Spectrum Technology

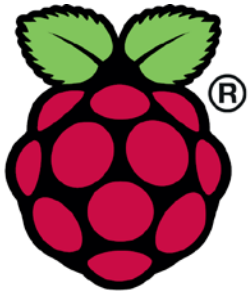
V1.0 2023/3/22

抜粋版

WiFiプロトコル・アナライザ V2

～Raspberry Piを使いwifi6e対応～

運用編



スペクトラム・テクノロジー株式会社

https://spectrum-tech.co.jp

sales1@spectrum-tech.co.jp

ST Spectrum Technology

目次

抜粋版のためページと本文は一致しません

プロトコル・アナライザ運用マニュアル

1. Raspberry Piでできること
   - WiFi, LAN, BLE（一部）のwiresharkを使ったプロトコル・アナライザ
   - Wifiのスキャン：airodumpのみ解説します
   - Ibeacon（BLE)のビーコン送信、受信
   - 他にweb,メール、センサ制御など無限大の利用価値がありますが説明は割愛します。
2. Linux基本的なコマンド

   ① システム関係
   - 起動：電源を入れると自動で起動します。
   - 再起動：# reboot

     又は、menu>shutdown>reboot；左上のメニューから
   - 終了： # shutdown

     又は、menu>shutdown>shutdown；左上のメニューから
   - ログアウト # exit

     又は、menu>shutdown>logout；左上のメニューから
   - 日本語／英語の入力切替：半角/全角のキー、切り替わらない場合は、上のiconのキーボードでmozc選択

プロトコル・アナライザ運用マニュアル

2. Linux基本的なコマンド

② ディレクトリ操作、コピー、移動、削除

masa@raspberrypi:~$cd /home/pi/Documents　　ディレクトリの切り替え

masa@raspberrypi:/home/pi/Documents# ls ファイルとディレクトリの表示（表示したら操作したいファイルを右クリックでコピペして操作します

masa@raspberrypi:~$ cp ファイル名　ディレクトリ　　配下のディレクトリのファイルを別のディレクトリへコピー

masa@raspberrypi:~$ mv ファイル名　ディレクトリ　　配下のディレクトリのファイルを別のディレクトリへ移動

masa@raspberrypi:~$ rm ファイル名　　ファイルの削除

便利な機能　　rm --help　　コマンドのオプションが分からない場合は、ヘルプで問い合わせる。すべてのコマンド共通(マイナスを2個とhelp)

③ ユーザ権限、プロセス他

pi@raspberrypi:~ $ su -　　スーパーユーザ（root)に切り替え、パスワードを入力

masa@raspberrypi:~$ ps　a　　現状の動いているプロセスを表示

masa@raspberrypi:~$ kill　　特定のプロセスを強制終了

masa@raspberrypi:~$ apt-get install pkg　　パッケージのインストールなどに使用

masa@raspberrypi:~$ date　　日付、時間の設定を行います。

masa@raspberrypi:~$ mousepad /etc/network/interfaces　　インタフェースに記述してい内容を変更します。Viよりも使いやすいです。

④ モジュール、usb、メモリ、HDDなどの表示

masa@raspberrypi:~$ lsmod　　linuxのモジュールリスト表示

masa@raspberrypi:~$ lsusb　　usbのデバイス表示

masa@raspberrypi:~$ free –mt　　メモリ使用状態表示

masa@raspberrypi:~$ df　　HDD（マイクロSD）の使用状態表示

プロトコル・アナライザ運用マニュアル

パーミッションエラーが出た場合は、sudoをつけて

3. プロトコル・アナライザ関係コマンド

① ネットワーク関係（wifi,LAN)

masa@raspberrypi:~$ifconfig	ネットワークインターフェースの状態表示
masa@raspberrypi:~$ ip l set wlan1 up	wlan1のインタフェースのup(LANの場合はeth0)
masa@raspberrypi:~$ ip l set wlan1 down	wlan1のインタフェースのdown
masa@raspberrypi:~$ iwconfig wlan1 mode monitor	wlan1のインタフェースをmonitoモードに切り替えます。
masa@raspberrypi:~$ iwconfig wlan1 channel 11	wlan1のチャンネルを11(2462MHz)に切り替えます。
masa@raspberrypi:~$ sudo wireshark	wiresharkを起動します。必ずsudoをつけること。Rootに切替て実施するとではエラー

masa@raspberrypi:~$ airodump-ng –band abg wlan1　wlan1のインタフェースで2.4G,5Gの全チャンネルのデータを取得できます。Wiresharkの個別チャンネルに比べて、データが欠落します。確認程度でお使いください。

masa@raspberrypi:~$ tshark –i wlan1 –w test0707.pcap　wiresharkを起動する代わりにコマンドでデータを取得し保存します。

