Digital Interruption

Software Defined Radio

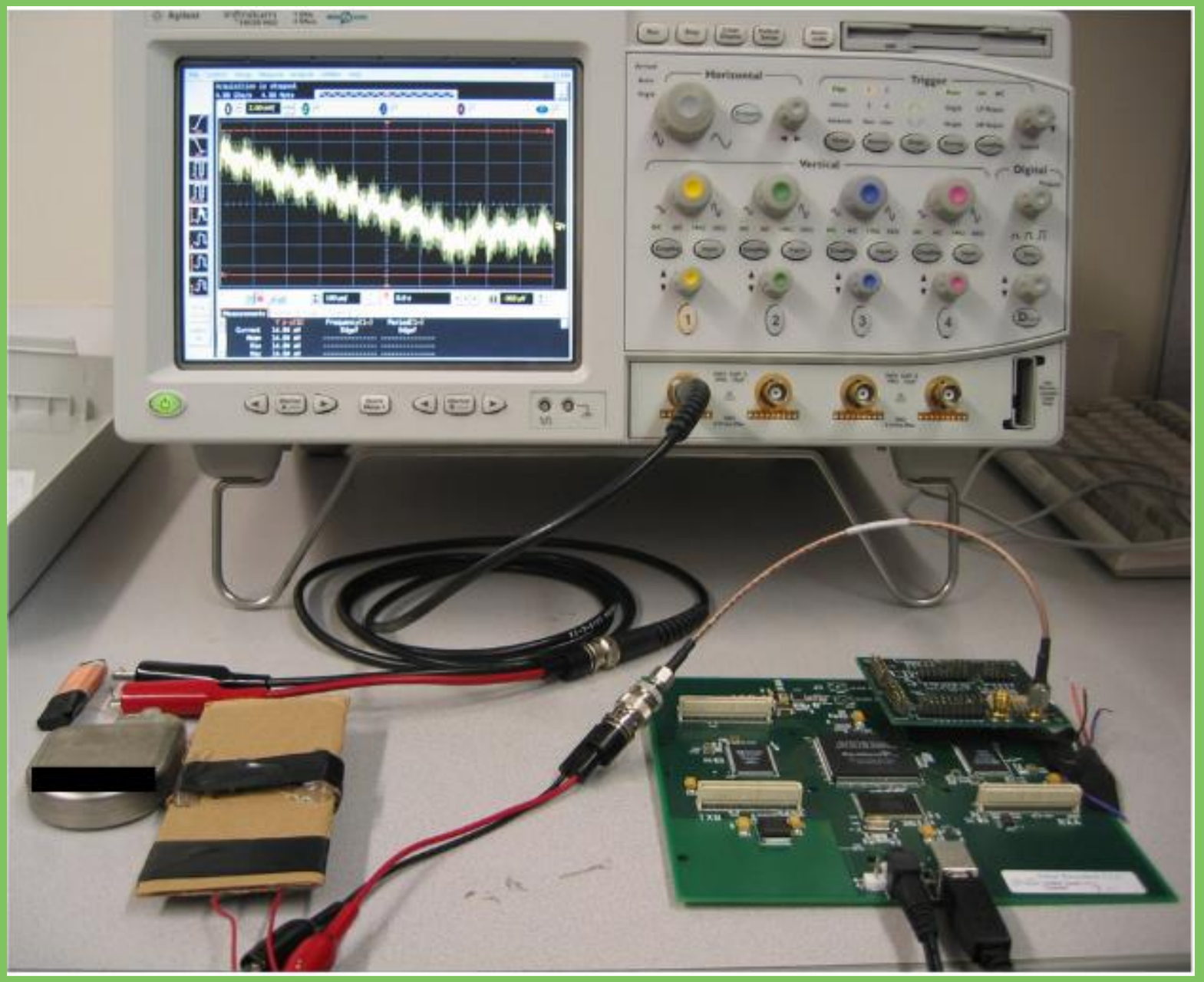
Attacking Wireless Communications with low cost SDR

Jahmel Harris

+44 (0)161-820-3056

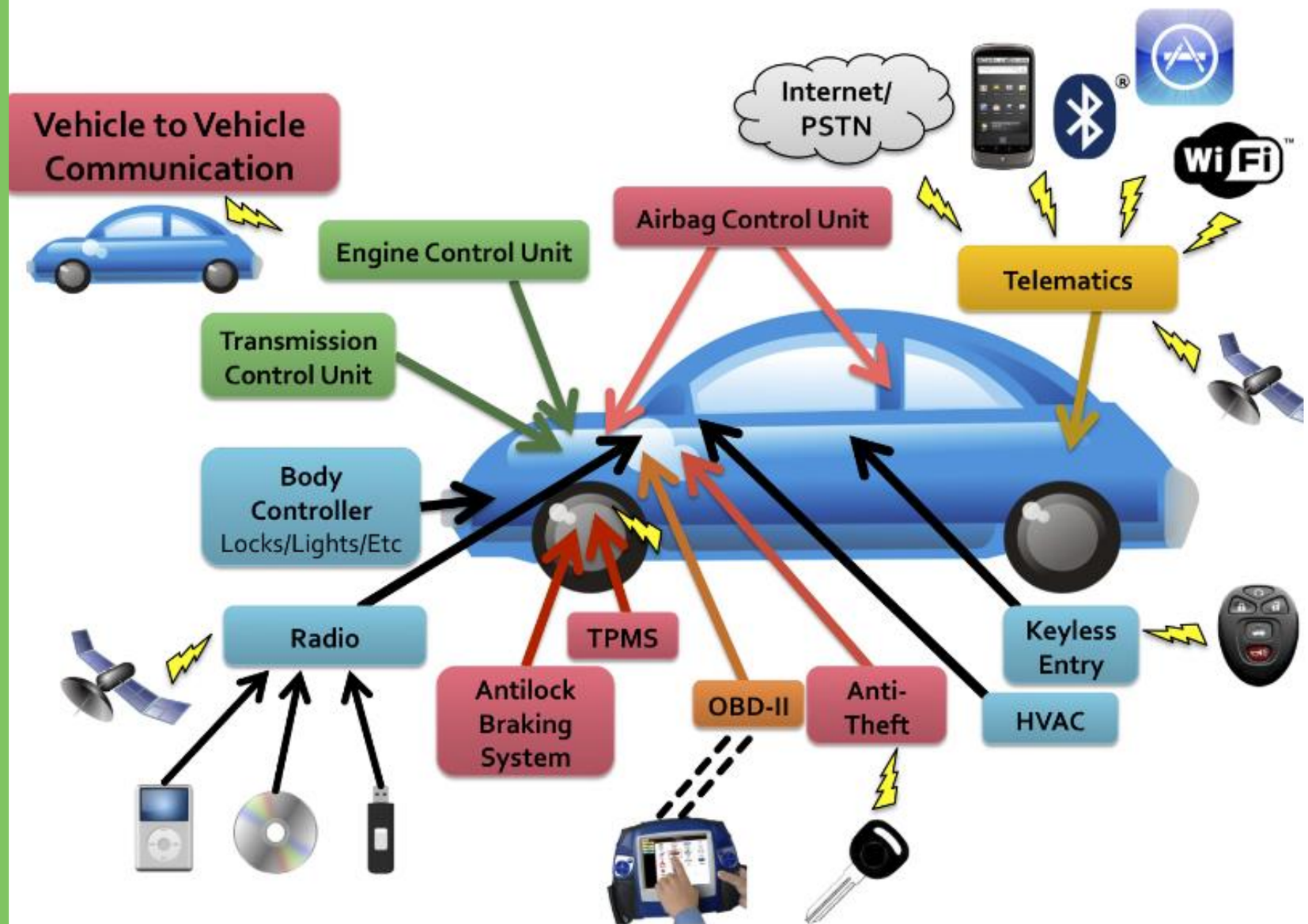
www.digitalinterruption.com

jahmel@digitalinterruption.com



Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and zero-power defenses

DIGITAL INTERRUPTION


Vehicle to Vehicle Communication
Internet/ PSTN
Wi Fi
Airbag Control Unit
Engine Control Unit
Telematics
Transmission Control Unit
Body Controller Locks/Lights/Etc
Radio
TPMS
Antilock Braking System
OBD-II
Anti-Theft
Keyless Entry
HVAC


