

無線LANルーターを作って パケットをみてみよう

～スマートホンのアプリが送受信してる
パケットはどこからきてどこへいくのか～



2023年9月

NTTコミュニケーションズ株式会社

イノベーションセンター 担当部長

シニア・テクノロジー・アーキテクト / エバンジェリスト

博士(工学) 宮川 晋

shin.miyakawa@ntt.com

自己紹介



宮川 晋 (みやかわ しん)

NTTコミュニケーションズ株式会社

イノベーションセンター (本務) / 第二ビジネスソリューション部 (兼務)

担当部長

シニア・テクノロジー・アーキテクト / エバンジェリスト

来歴と主な所属

平成7年 東京工業大学 博士 (工学) 学位取得 同年にNTT入社

NTTソフトウェア研究所、NTT MCL (シリコンバレー)、NTTコミュニケーションズ 技術開発部

慶應義塾大学SFC研究所上席研究員(客員)

主な研究関係の業績

IETF RFC6888, 3769, 4241, 4925

IPv6、Carrier Grade NATなど

BSDを256倍つかうための本 (アスキー出版局)

はやわかりPCUNIX (共立出版)

西麻布のバーでNTT Comの宮川エバに聞いたテッキーなお話

<https://ascii.jp/elem/000/000/988/988432/>

Google IPv6 Conference 2008

- <https://www.youtube.com/watch?v=mZo69JQoLb8>
- Google IPv6 Conference 2008: What will the IPv6 Internet look like?



<https://ja.wikipedia.org/wiki/%E3%83%B3%E3%83%84%E3%83%97>

ヴィントン・グレイ・サーフ（**Vinton Gray Cerf**^[1], [1943年6月23日](#) - ）は**アメリカ合衆国**の**計算機科学者**であり、**ロバート・カーン**と共に^{[4][5]}**インターネット**と**TCP/IPプロトコル**の創生に重要な役割を演じた「**インターネットの父**」の1人^{[6][7]}。その功績により、**アメリカ国家技術賞**^[1]、**チューリング賞**^[8]、**大統領自由勲章**^[9]を受賞（受章）し、**全米技術アカデミー**会員にも選ばれている。通称は**ヴィント・サーフ**（**Vint Cerf**）。

Mobile World Congress 2018

- McLaren's Keynote at MWC 2018 with Dr. Shin Miyakawa from NTT Communications on 27th Feb 2018 at Barcelona Spain
- <https://www.mobileworldlive.com/on-stage/mwc/keynote-mclaren-formula-1-driver-fernando-alonso-and-zak-brown/>



<https://ja.wikipedia.org/wiki/フェルナンド・アロンソ>

フェルナンド・アロンソ・ディアス (Fernando Alonso Díaz, [1981年7月29日](#) -) は、[スペイン・アストurias州オビエド](#)出身の[レーシングドライバー](#)である。[2005年](#)に、当時のF1史上最年少[ドライバーズチャンピオン](#)記録を樹立し、翌[2006年](#)には連覇を達成した。また2018年にはF1と並行して[ル・マン24時間](#)にも参戦し、総合優勝を収めた。2019年に[ル・マン24時間](#)を連覇し、2018/2019シーズンの[FIA世界耐久選手権LMPドライバーチャンピオン](#)を獲得した。

おまけ

- <https://www.as-web.jp/overseas/486286>
- **ラップダウンから優勝争いへ。30万人を沸かせた琢磨10度目のインディ500「今日は喜んでもいい3位」**
 - 2019年 5月 INDY 500 佐藤琢磨選手 三位
 - 佐藤琢磨選手の左奥のほう。。



ウォーリーを探せ状態

- 「優勝に値する4位」苦しみ抜いた大嶋和也が[https://www.as-web.jp/super-formula/956801SF第5戦SUGOで結果を残す。チームスタッフに涙 | スーパーフォーミュラ | autosport web \(as-web.jp\)](https://www.as-web.jp/super-formula/956801SF第5戦SUGOで結果を残す。チームスタッフに涙 | スーパーフォーミュラ | autosport web (as-web.jp))
- <https://www.as-web.jp/super-formula/956801>