② BLE関係

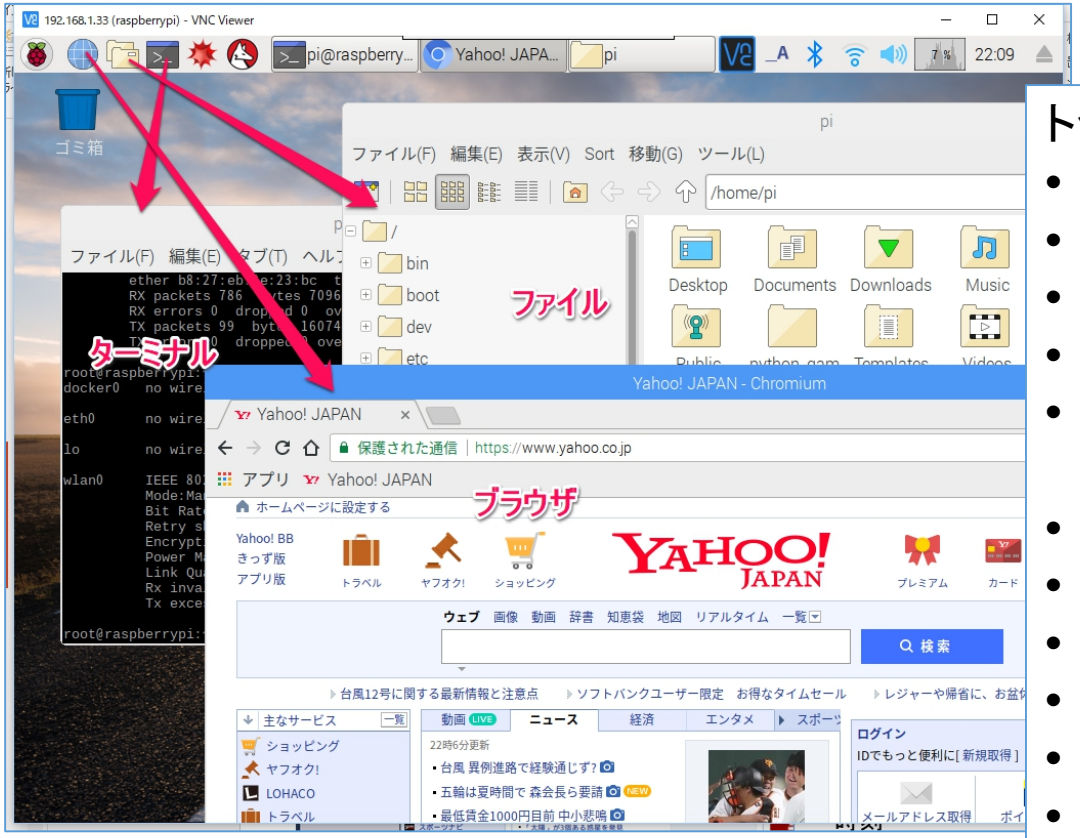
masa@raspberrypi:~$ hciconfig	BLEのインタフェース状態を表示
masa@raspberrypi:~$ hciconfig hci0 up	hci0のインタフェースをup
masa@raspberrypi:~$ hcitool lescan	BLEのデバイスを検索します。wiresharkを立ち上げてBLEのインタフェースを選択しておくとプロトコルが取得できます。RF帯ではありません。限られたプロトコルになります。
masa@raspberrypi:~$ hcidump –a	BLEの接続状態をダンプします。

Spectrum Technology

プロトコル・アナライザ運用マニュアル

4. Raspberry Piの基本操作

① 表示画面と内容



トップ画面（上段のタスクバーで選択）

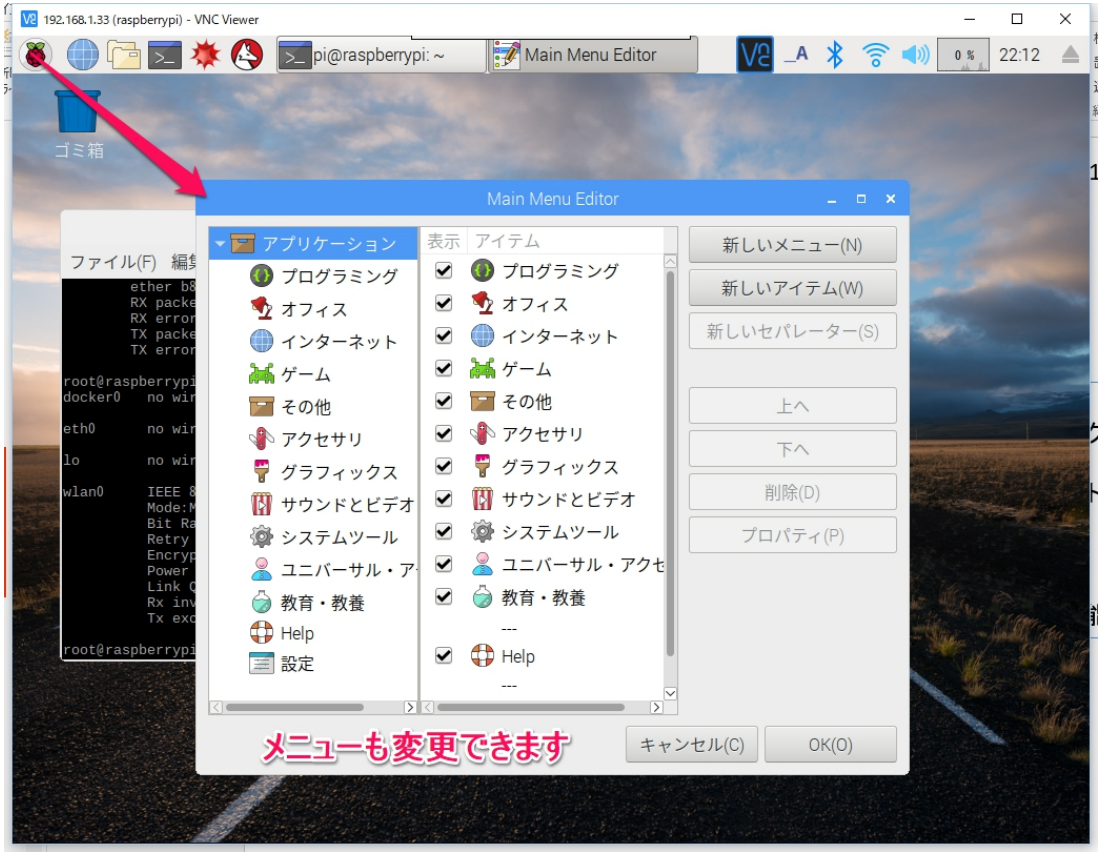
- メニュー
- ブラウザ
- ファイルマネジャ
- ターミナル
- マルチ画面選択

