

CONTENTS IN DETAIL

FOREWORD	xxiii
-----------------	--------------

PREFACE	xxv
----------------	------------

ACKNOWLEDGMENTS	xxvii
------------------------	--------------

INTRODUCTION	xxix
---------------------	-------------

Who Is This Book For?	xxx
Why This Book?	xxx
Hardware Considerations	xxxii
How to Use This Book	xxxiii
Online Materials	xxxiii
Conventions Used	xxxiv
How This Book Is Organized	xxxv
Wrapping Up	xxxvi

PART I THE BIG PICTURE

1 WIRELESS FUNDAMENTALS	3
------------------------------------	----------

Electromagnetic Radiation	4
What's in a Name?	5
Wi-Fi Technology Working Principle	6
IEEE 802.11 Standards	6
Broadcast Range	8
Bandwidth, Throughput, and Latency	10
Signal Strength	12
Channel Surfing	13
Channel Widths	14
Channels on the 2.4 GHz Band	15
Channels on the 5 GHz Band	16
A Word on MIMO	18
Wireless Regulatory Domains	19
Evaluating Performance	20

Wireless Adapter Hardware	23
The CYW43455 Chipset	24
The SYN43436 Chipset and Antenna	27
Wi-Fi Antennas	28
Kernel Drivers	31
Making a Connection	33
Bluetooth Wireless	36
Long Range Wireless	38
The LoRa Physical Layer	38
LoRaWAN	39
Wrapping Up	40

2 GETTING STARTED 41

Choosing Your Environment	42
Direct Access via the Terminal	42
Self-Hosted code-server	46
Remote Development	49
Prerequisites	51
Kernel and Package Updates	51
Wireless LAN Countries	52
Headless Access	53
Software Components	54
Using NetworkManager	54
Using RaspAP	56
A Brief Tour of Linux	63
Common Keystrokes	63
Overview of the Filesystem	65
Wrapping Up	66

PART II THE RECIPES

3 MONITORING WI-FI WITH A MINI TFT DISPLAY 69

Use Cases	70
Hardware Required	70
Compatible Raspberry Pi Models	70
Mini PiTFT Add-on	70
Lithium-Ion Polymer Battery	71
Software Used	72
A Closer Look at GPIO	73
Pinout Guide	73
Mini PiTFT Pinout	75

Assembling the Components	76
Attaching the PiTFT Display	76
Attaching the LiPo Battery	76
Preparing the SD Card	78
Writing to the Display	78
Prerequisites	79
Python Setup	82
Running the Signal Strength Monitor	83
Examining the Monitor Code	84
Executing on Boot	85
Running the Access Point Monitor	86
Starting the AP Monitor	86
Examining the Stats Code	87
Running at Startup	87
Monitoring the LiPo Battery	88
Going Further	88
Customizing the Signal Monitor	88
Customizing the AP Monitor	89
Wrapping Up	90

4 BASIC AND ADVANCED CAPTIVE PORTALS 91

Use Cases	91
Hardware Required	92
Software Used	93
A Closer Look at Captive Portals	93
The Splash Page Sequence	95
Security Measures	95
Creating the Access Point	96
Prerequisites	96
Installing openNDS	97
Configuring the Router	97
Checking Network Ports	98
Configuring DNS	99
Creating a Basic Captive Portal	100
Configuring openNDS	100
Starting openNDS	100
Connecting a Client	102
Customizing the Basic Portal	103
Creating a Voucher System	103
Creating a Dynamic Captive Portal	105
Setting Up openNDS	106
Implementing Forward Authentication	107
Configuring the Web Service	108
Connecting a Client Device	112
Managing Clients	113

Setting Quotas	114
Global Quota Settings	114
Individual Quota Settings	116
Traffic Shaping	117
Troubleshooting	118
Going Further	119
Wrapping Up	120

5

BLUETOOTH AUDIO IN TWO WAYS **121**

Use Cases	121
Hardware Required	122
Compatible Raspberry Pi Models	123
Bluetooth-Ready Speaker	123
Bluetooth USB Adapter	123
Digital-to-Analog Converter	123
Software Used	126
A Brief Tour of Linux Audio	126
Prerequisites	128
Installing PulseAudio with Bluetooth	128
Creating a PulseAudio Service	129
Enabling Communication with BlueZ	130
Enabling PulseAudio Bluetooth Modules	130
Connecting Bluetooth Speakers	131
Using the Bluetooth Controller	131
Pairing a Bluetooth Speaker	132
Getting Device Properties	133
Testing Audio Output	133
Streaming Internet Radio from the Console	134
Playing Music from an Audio Library	134
Playing Audio from Other Streaming Sources	135
Creating a Bluetooth Audio Receiver	137
Configuring a Bluetooth A2DP Sink	137
Using an External USB Adapter	138
Activating the Bluetooth Sink	140
Conducting a Pairing Test	140
Configuring Automatic Pairing (Optional)	141
Conducting an Audio Test	142
Integrating a DAC	143
Connecting the DAC to Hi-Fi Equipment	144
Initiating Audio Playback	144
Controlling Volume	144
Create a Spotify Connect Box with Spotifyfy	145
Setting the Scene	145
Installing Spotifyfy	146
Configuring Spotifyfy	147