豊田章男
トヨタ自動車会長



私

**スマートホンのアプリが通信してる
パケットをみたくない？**

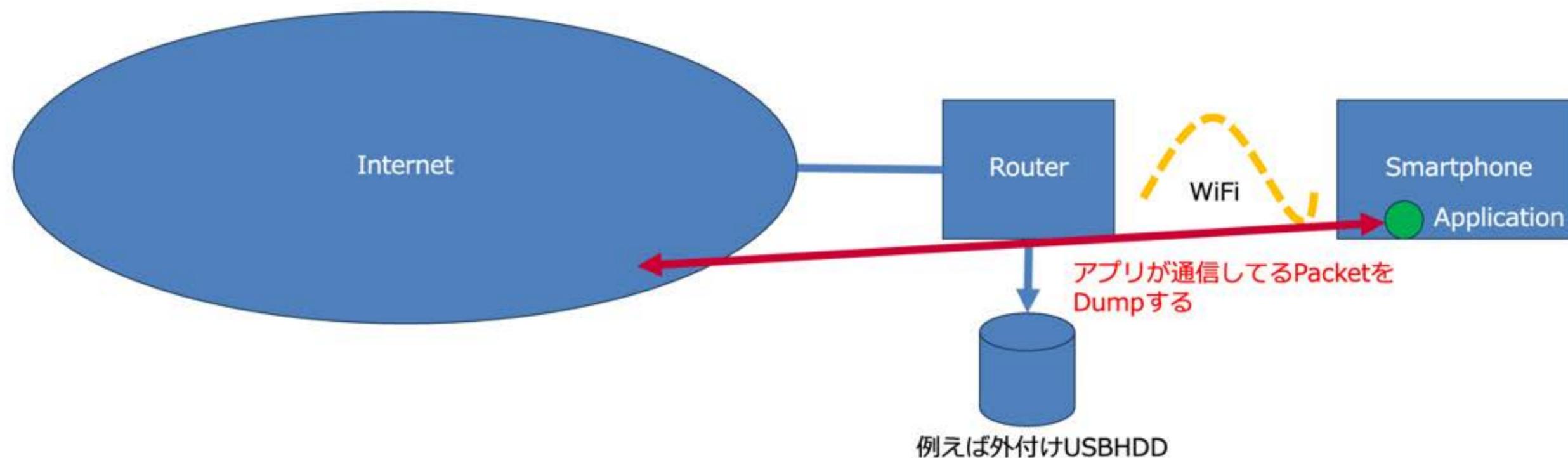
ある種のアプリアルーターは「危険」といわれてる

- [結局、TikTokは安全なのか？ それとも危険なのか？【ニューヨーク大学教授が解説】\(esquire.com\)](#)
- [TP-LINKはやばい？中国製Wi-Fiルーターがトラフィックを送信 | invisibletechnology](#)
- 本当なのかしら?? ま、そうなのかもねええ。。っておもってるのはいいんですが。
- やっぱり自分で、実際にどうなってるのか調べてみたい
- まあ、パケット自体が暗号化されていたら「中身」をみるのは至難のわざだけど
- せめて、パケットが「どこへむかっているのか」「どこからきてるのか」は、みてみたいなあとおもいませんか？

ルーターでパケットをダンプしたいよね

上流につながるルーターでパケットを捕まえればいい

- 調べたいアプリが動いているスマートフォンや機材を、インターネットにつなげるための「ルーター」で、流れているパケットをファイルにコピーしたい
- ま、Ciscoとかでもできるっちゃできるんだけど、
- あまりその辺には転がってないし、とりまわしもあれなんで。自分で作っちゃえ



