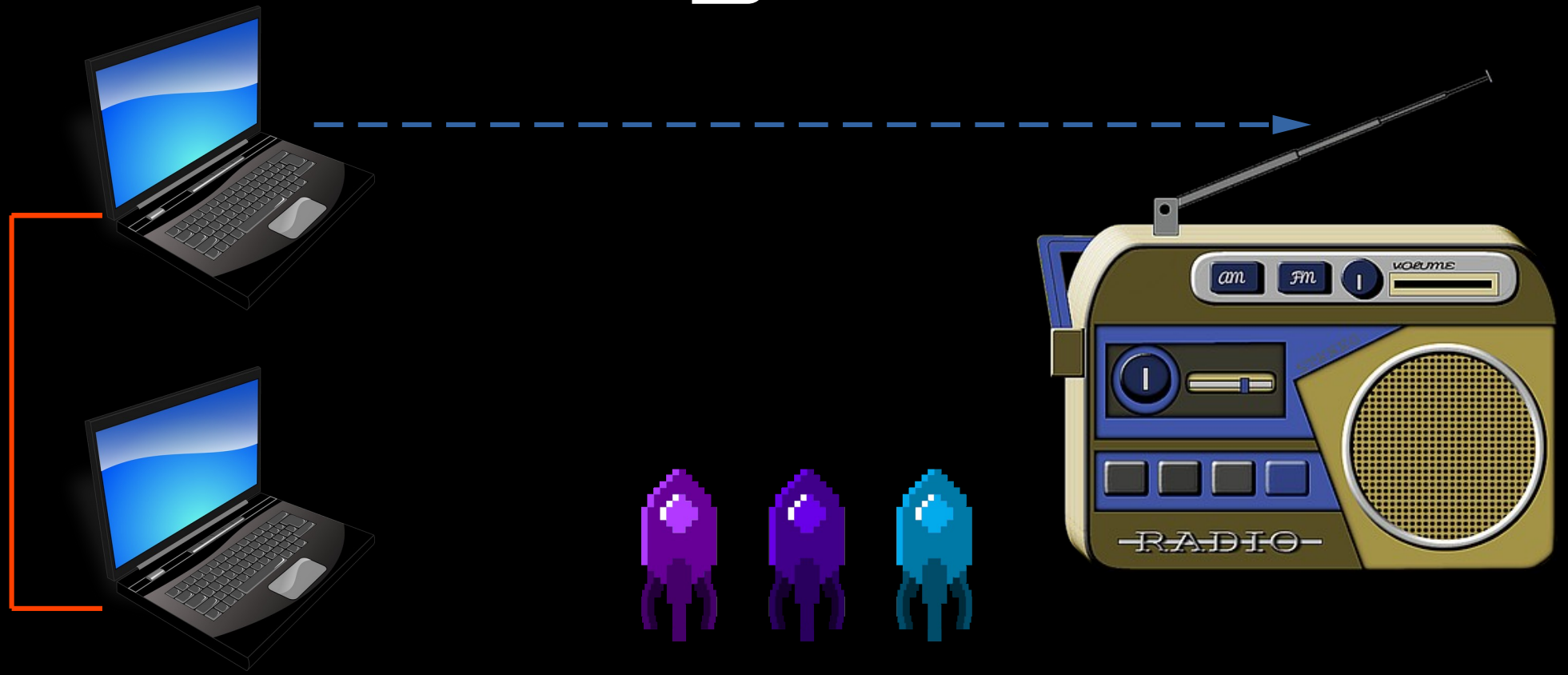
Link-up after speed change is about 2-3s, bad for regular morse code but can do QRSS CW.

Receive at harmonics of 125MHz (maybe 25MHz?), decode visually from a slow spectrogram.