MPH
0
20
40
60
80
100
120
140
Pwned by CarShark
CARSHARKED X_X
P R N D 3 2 1

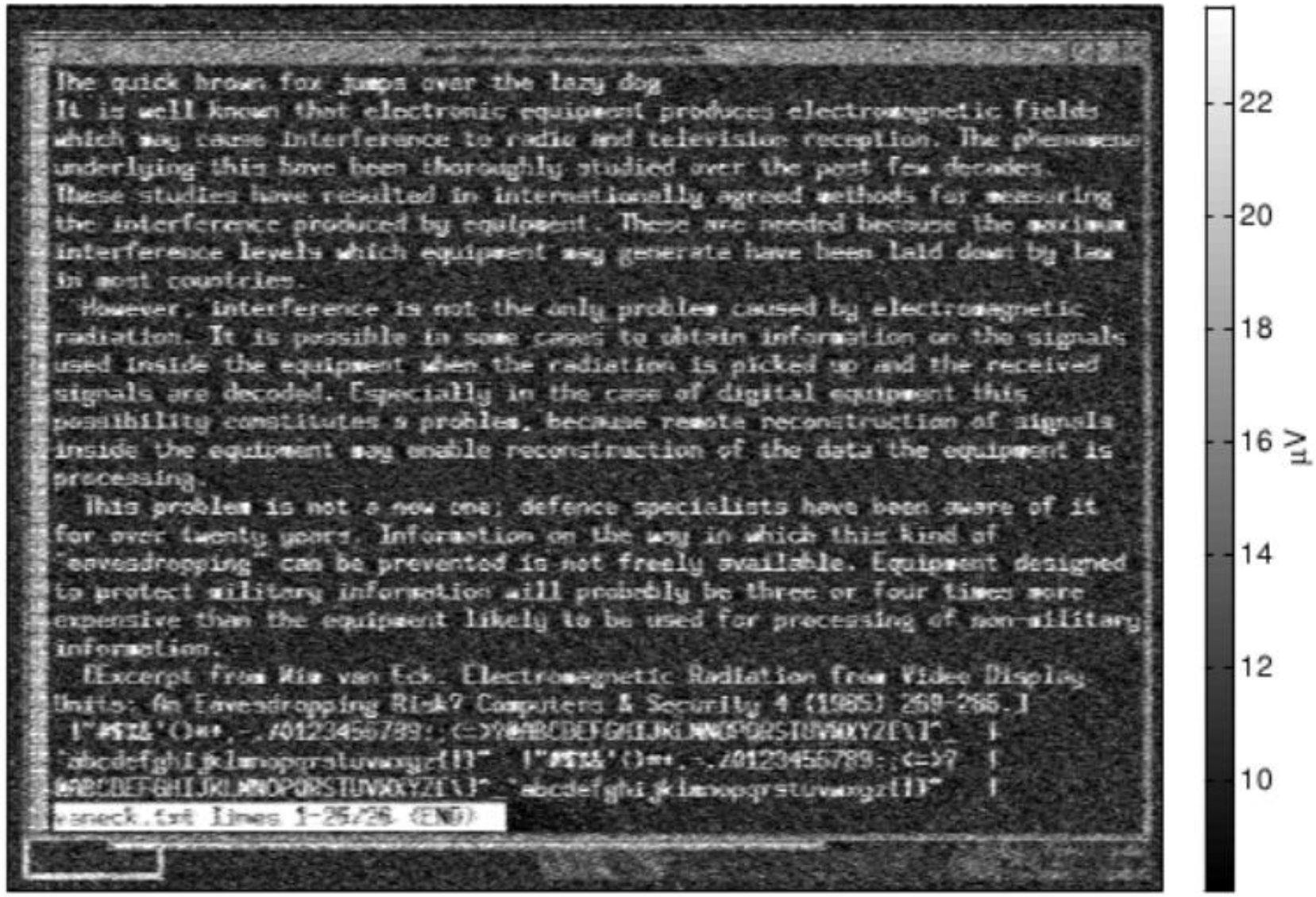


Figure 4.3: Text signal received from a 440CDX laptop at 10 m distance through two intermediate offices (3 plasterboard walls).

Whoami

Jahmel Harris
@JayHarris_Sec

Freelance Security Consultant and researcher
@DI_Security

Manchester Grey Hats
@mcrgreyhats

Mobile|Radio|Reverse Engineering

Section:

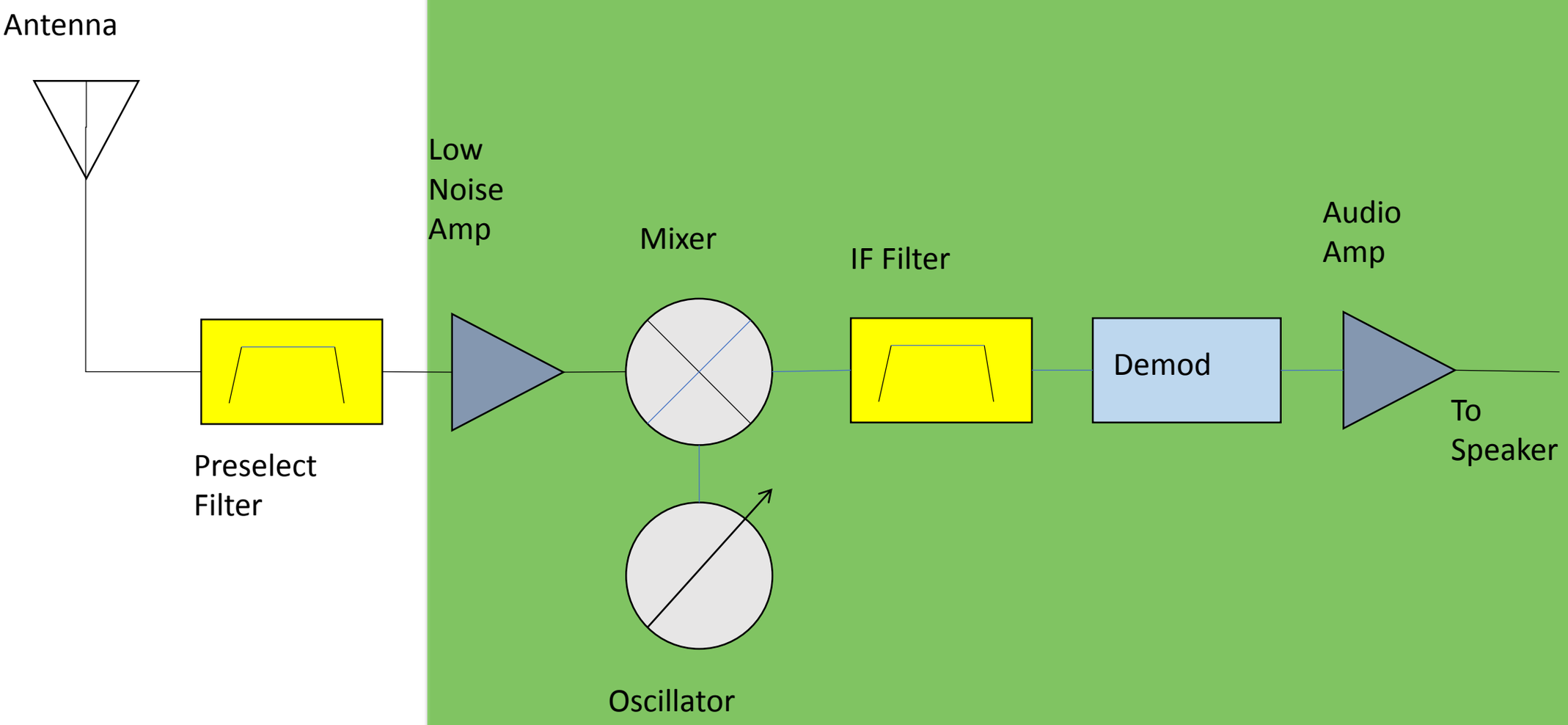
Introduction to Software Defined Radio

Attacking Radio Systems

Reading Data from the air

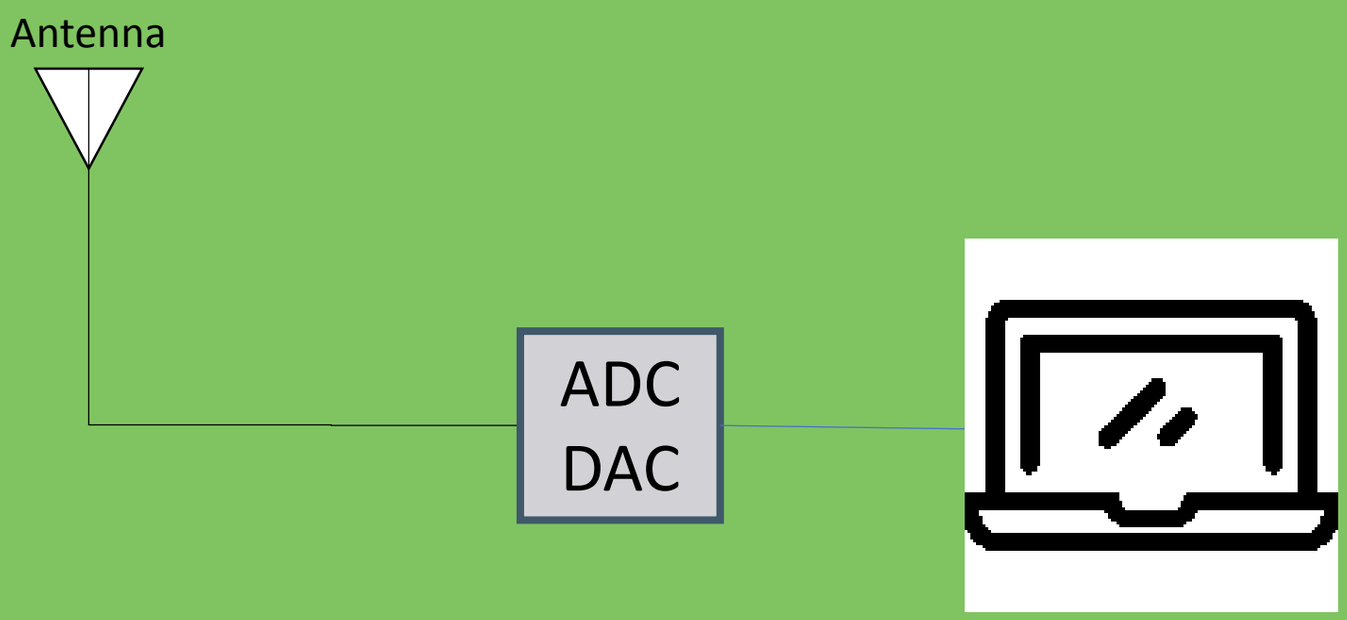
Common wireless protocols

Introduction to SDR



DIGITAL INTERRUPTION

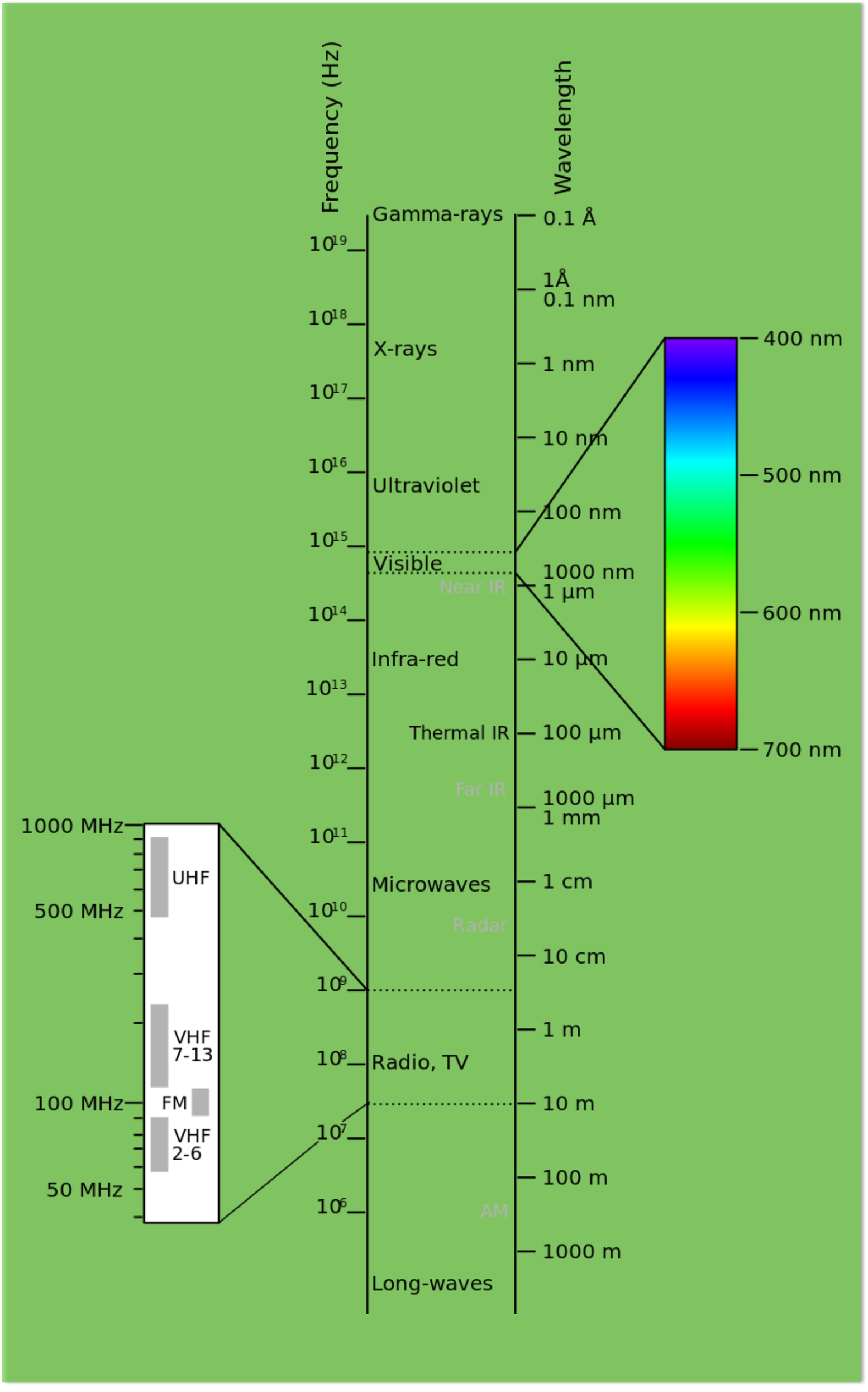
Introduction to SDR

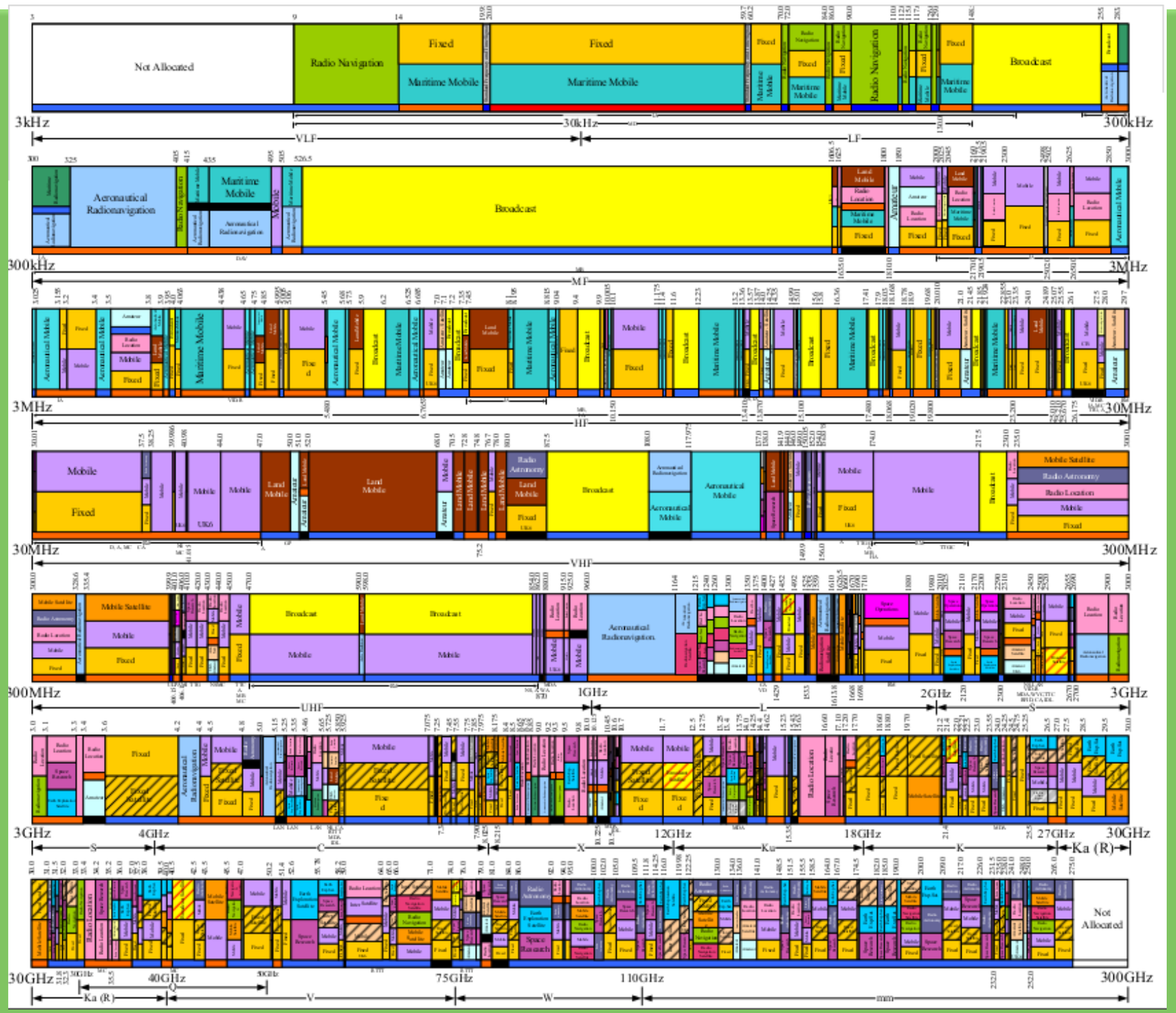


DIGITAL INTERRUPTION

	USRP*	HackRF One	RTLSDR
Frequency Range	1MHz–6000MHz	1MHz-6000MHz	24MHz-1766MHz
Bandwidth	16-61MHz	20MHz	2MHz
Sample Rate	8-128 MS/s	20 MS/s	2.5 MS/s
Rx/Tx	Full Duplex	Half Duplex	Receive Only
Price	£600-£4500	£230	£10

DIGITAL INTERRUPTION


Frequency (Hz)
Wavelength
Gamma-rays
0.1 Å
10^19
1Å
0.1 nm
10^18
X-rays
1 nm
10^17
10 nm
10^16
Ultraviolet
100 nm
10^15
Visible
1000 nm
Near IR
1 µm
10^14
Infra-red
10 µm
10^13
Thermal IR
100 µm
10^12
Far IR
1000 µm
1 mm
10^11
Microwaves
1 cm
10^10
Radar
10 cm
10^9
1 m
10^8
Radio, TV
10 m
10^7
100 m
10^6
AM
1000 m
Long-waves
400 nm
500 nm
600 nm
700 nm
1000 MHz
UHF
500 MHz
VHF
7-13
100 MHz
FM
VHF
2-6
50 MHz



The UK Frequency Allocations (http://www.roke.co.uk/resources/datasheets/uk-frequency-allocations.pdf)

DIGITAL INTERRUPTION

Bluetooth™ 4.0

ZigBee®

lte™

Wi Fi ALLIANCE

GSM™

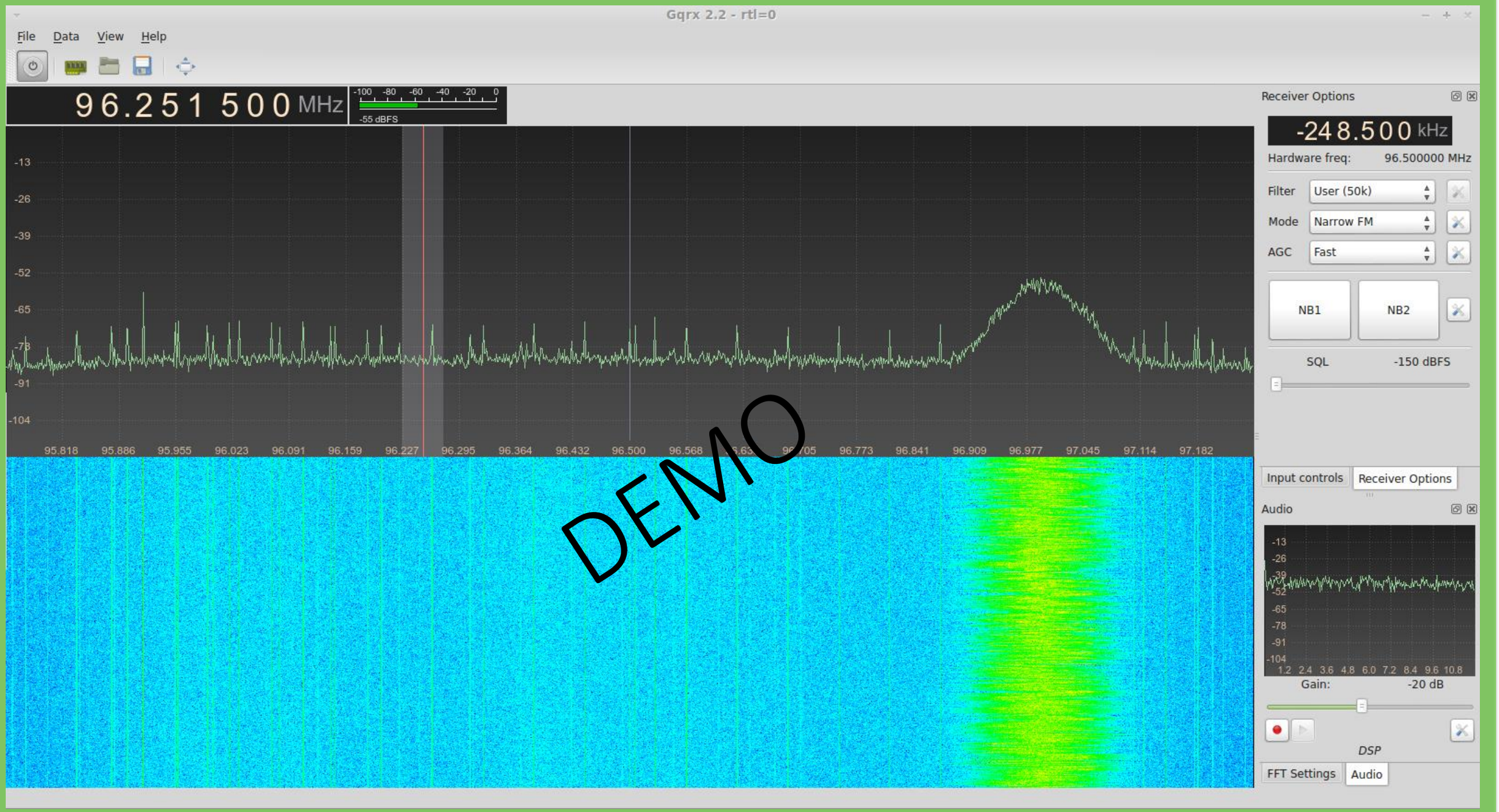
DIGITAL INTERRUPTION

INTERRUPTION

Security won't get better until tools for practical exploration of the attack surface are made available