Creating a systemd Service	148
Starting the Spotifyd Service	150
Controlling Playback via the Spotify App	150
Troubleshooting	151
No Audio Output from Speakers.....	151
Unable to Connect to the A2DP Sink	151
Choppy or Stuttering Audio	152
Poor-Quality or Tinny Sound Output.....	152
Going Further	152
Displaying Audio Properties	153
Integrating with a TFT Display	154
Wrapping Up	155

6 EXPLORING LONG RANGE WITH LORA 157

Use Cases	158
Hardware Required.....	158
Compatible Raspberry Pi Models	159
LoRa Expansion Boards	160
LiPo Battery HAT	162
Software Used	162
A Closer Look at the SX1262	163
Prerequisites	164
Enabling the SPI Port	164
Enabling the UART Port	165
Preparing Your Environment.....	167
Installing the Python Package.....	169
Attaching the Antenna	171
Running the LoRa Example	171
Configuring the Transmitter	171
Configuring a Receiver	173
LoRa Modulation in Detail	174
Core LoRa Parameters	176
Bandwidth	176
Spreading Factor	177
Coding Rate.....	178
A Closer Look at LoRa Packets	179
An Example Packet Definition	179
Message Size Constraints.....	180
Conducting Long-Range Tests	180
Ideal Conditions	181
A Technique for Evaluating Range	182
LoRa Parameter Tuning	183
Connecting to a LoRaWAN Gateway	185
Participating in the Network.....	186
Configuring the Pi Supply IoT pHAT	187

Installing The Things Stack CLI	190
Joining the Network	194
Troubleshooting	194
GPIO Edge Detection	195
Serial Console (Getty) Deactivation	195
LoRaWAN End Device Activity	196
Going Further	197
Using the RAK811 Examples	197
Adding IoT Sensors	197
Building Your Own LoRaWAN Gateway	198
Wrapping Up	199

7

INTRUSION DETECTION WITH KISMET **201**

Wardriving: A (Very) Brief History	202
Use Cases	204
Hardware Required	204
Compatible Raspberry Pi Models	204
External Wireless Adapter	205
Software Used	206
A Closer Look at WIDS	206
Configuring Headless Access	208
Installing Kismet	208
Using the Official Kismet Packages	209
Building from Source (Optional)	210
Configuring the Wireless Adapter	212
Monitoring Traffic	214
Kismet Startup	214
Bluetooth Sources	217
Packet Capture	217
Alerts and WIDS	218
Configuring Alerts	218
Operating the WIDS	219
Creating a WLAN Security Test Bench	219
Generating Alerts	220
Continuing Your Tests	223
Parsing Kismet's Logs	223
Using Kismetdb Statistics	223
Converting to PCAP Files	224
Going Further	225
Wrapping Up	225

8

WIRELESS AIR QUALITY MONITORING

227

Use Cases	228
Hardware Required	230
Raspberry Pi Zero 2 W	230
Male GPIO Header	231
Nova SDS011 Particle Sensor	231
Bosch BME680 Sensor (Optional)	232
3G–4G/LTE Base HAT (Optional)	232
3D-Printed Enclosure (Optional)	233
Software Used	233
Prerequisites	233
Configuring Headless Access	233
Preparing the Serial Port	234
Getting to Know the GPIO	235
Power Pins	236
UART Pins	236
Ground Pins	237
Programming Language	237
Nova SDS011 Connection	238
Gathering Sensor Data	239
Installing InfluxDB and Grafana	239
Creating a Virtual Project Environment	239
Installing pySerial	240
Obtaining Your Geohash	241
Starting the Sampler	242
Verifying Sample Data	243
Enabling the Service	244
Building the Dashboard	245
Adding a Data Source	245
Importing the Model Dashboard	246
Using the Dashboard	247
Editing the Dashboard	248
Creating Alerts	249
Testing Alerts	250
Creating an Outdoor Enclosure	251
Enter the Thingiverse	252
Assembly Tips	253
Siting Considerations	253
Battery Power	254
Publishing Your Data	254
Creating Data Feeds	254
Sending Data with Python	255
Creating an Adafruit IO Dashboard	256
Troubleshooting	257