Clock frequency modulation/drift when changing speed

https://lipkowski.com/etherify4

Etherify 4 DEMO



Etherify 5

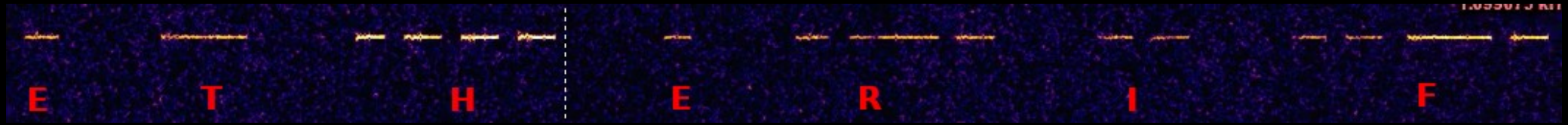
Etherify 4, but on Linksys LGS318 switches

(will try other switches, I promise)

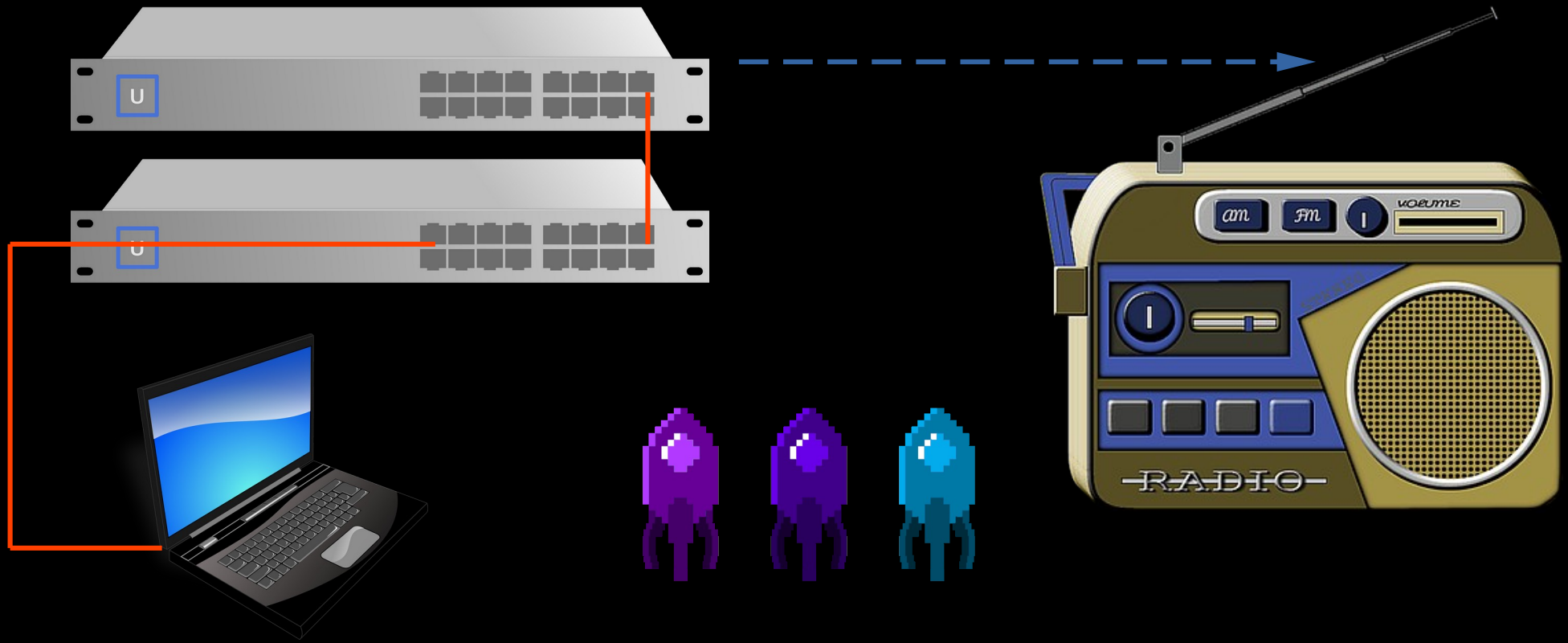
Speed is changed via SNMP

Listen at harmonics of RGMII clock (50MHz is fine)

https://lipkowski.com/etherify5



Etherify 5 DEMO



Sonify 1

This was supposed to be a collection of Soft TEMPEST demos, but got too focused on radio.