Joshua Wright, 2011

DIGITAL INTERRUPTION



DIGITAL INTERRUPTION

Section:

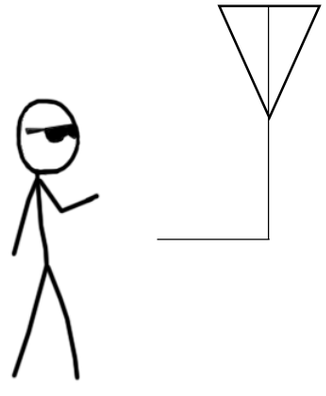
Introduction to Software Defined Radio

Attacking Radio Systems

Reading Data from the air

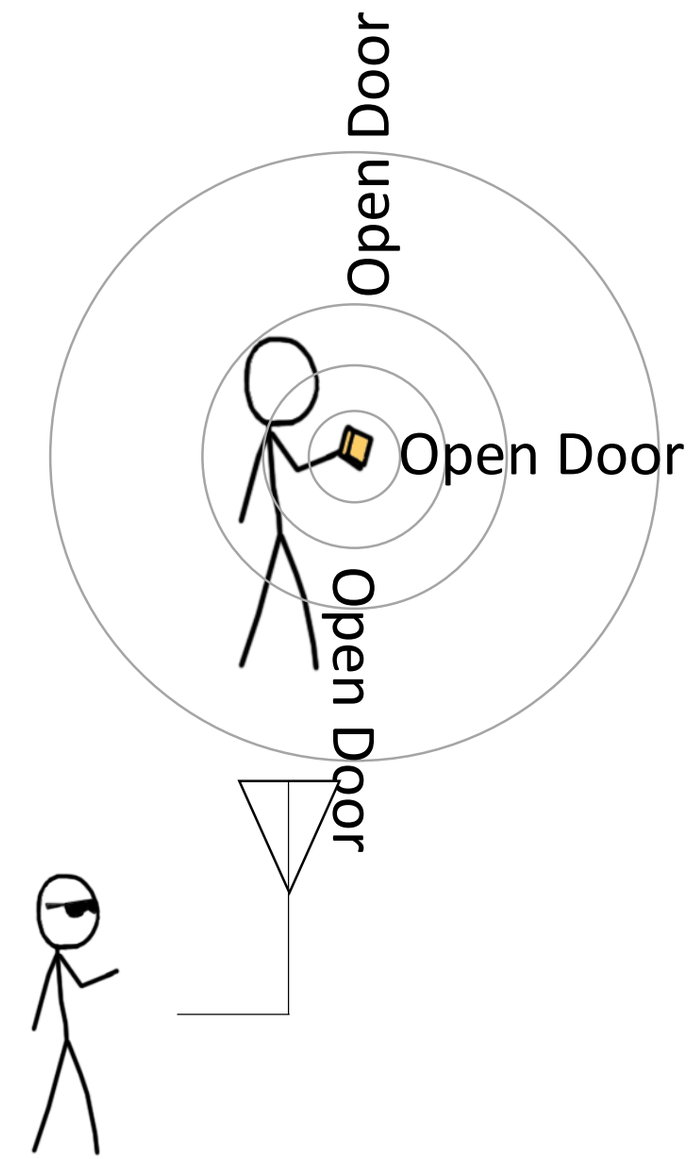
Common wireless protocols

Replay Attacks



DIGITAL INTERRUPTION

Replay Attacks

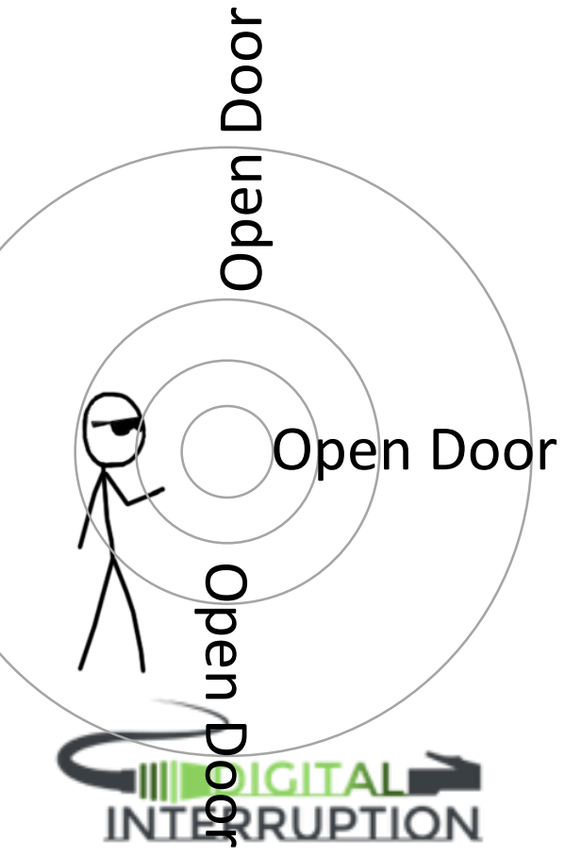


DIGITAL INTERRUPTION

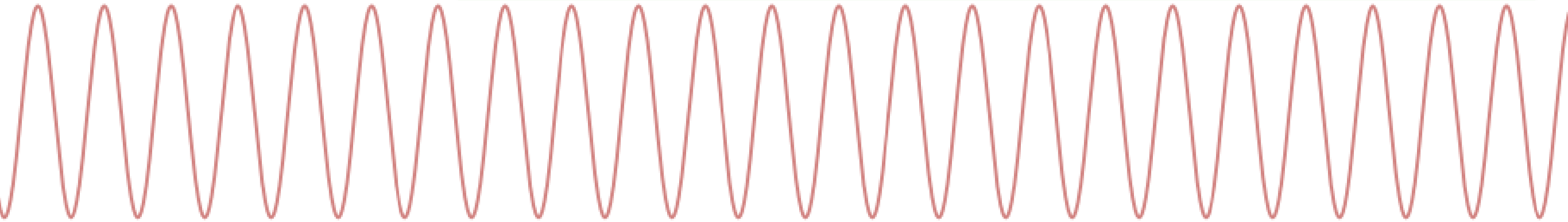
Replay Attacks

DIGITAL INTERRUPTION

Replay Attacks



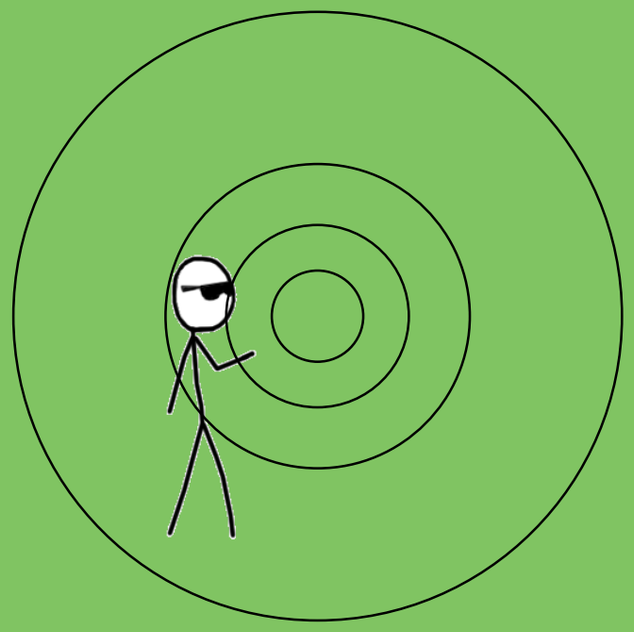
Data Recovery



1001101100101011000110111001001100101011101000100010001100001011101000110000 1

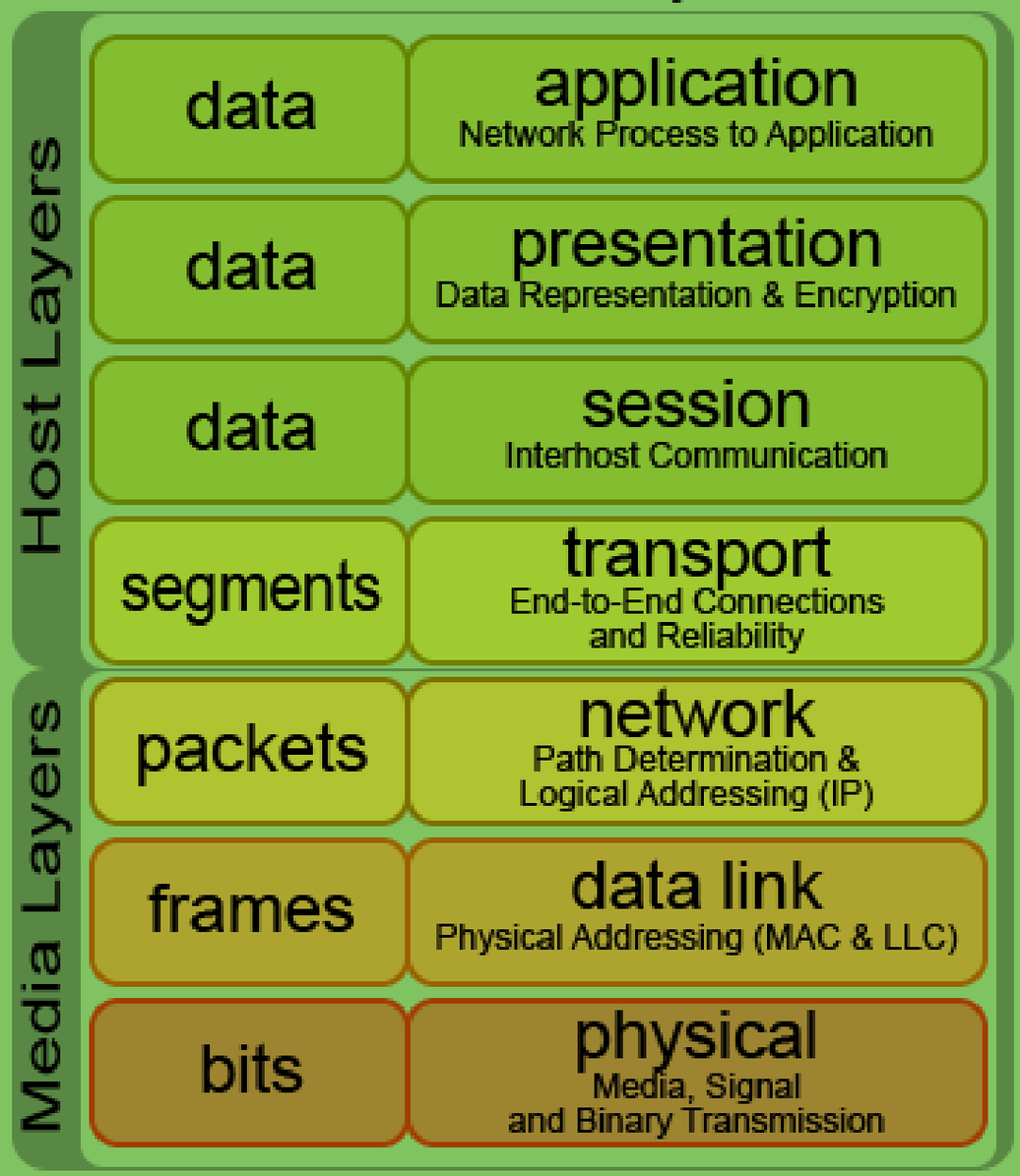
DIGITAL INTERRUPTION

Denial of Service



DIGITAL INTERRUPTION

Fuzzing



00101010010

DIGITAL INTERRUPTION

kingavonDoorbellPlayData.grc (read only) - /home/harrisj/clientWork/MWR/briefing2014/demo/scripts - GNU Radio Companion