- VNC
- 日本語入力
- BLE
- WiFi
- 音量（ジャックで聴けます）
- 回線効率
- 時刻

プロトコル・アナライザ運用マニュアル

4. Raspberry Piの基本操作

② メニュー内容



メニュー内容
- プログラミング
- オフィス
- インターネット

カスタマイズ可能です。

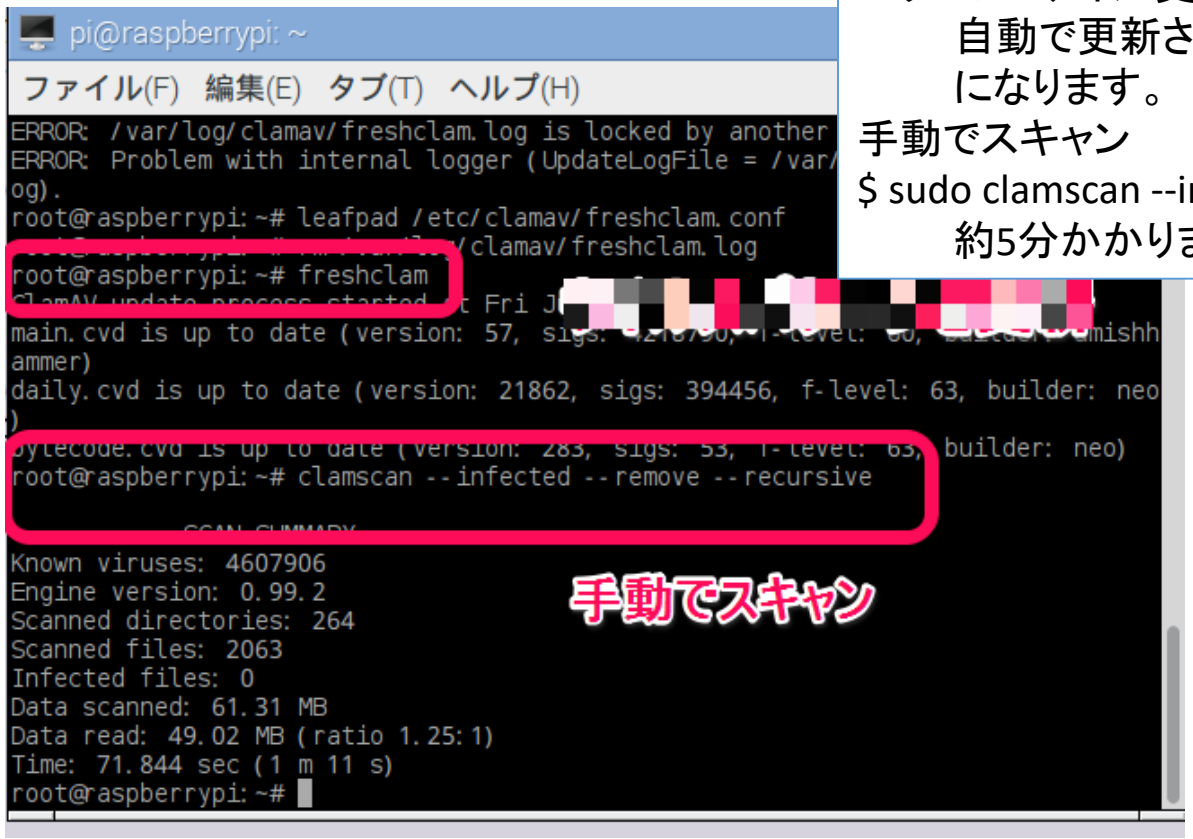
プロトコル・アナライザ運用マニュアル

5. 日常運用

① セキュリティ対策（アンチウイルス更新、スキャン）

- アンチウイルス対策として無料のclamAVをインストールしてます。
- 手動での運用を基本としてます。

パターンファイル更新
　　自動で更新されます。# freshclamはエラーになります。
手動でスキャン
$ sudo clamscan --infected --remove --recursive
　　約5分かかります。