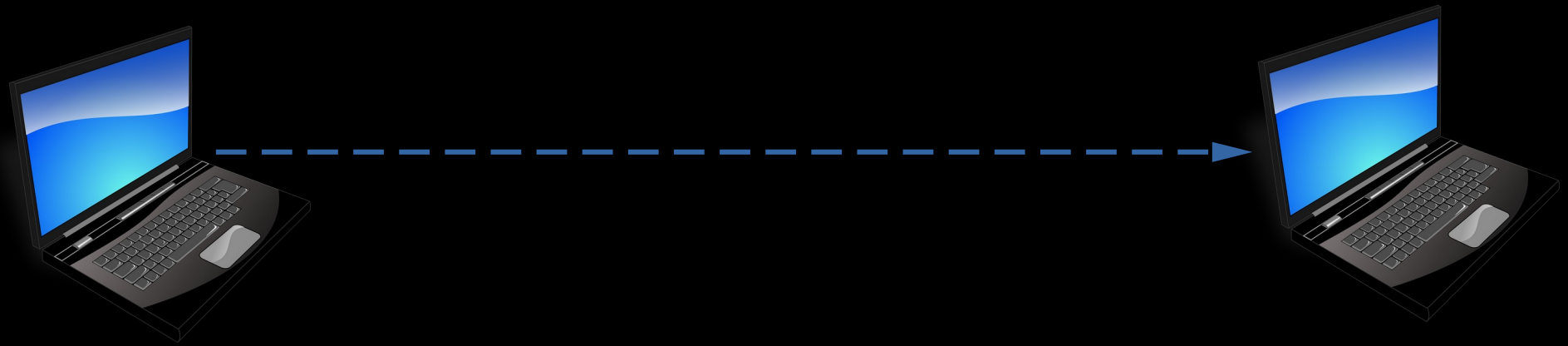
Did a quick ultrasound hack with laptop speakers (Dell Latittude 6220) and microphone (Dell Lattitude 5310).

https://lipkowski.com/sonify

Result: good reception at 21.5kHz distance 20m. Can be extended with an ultrasound directional microphone.

Sonify 1 DEMO

If we have time left :)



TODO

Test on other hardware

Look at data encoding (this is what espthernet does)

Look at the e1000e (and other) NIC registers, play around with PLL settings/clock frequencies if possible

Implement other simple Soft TEMPEST demos (optical)

Keep it as primitive as possible.

Try it yourself

Get a cheap RTL-SDR dongle if you still don’t have one

Try one of these demos

Remember that this is as primitive as possible on purpose. This is a fun demo, not a military data exfiltration exercise :)

Literature

[1] „TEMPEST: a signal problem” (1972) https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/cryptologic-spectrum/tempest.pdf

[2] „How old is TEMPEST?” http://cryptome.org/tempest-old.htm

[3] „TEMPEST 101” http://www.tscm.com/TSCM101tempest.html

[4] „Spycatcher” Peter Wright

[5] „Electromagnetic Radiation from VideoDisplay Units: An Eavesdropping Risk?” Wim van Eck http://www.tscm.com/vaneck85.pdf

[6] „TEMPEST HDMI demo” Oona Räisänen

https://www.youtube.com/watch?v=BpNP9b3aIfY

Literature

[7] https://www.researchgate.net/publication/327173348_Optical_TEMPEST

[8] „BitWhisper: Covert Signaling Channel between Air-Gapped Computersusing Thermal Manipulations” https://arxiv.org/pdf/1503.07919.pdf

[9] „PowerHammer: Exfiltrating Data from Air-GappedComputers through Power Lines” https://arxiv.org/pdf/1804.04014.pdf

[10] „Acoustic Surveillance of Physically Unmodified Pcs” http://seclab.illinois.edu/wp-content/uploads/2011/03/LeMayT06.pdf

[11] „ODINI : Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields” https://arxiv.org/pdf/1802.02700.pdf

[12] https://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf

Literature

[13] “Soft Tempest - An Opportunity for NATO” Ross J. Anderson, Markus G. Kuhn https://www.cl.cam.ac.uk/~rja14/Papers/nato-tempest.pdf

[14] „GSMem: Data Exfiltration from Air-Gapped Computers over GSM Frequencies” https://www.usenix.org/system/files/sec15-paper-guri-update_v2.pdf

[15] “Screaming Channels” Giovanni Camurati and Aurélien Francillon and François-Xavier Standaert https://eurecom-s3.github.io/screaming_channels/

Questions?

VY 73

Jacek / SQ5BPF

sq5bpf@lipkowski.org