File Edit View Build Tools Help

untitled ✖ kingavonDoorbellPlayData (ro) ✖

Options
ID: top_block
Generate Options: WX GUI

Variable
ID: samp_rate
Value: 2M

File Source
File: ...187200_2000000.cfile
Repeat: Yes
out

osmocom Sink
Sample Rate (sps): 2M
Ch0: Frequency (Hz): 432.187M
Ch0: Freq. Corr. (ppm): 0
Ch0: RF Gain (dB): 10
Ch0: IF Gain (dB): 20
Ch0: BB Gain (dB): 20
in

WX GUI Waterfall Sink
Title: Waterfall Plot
Sample Rate: 2M
Baseband Freq: 0
Dynamic Range: 100
Reference Level: 0
Ref Scale (p2p): 2
FFT Size: 512
FFT Rate: 15
Freq Set Varname: None
in

WX GUI FFT Sink
Title: FFT Plot
Sample Rate: 2M
Baseband Freq: 0
Y per Div: 10 dB
Y Divs: 10
Ref Level (dB): 0
Ref Scale (p2p): 2
FFT Size: 1.024k
Refresh Rate: 15
Freq Set Varname: None
in

DEMO

[ACARS]
[Audio]
[Boolean Operators]
[Byte Operators]
[Channelizers]
[Channel Models]
[Coding]
[Control Port]
[Debug Tools]
[Deprecated]
[DOA]
[Equalizers]
[Error Coding]
[Error Correction]
[FasTrak]
[FCD]
[File Operators]
[Filters]
[Fourier Analysis]
[Graphical Sinks]
[GUI Widgets]
[Impairment Models]
[Instrumentation]
[IQ Balance]
[Level Controllers]
[Math Operators]
[Measurement Tools]
[Message Tools]
[Misc]

Loading: "/home/harrisj/untitled.grc"
>>> Done

DIGITAL INTERRUPTION

Section:

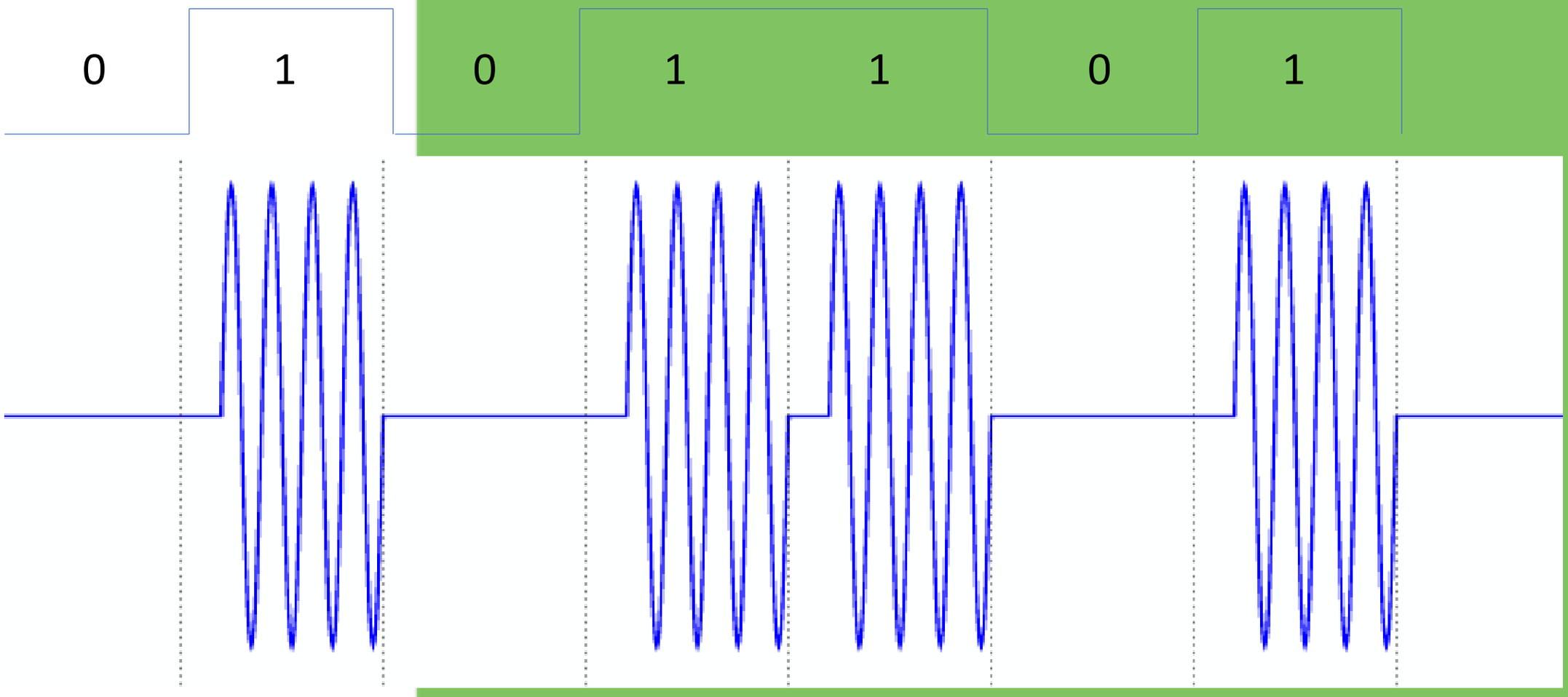
Introduction to Software Defined Radio

Attacking Radio Systems

Reading Data from the air

Common wireless protocols

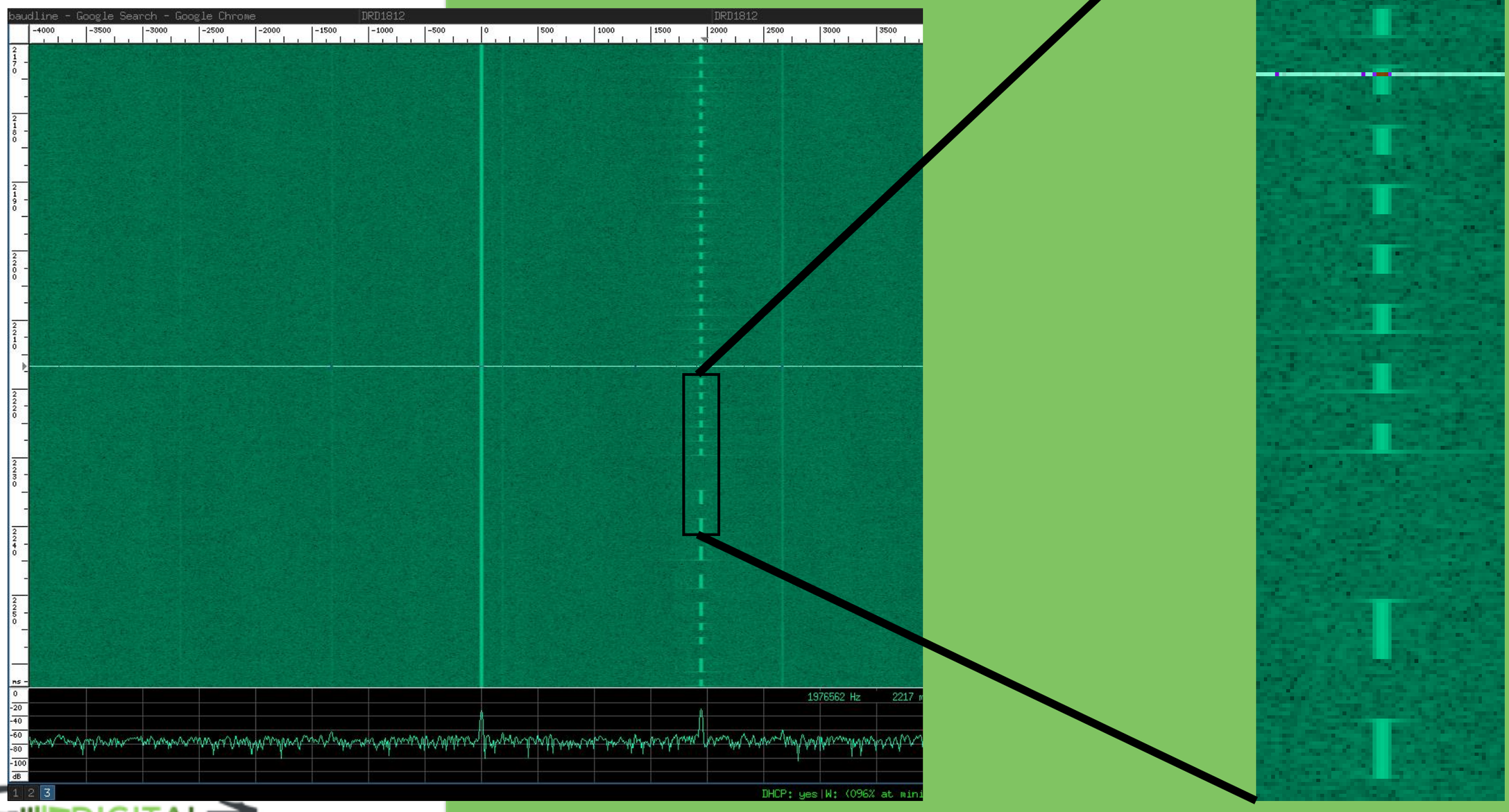
OOK(On Off Keying) Overvierw



http://www.st-andrews.ac.uk/~www_pa/Scots_Guide/RadCom/part19/fig1.gif

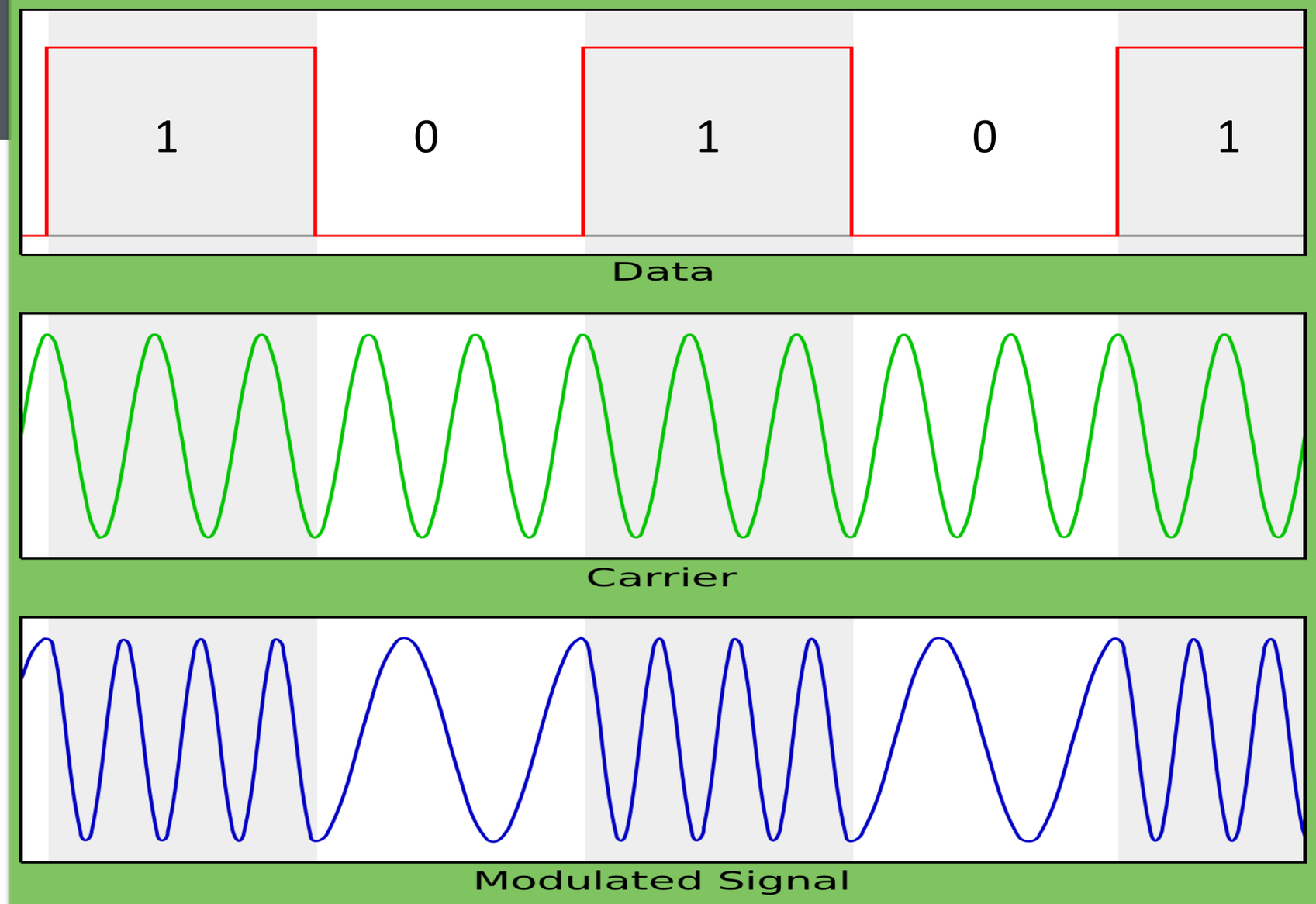