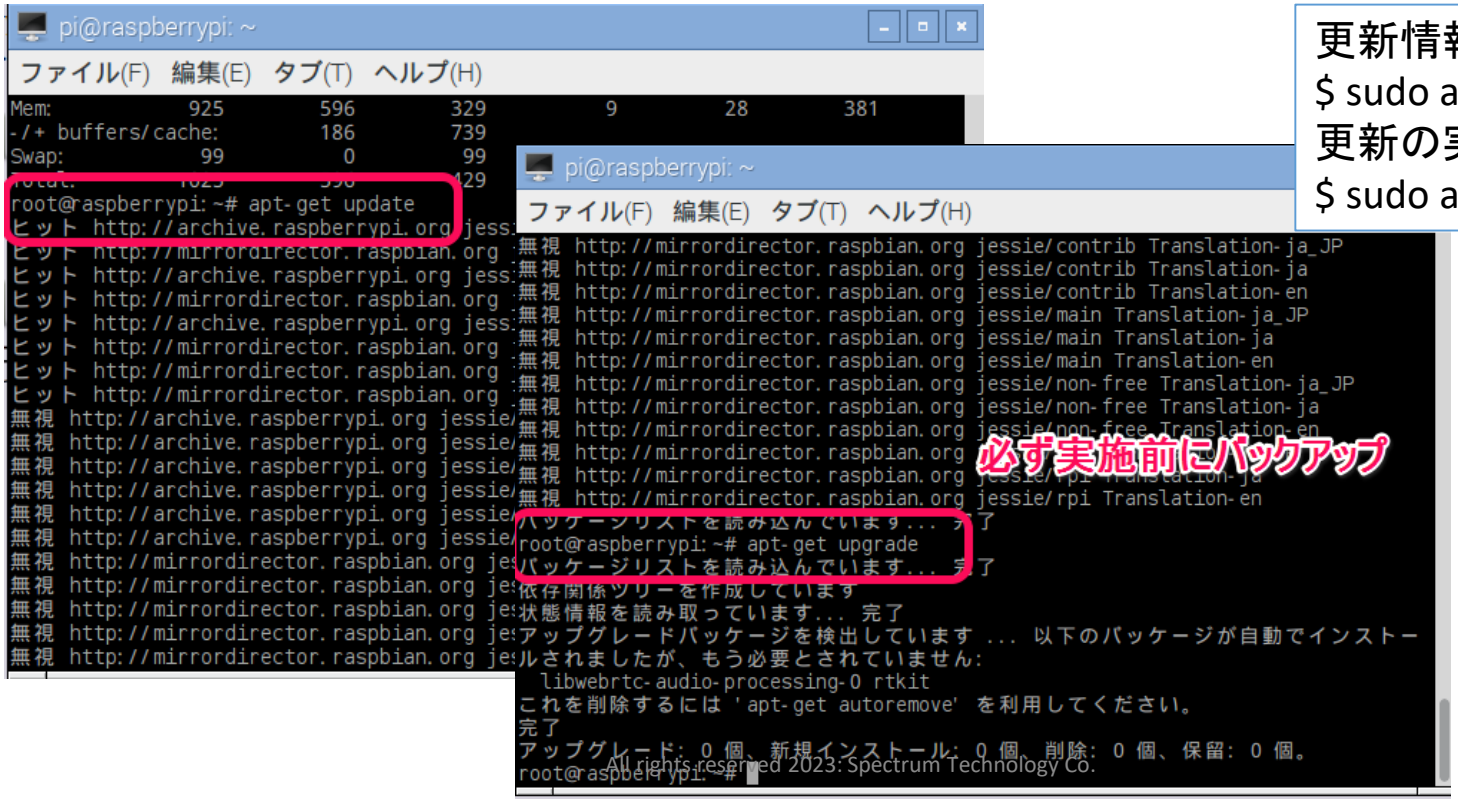


プロトコル・アナライザ運用マニュアル

5. 日常運用

② インストール済パッケージの更新情報収集、アップグレード

- Linuxの場合は、頻繁に更新が発生します。アップデートとアップグレードを定期的に実施してください。
- 更新前には、バックアップを取ることをお勧めします。特にアップグレードはまれに動作不良、戻せない状態が発生します。