Going Further	258
Adjusting Alert Thresholds	258
Calibrating Your Station	258
Adding Sensors	258
Wrapping Up	260

9

PWNING WI-FI WITH PWNAGOTCHI 261

Use Cases	262
Hardware Required	262
Compatible Raspberry Pi Models	263
External Battery Module	263
Assembling the Components	266
Creating a Short Stack	267
Software Used	268
TensorFlow and Keras	268
Bettercap	269
Nexmon Firmware	269
Hcxtools and Hashcat	271
Preparing the SD Card	271
Configuring Pwnagotchi	272
First Boot	273
A Brief Tour of the Interface	274
A Closer Look at Pwnagotchi's AI	275
The Actor–Critic Process Loop	276
The Reward Function	278
Using USB Ethernet Gadget Mode	279
Configuring the Device on macOS	279
Configuring the Device on Windows	280
Configuring the Device on Linux	280
Sharing Internet Connectivity	282
Connecting via SSH	283
Using MANUAL Mode	283
Using Plug-ins	285
Installing the PiSugar Plug-in	286
Saving and Restoring a Configuration	287
Performing a Full Backup and Restore	288
Using Bettercap	289
Starting an Interactive Session	289
Scripting with Caplets	289
Accessing the Web Interface	291
Collecting Handshakes	292
Creating a Target Network	294
Processing PCAP Files	295
Using Hashcat	297

Troubleshooting	299
Local Network Conflicts	299
GPIO Faults	299
Internet Connection Sharing Failure	301
Nexmon Driver Blindness	302
Going Further	302
Customizing Personality and Expressions	302
Mapping Handshakes with GPS	303
Leveling Up with Experience	304
Testing with Kismet	305
Streamlining Your Data Collection	306
Wrapping Up	307

10

EXPLORING MESH NETWORKING

309

A Brief History	310
Use Cases	311
Hardware Required	311
Compatible Raspberry Pi Models	311
Mesh-Capable Adapter	312
Squid RGB (Optional)	312
Uninterruptible Power Supply HAT	313
Software Used	313
Preparing the Nodes	315
Creating the Mesh Network	316
Working with MTU Values	319
Adding More Nodes	320
Diagnosing Mesh Network Connectivity	320
Creating Mesh Hostnames	322
Running at Boot	323
Extending the Mesh Network	324
Configure a Gateway and Allow Access	325
Adding a Gateway	326
Rebooting the Mesh Network	328
Verifying Your Mesh	329
Managing Nodes with the Gateway	331
A Closer Look at the Protocol	332
Pointers on Fine-Tuning	333
A Word on Security	334
Monitoring the Mesh Network	335
Using the Terminal	335
Using LED Activity Indicators	336
Troubleshooting	339
Going Further	340
Wrapping Up	341

Use Cases	344
Hardware Required	344
Compatible Raspberry Pi Models	344
HDMI Cable	345
VESA-Compatible Project Case (Optional)	346
Software Used	346
Windows and Android Support	346
Apple Device Support	347
Casting Call	347
AirPlay	347
Miracast	348
Chromecast	349
Casting Devices Compared	349
A Closer Look at Wi-Fi Direct	350
Operating Principle	350
Adapter Support	352
Interface Combinations	352
Installing Lazycast	353
Disabling the Onscreen Prompt	354
Installing the Dependencies	354
Updating the Driver	355
Building the Lazycast Binaries	356
Starting Lazycast	357
Connecting a Source	357
Peeking Under the Hood	359
A Brief Detour into VideoCore	361
Installing RPiPlay	362
Installing the Prerequisites	363
Building the RPiPlay Binaries	364
Starting RPiPlay	365
Connecting the Source	366
Looking Under the Hood	367
Troubleshooting	369
Code Compilation Errors	369
Linux Networking	370
Expected Performance Levels	370
Going Further	372
Smart TV Spying	372
An Alternative to Surveillance	373
Wrapping Up	374

APPENDIX: THE ENGINEER’S MINDSET	375
Of Astrophysics and Coffee	375
Developing an Engineer’s Mindset	377
Three Key Traits of an Engineer	377
Two Kinds of Constraints	377
Systems-Level Thinking	378
A Problem-Solving Methodology	379
Defining the Problem	380
Making Observations	380
Forming a Hypothesis	383
Narrowing Focus	383
Applying a Fix	384
Iterating as Required	384
Putting It into Practice	385
Top Tips and Strategies	387
Querying System Logs	388
Tracing Socket Conflicts	391
Final Thoughts	393
 INDEX	 395