DIGITAL INTERRUPTION

Identifying OOK



DIGITAL INTERRUPTION

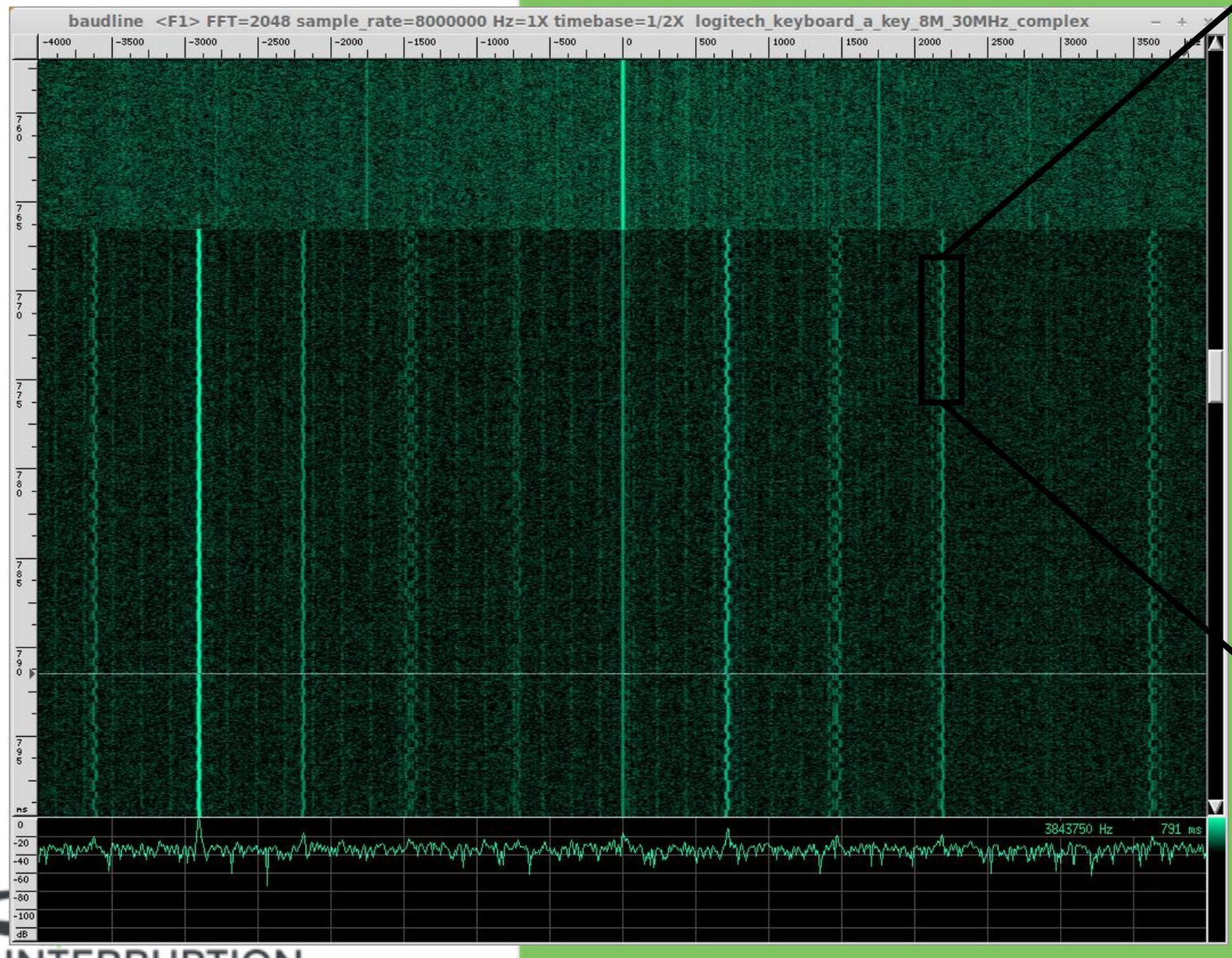
FSK (Frequency Shift Keying) Overview

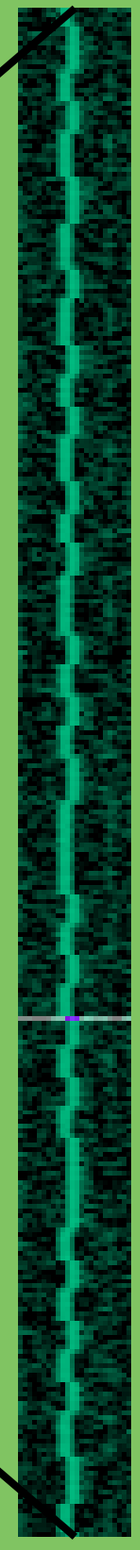


DIGITAL INTERRUPTION

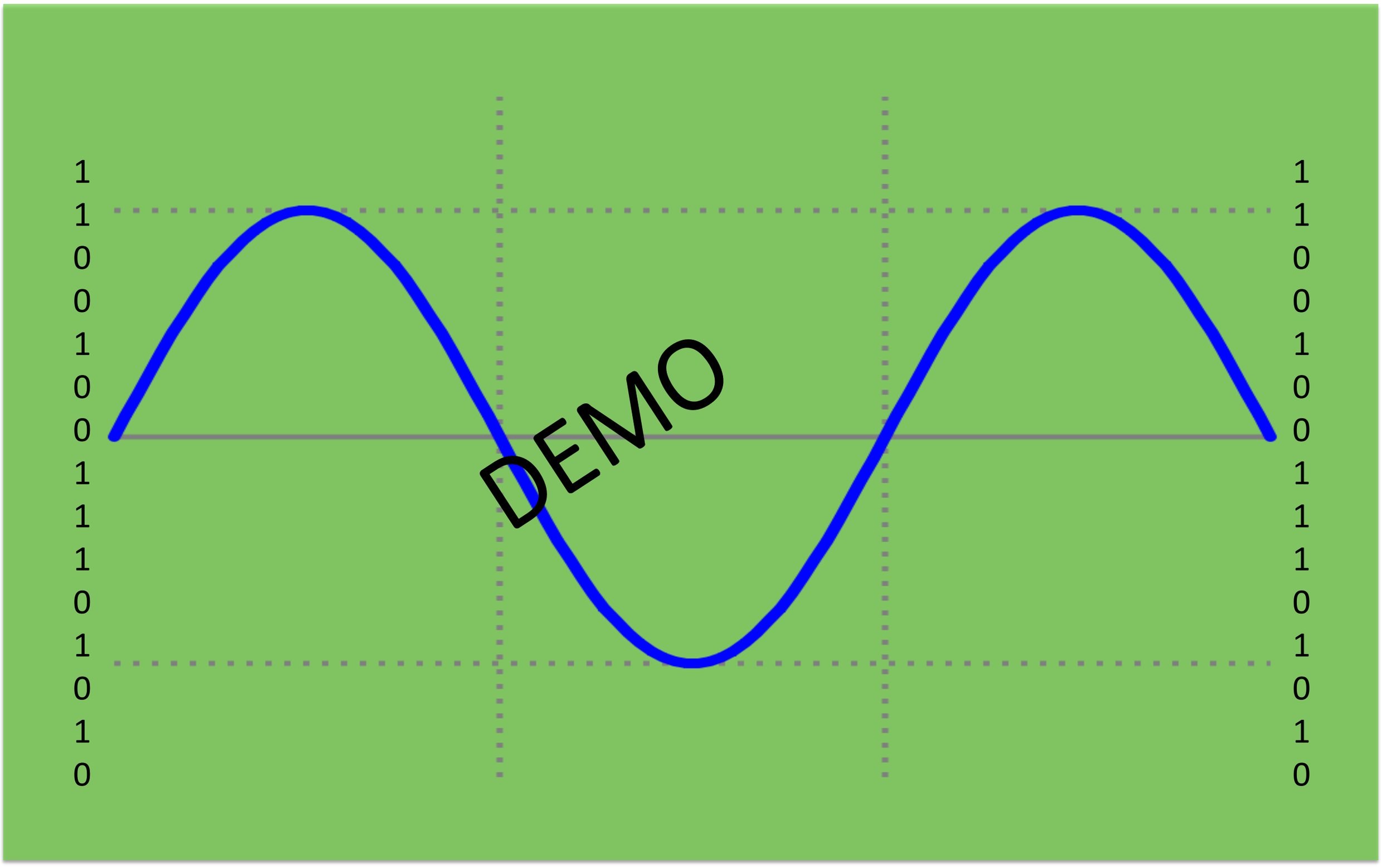
http://en.wikipedia.org/wiki/File:Fsk.svg

Identifying FSK





INTERRUPTION



DIGITAL INTERRUPTION

Section:

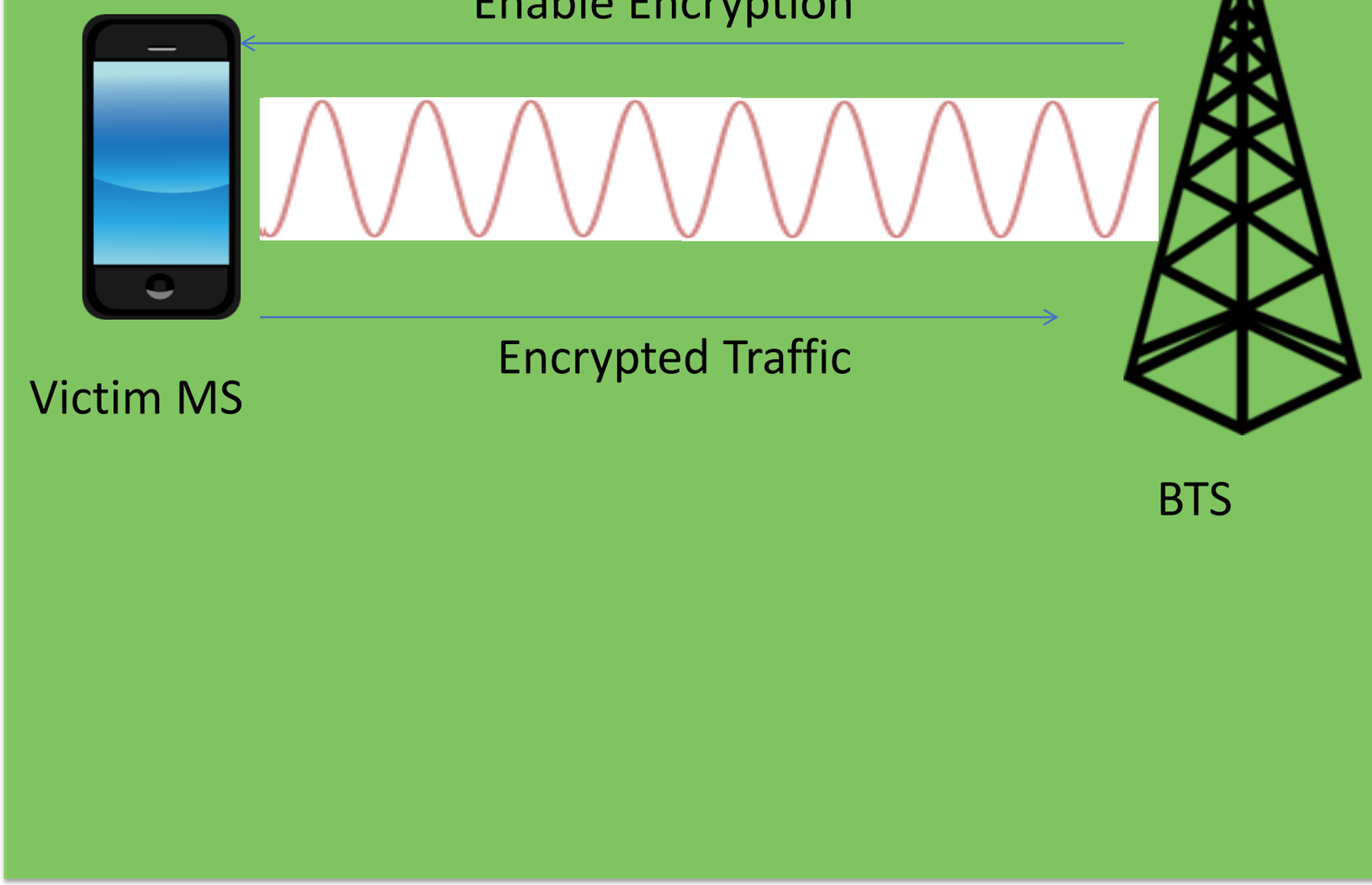
Introduction to Software Defined Radio

Attacking Radio Systems

Identifying Signals

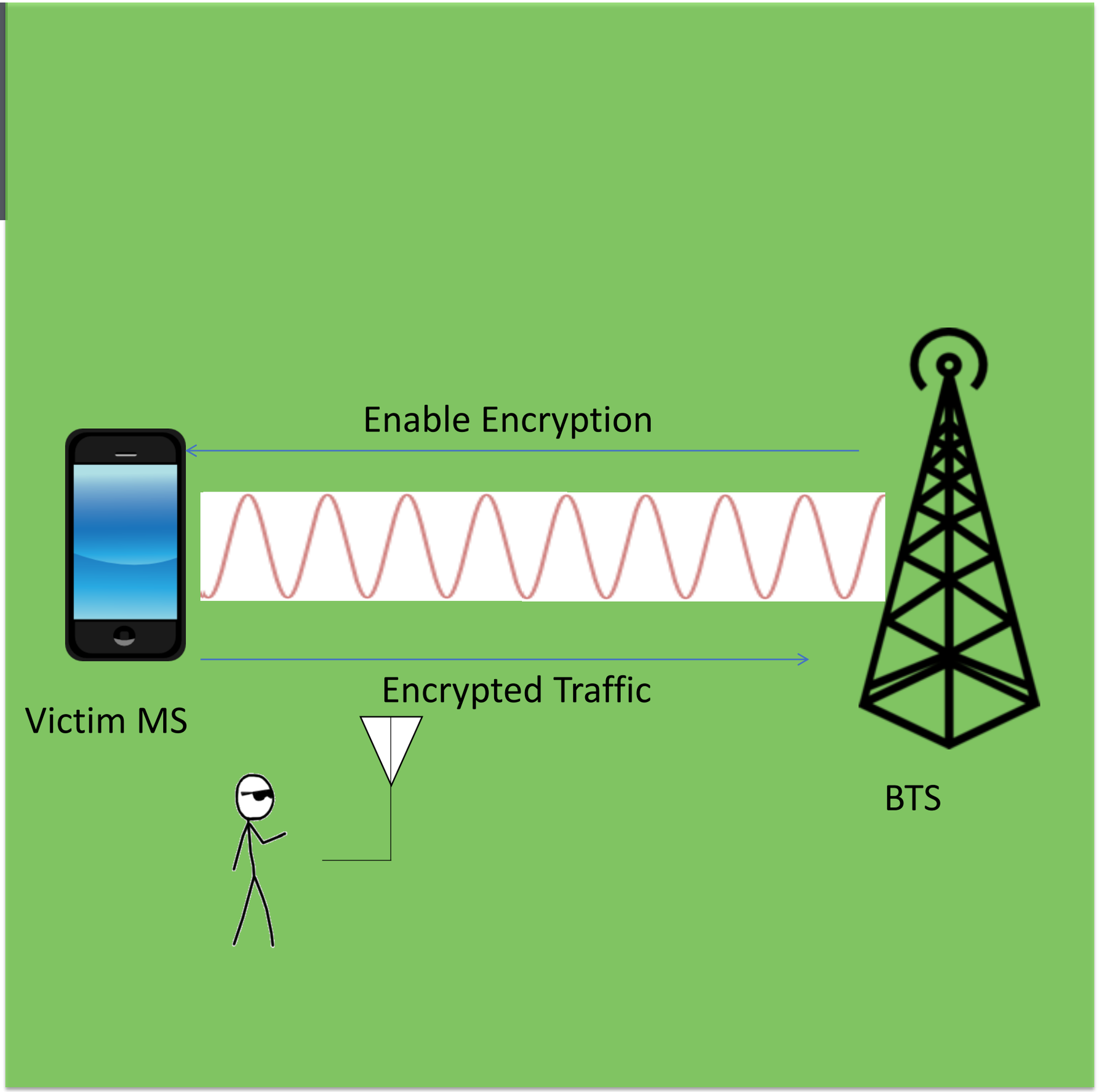
Common wireless protocols

GSM



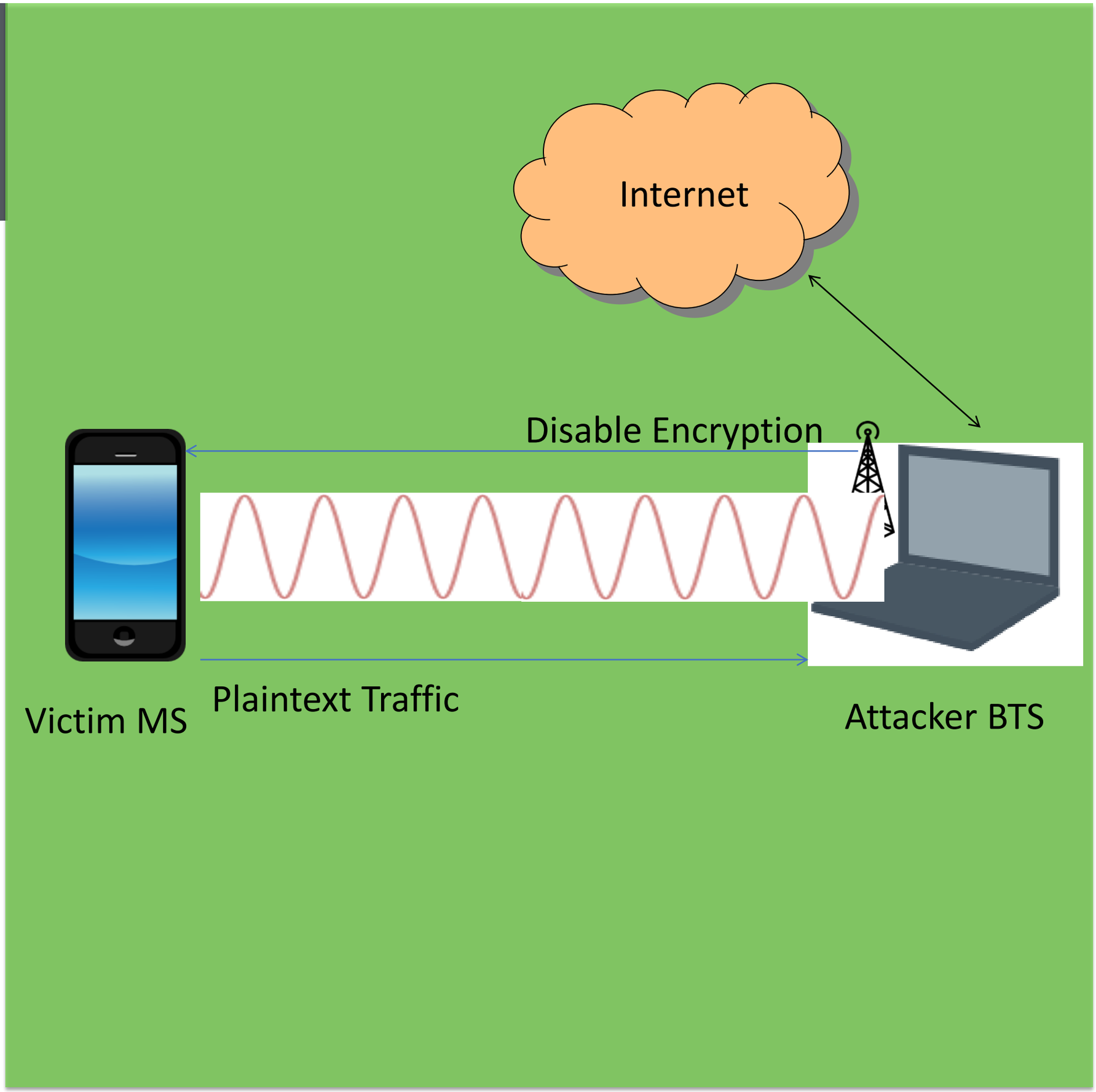
DIGITAL INTERRUPTION

GSM



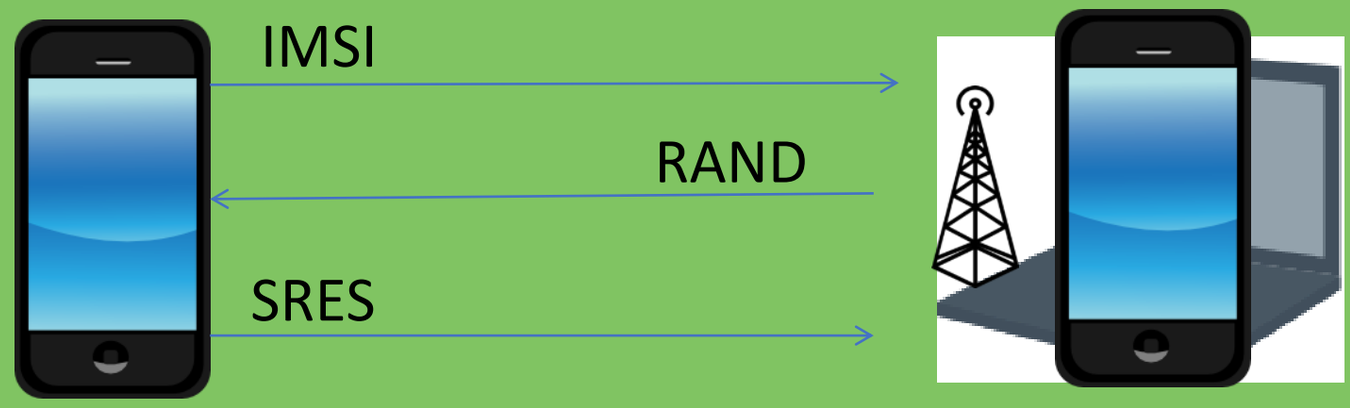
DIGITAL INTERRUPTION

GSM



DIGITAL INTERRUPTION

GSM



Victim MS

Attacker BTS

Cloned MS

DIGITAL INTERRUPTION

GSM

Attack	Vulnerable
Replay	✓
Sniffing	✓
DoS	✓
Fuzzing	✓
Crypto attacks	✓

DIGITAL INTERRUPTION

Bluetooth Low Energy

"Analysts forecast Bluetooth Smart to lead market share in wireless medical and fitness devices"
http://www.bluetooth.com/Pages/Press-Releases-Detail.aspx?ItemID=165

Bluetooth® SMART READY

DIGITAL INTERRUPTION

Bluetooth Low Energy

Just works

TK->STK->LTK

Pin

OOB

DIGITAL INTERRUPTION

Bluetooth Low Energy

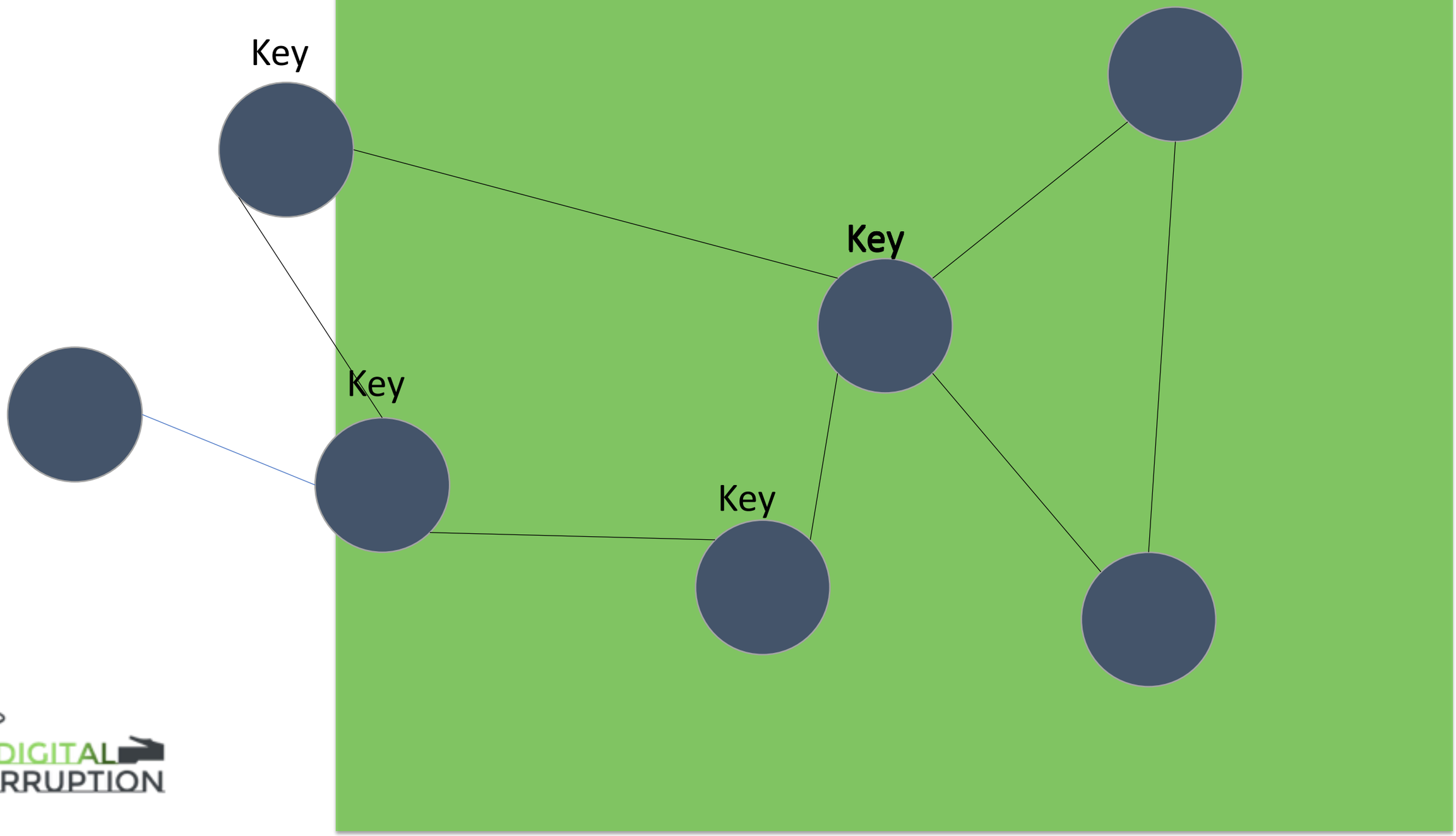
Attack	Vulnerable
Sniffing	✓
DoS	✓
Fuzzing	✓
Poor key exchange	✓

DIGITAL INTERRUPTION

ZigBee

DIGITAL INTERRUPTION

ZigBee



DIGITAL INTERRUPTION

ZigBee

Attack	Vulnerable
Replay	✓
Sniffing	✓
DoS	✓
Fuzzing	✓
Poor key exchange	✓

DIGITAL INTERRUPTION

Section:

Introduction to Software Defined Radio

Attacking Radio Systems

Reading Data from the air

Common wireless protocols


brother


Terminal - andrew@x60c: ~/CR/gqrx/build
HackRF Jawbreaker

Digital Interruption

Questions?

Jahmel Harris

JayHarris_Sec

+44 (0)161-820-3056

www.digitalinterruption.com

jahmel@digitalinterruption.com