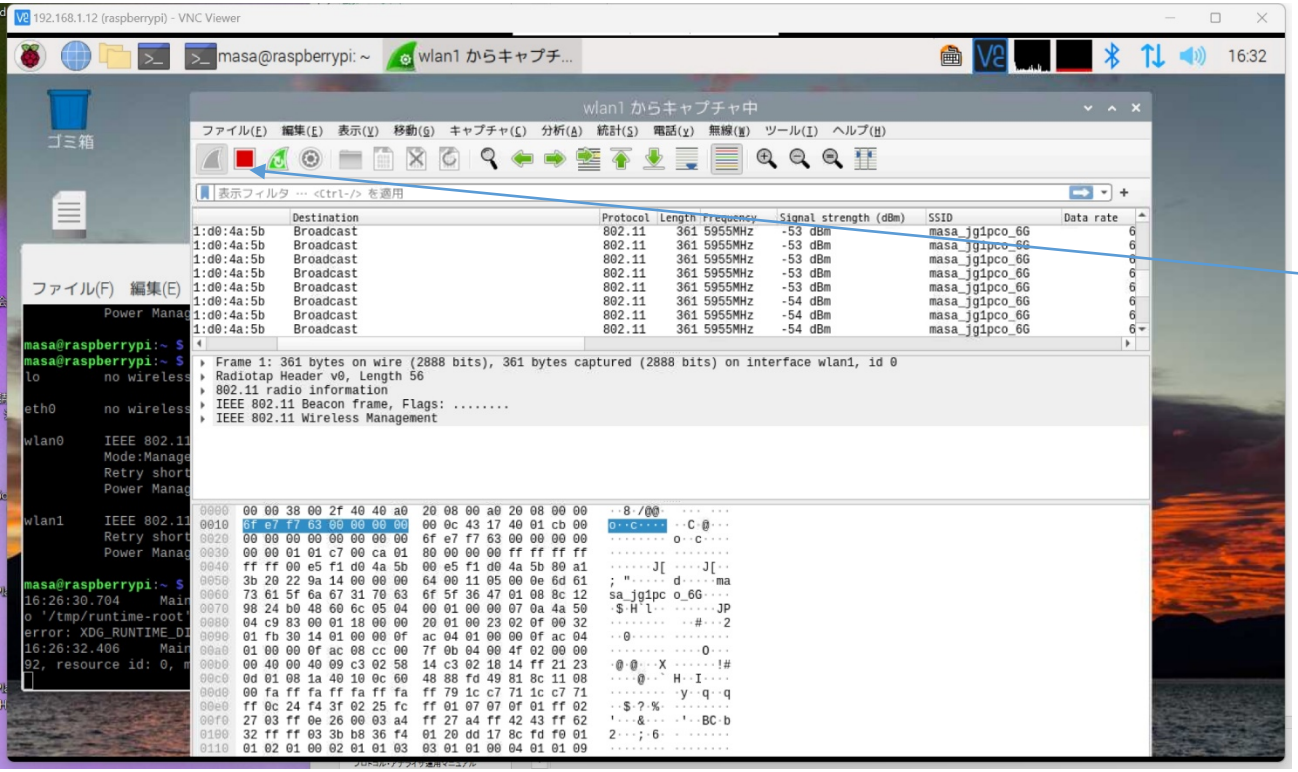


更新情報収集
$ sudo apt-get update
更新の実施
$ sudo apt-get upgrade

プロトコル・アナライザ運用マニュアル

6. Wifiプロトコル・データの取得

① WiFi6e 6GHzチャンネル モニタ Wiresharkによるパケット取得



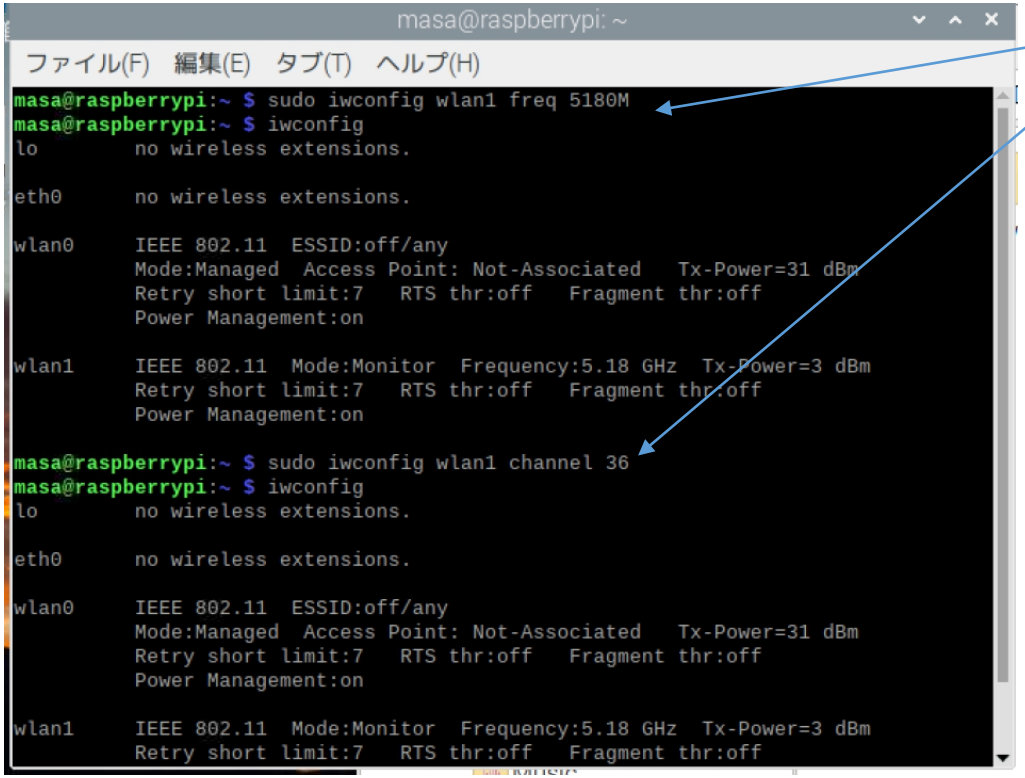
$ sudo wireshark
wireshark起動
オプション＞wlan1選択し、開始
取得終了したら、赤ボタンで停止
ファイル＞として保存。以下のフォルダ
/home/masa/Documents/wifi
ファイルをsamba経由で取り出す場合は、権限を変更のこと。wifiフォルダ全部変更の場合
$ sudo chmod a=rwx -R wifi

プロトコル・アナライザ運用マニュアル

6. Wifiプロトコル・データの取得

② 2.4G/5GHzチャンネル モニタ 20MHz wlan1のモニタチャンネル設定

- 現在、netgearは、160MHzは未対応。
- 40MHz, 80MHzの設定はこちらへ



$ sudo iwconfig wlan1 freq 5180M
又は
$ sudo iwconfig wlan1 channel 36
$ iwconfig
設定チャンネルを確認

別紙の2.4GHz, 5GHzチャンネル配置を参照

プロトコル・アナライザ運用マニュアル

6. Wifiプロトコル・データの取得

⑤ airodumpを使ってスキャン 2.4G/5G

airodumpで全チャンネルスキャンします。
周辺のアクセスポイントの状況確認に使用
2.4G/5G(ch140まで)の場合
$ sudo airodump-ng --band abg wlan1

スキャンを停止する場合はCTLとcを同時に押してください。
6GHzの全チャンネルの場合
$ sudo airodump-ng -C 5955-6415 wlan1

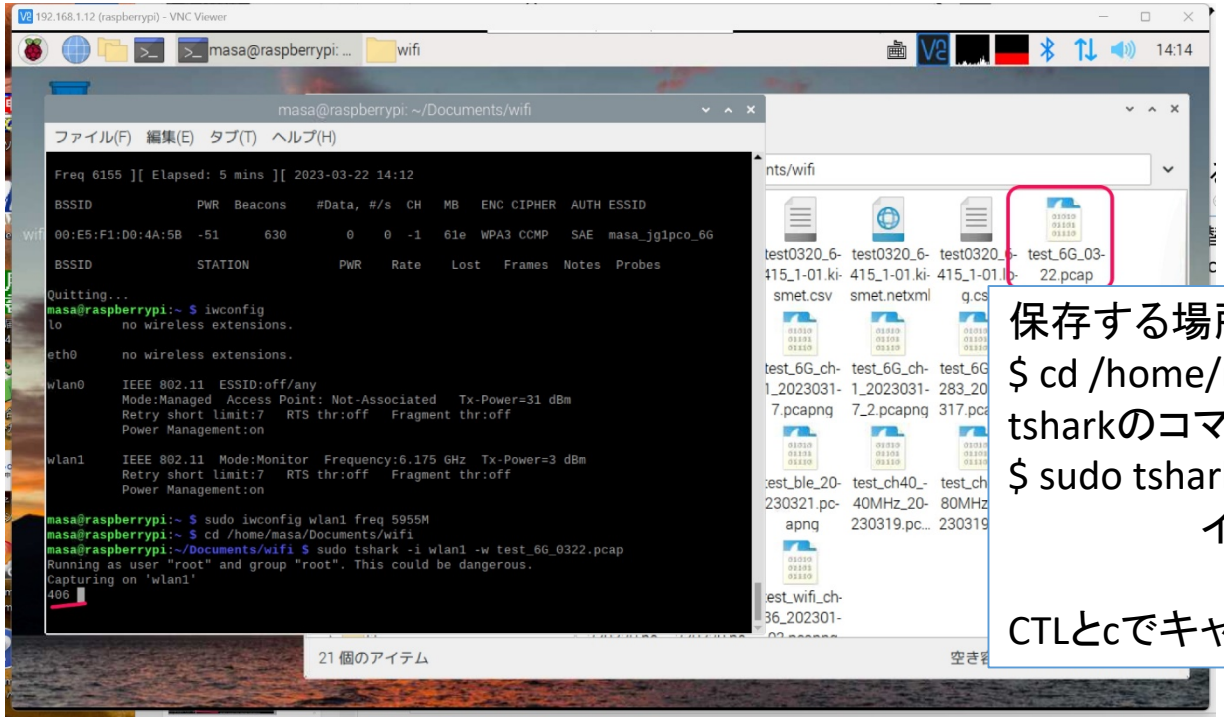
- 個別に複数のチャンネルを指定するこもできます。
- 使用チャンネル、暗号化方式などがわかります。
- Macアドレスなどが含まれてますので、個人情報保護法に基づいて使用してください。

プロトコル・アナライザ運用マニュアル

6. Wifiプロトコル・データの取得

⑦ tsharkによるデータ取得

wiresharkのGUIの場合途中止まるとデータがなくなるおそれがあるので、ファイルに都度書き込むtsharkを使います。



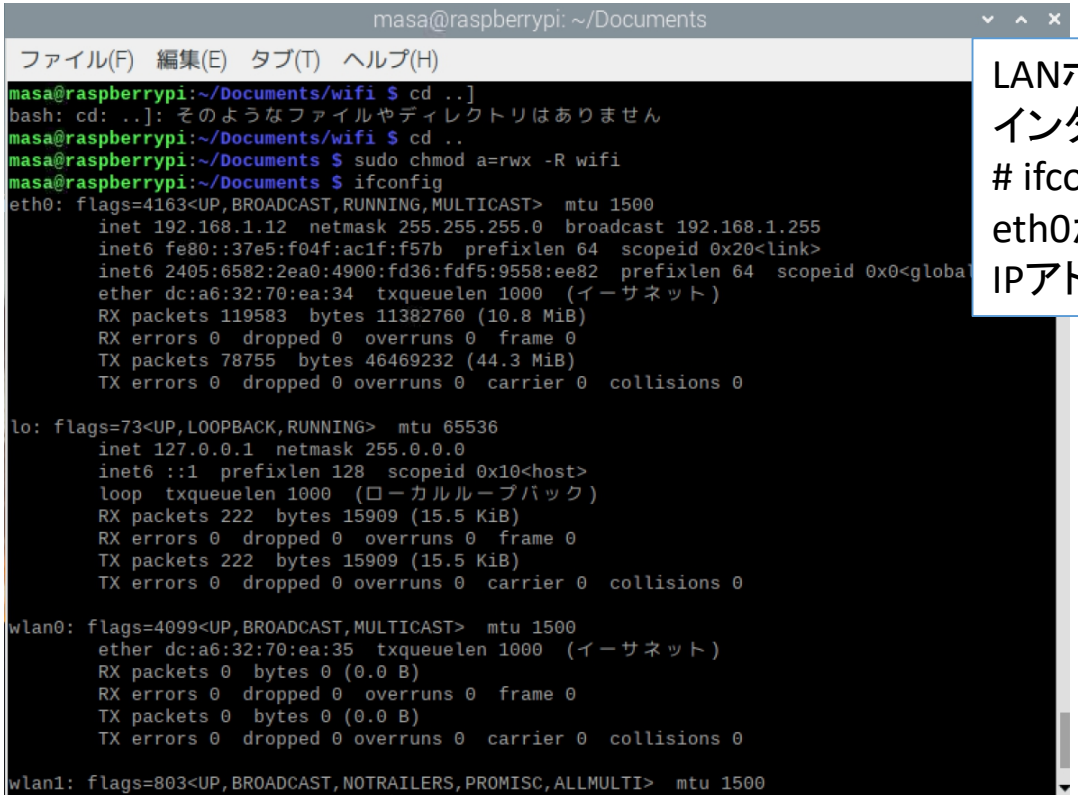
保存する場所に切り替えます。
$ cd /home/masa/Documents/wifi
tsharkのコマンド
$ sudo tshark -i wlan1 -w test_6G_0322.pcap
インタフェース ファイル名

CTLとcでキャプチャを停止します。

プロトコル・アナライザ運用マニュアル

7. LANプロトコル・データの取得

① LAN上のプロトコル・データの取得してみます。Wifiと同じです。

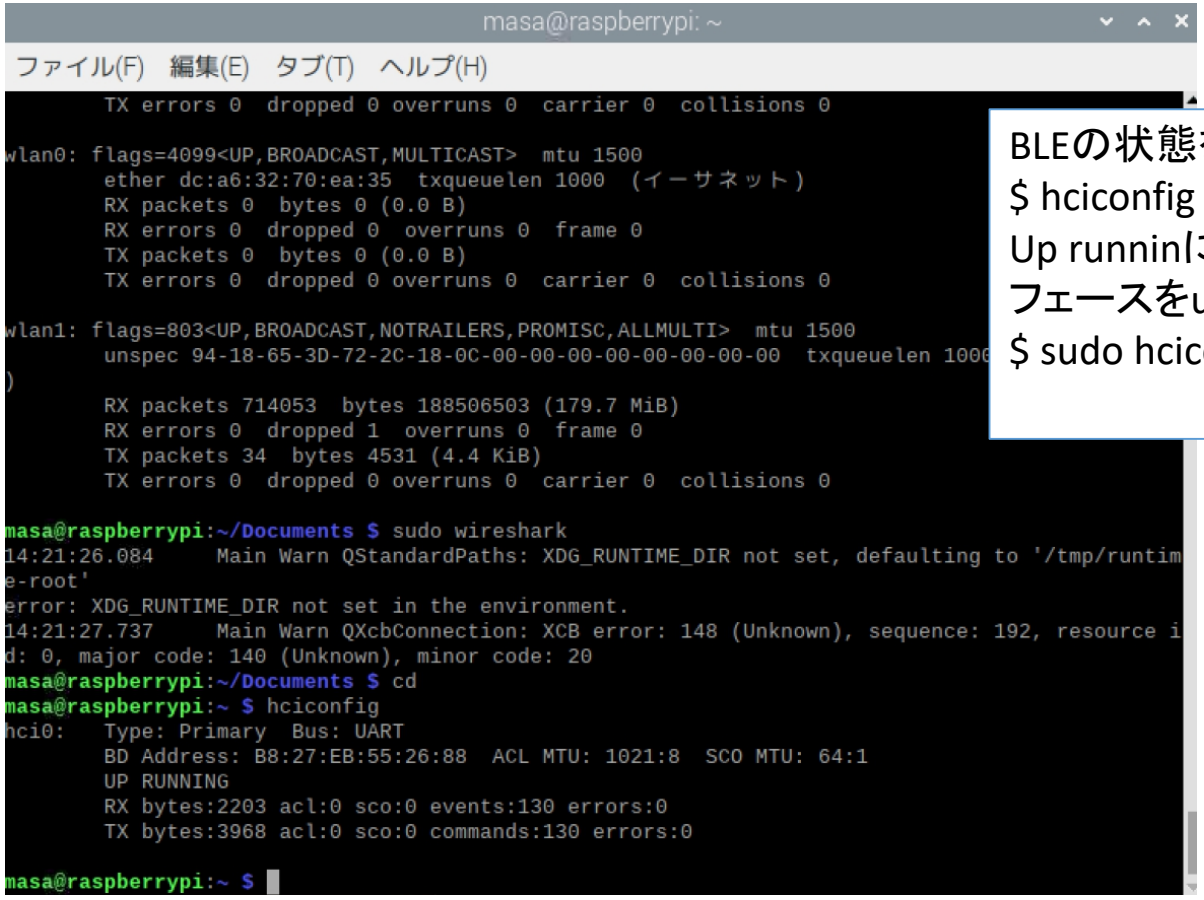


LANポートにケーブルを接続します。
インタフェースの状態を確認します。
ifconfig
eth0がインターフェース名になります。
IPアドレスが確認できます。

プロトコル・アナライザ運用マニュアル

8. BLEのプロトコル・データの取得

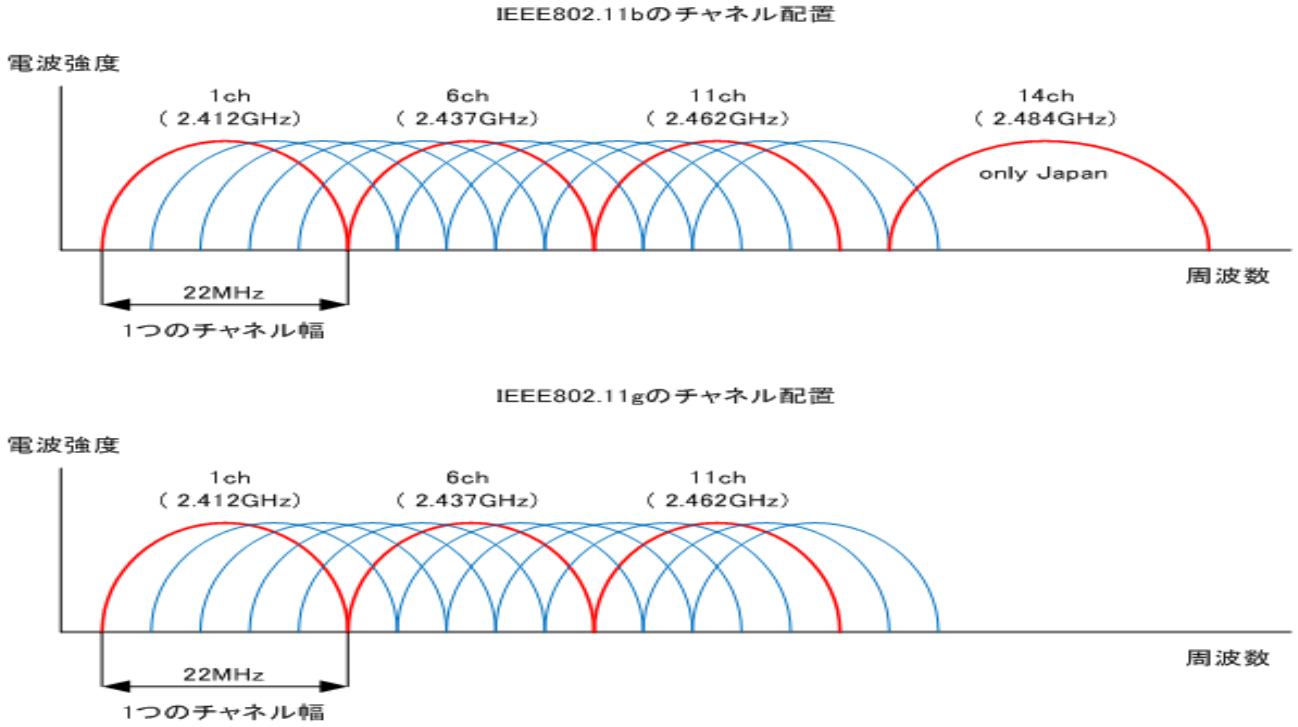
① hci0のプロトコル・データの取得



BLEの状態を表示します。
$ hciconfig
Up runninになっていない場合は、インタフェースをupします。
$ sudo hciconfig hci0 up

参考

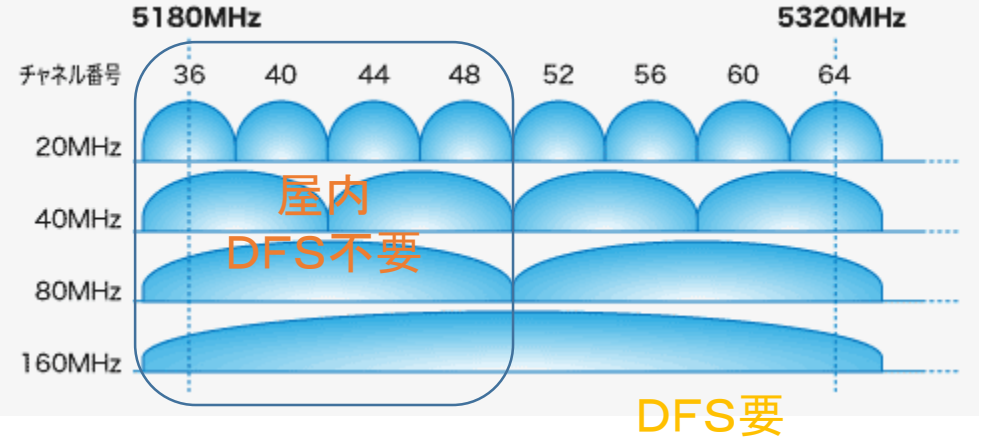
2.4GHzチャンネル配置



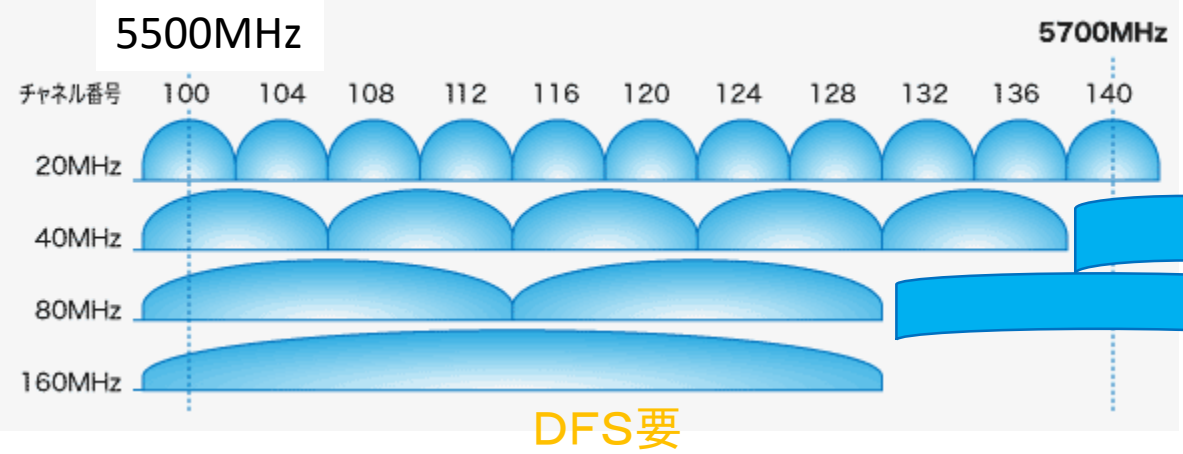
屋内外

- 周波数帯：2．4GHz－2．5GHzの100MHz
- チャネル番号は、CH1－CH14。通常使っているのは3波（CH1，CH6，CH11）

5GHzチャンネル配置



屋内（固定衛星up、無線標定(気象レーダ)、地球探査衛星に割当しているため）



周波数帯：5.15GHz-5.35GHz, 5.47GHz-5.73GHzの460MHz
CH番号：CH36-CH64までの8ch, CH100-CH144までの12CH

Spectrum Technology

Wifi6e 6GHzチャンネル配置

ch	freq(MHz) 20M	40M	80M	160M
1	5955			
3		5965		
5	5975			
7			5985	
9	5995			
11		6005		
13	6015			
15				6025
17	6035			
19		6045		
21	6055			
23			6065	
25	6075			
27		6085		
29	6095			
31				
33	6115			
35		6125		
37	6135			
39			6145	
41	6155			
43		6165		
45	6175			
47				6185
49	6195			
51		6205		
53	6215			

ch	freq(MHz) 20M	40M	80M	160M
55			6225	
57	6235			
59		6245		
61	6255			
63				
65	6275			
67		6285		
69	6295			
71			6305	
73	6315			
75		6325		
77	6335			
79				6345
81	6355			
83		6365		
85	6375			
87			6385	
89	6395			
91		6405		
93	6415			

6GHzのチャンネル

- 20MHz帯域：24ch
- 40MHz帯域：12ch
- 80MHz帯域：6ch
- 160MHz帯域：3ch

表が各チャンネルと中心周波数