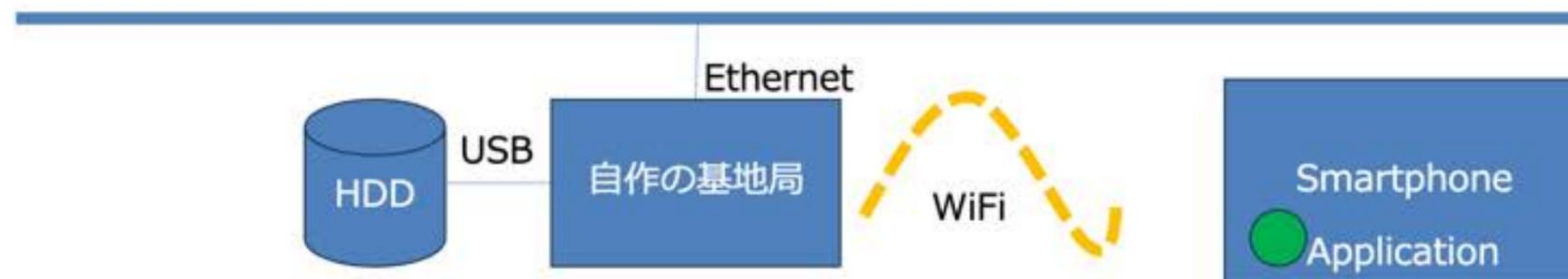
「WiFiルーター」を作ろう（超初級者編）

WiFiの基地局をつくってスマホをその下につなげるには

いまそこにあるインターネットをWiFi基地局ルーターで延長することを考える

1. WiFi基地局を作る
2. そのWiFi基地局の「下」にWiFiでスマホを接続する
3. 調査したいアプリをスマホにいれる
4. 基地局のところでパケットを捕まえてハードディスクに貯める
5. 解析する

難しいように思えるのは「1. 基地局をつくる」ことそのものですよ



無線ルーターなんてすぐつくれるんですよ、ほんとに



- え。どうやってつくればいいんですか
- PCにFreeBSDを入れて…っていうのが理想だったんだけど（もう256倍なんて知らないよね。。じみじみ）、ちょっとハードル高い・・・
- 適当なLinuxをつかえばできるらしいし、きっと調べれば自分でもできるはず！って思ってる人は多い
- が、実際にやってみたことある人は少ない
- 今回トライしてみました。最初はUbuntuからはじめたんですが、いろいろといじるにはDebianのほうが細かくできるので、Debianで修業したんですよ
- で、いったんDebianで作れるようになったんですけどね。ふと、
- Raspberry Piでできるんじゃない？
- っておもったら、超簡単にできた

Raspberry Piで、簡単に作れます（全体の流れ）

- Raspberry Piを買ってくる
 - ブート用のSDカードを買ってくる
 - 手持ちのPCをつかって、SDカードにRaspberry Pi用のLinux、Raspberry Pi OS (旧称 Raspbian OS)を入れる
 - SDカードをRaspberry Piにさす
 - その辺の有線EthernetをRaspberry Piにさす
 - Raspberry Piを起動して初期化する
 - キーボードだのはお好みで適当に設定する
 - “network manager”に設定変更する
 - 画面で右上のWiFiのボタンを押すと、なんと「基地局にする」設定ができる
 - 適当に設定する
 - スマホがWiFiにつながるようになる
-
- Raspberry PiにUSBの外付けハードディスクをつける。大丈夫Windows用のフォーマットをLinuxは無理なく理解する。
 - WiresharkというコマンドをAPT GETしてくる
 - Wiresharkを起動してパケットをハードディスクにぶちこむようにしたのち
 - アプリをスマホで起動すると、ハードディスクにパケットのコピーが流れ込む
 - 適当に止める
 - 解析する



Raspberry Pi の本体。
ちっちゃい基盤にEthernetと
USB (USB2とUSB3がふたつづつ)
HDMIの小さいI/Fがふたつ。電源 (USB-C)
無線LAN。そしてIoT用のピンがある
小さいのに高性能で安い



ケース (別売り) にいれてみたところ
取り回しするにはケースにいれとくほうがいい



USB2のI/Fのほうが遅いのでキーボードとマウスはこちらにいれましょう
Ethernetをその辺のLAN（たとえば家庭のFlet's）とかに刺しておきます
え？WiFi？ WiFiのインターフェースはベースステーション（基地局）にする
ので取っついてください。あとで使います



外付けHDDはUSB3のほうにつなげて速度を稼ぎます。
Raspberry PiのOSはWindowsのファイルシステムをそのまま理解するので再フォーマットとかしなくていいです。買ってきたのをそのままつけて大丈夫



ちょっと「強力な（すなわちパワーのでかい）」USB-C電源を用意します



USB電源をさすと起動しちゃうのでそのおつもりで
HDMIもつなげて画面をつかえるようにしておきましょう

Raspberry Pi OS をもってくる

マイクロSDカードを用意する

32GB くらいあれば十分

マイクロSDカードをアダプターにさしてPCのスロットへさす

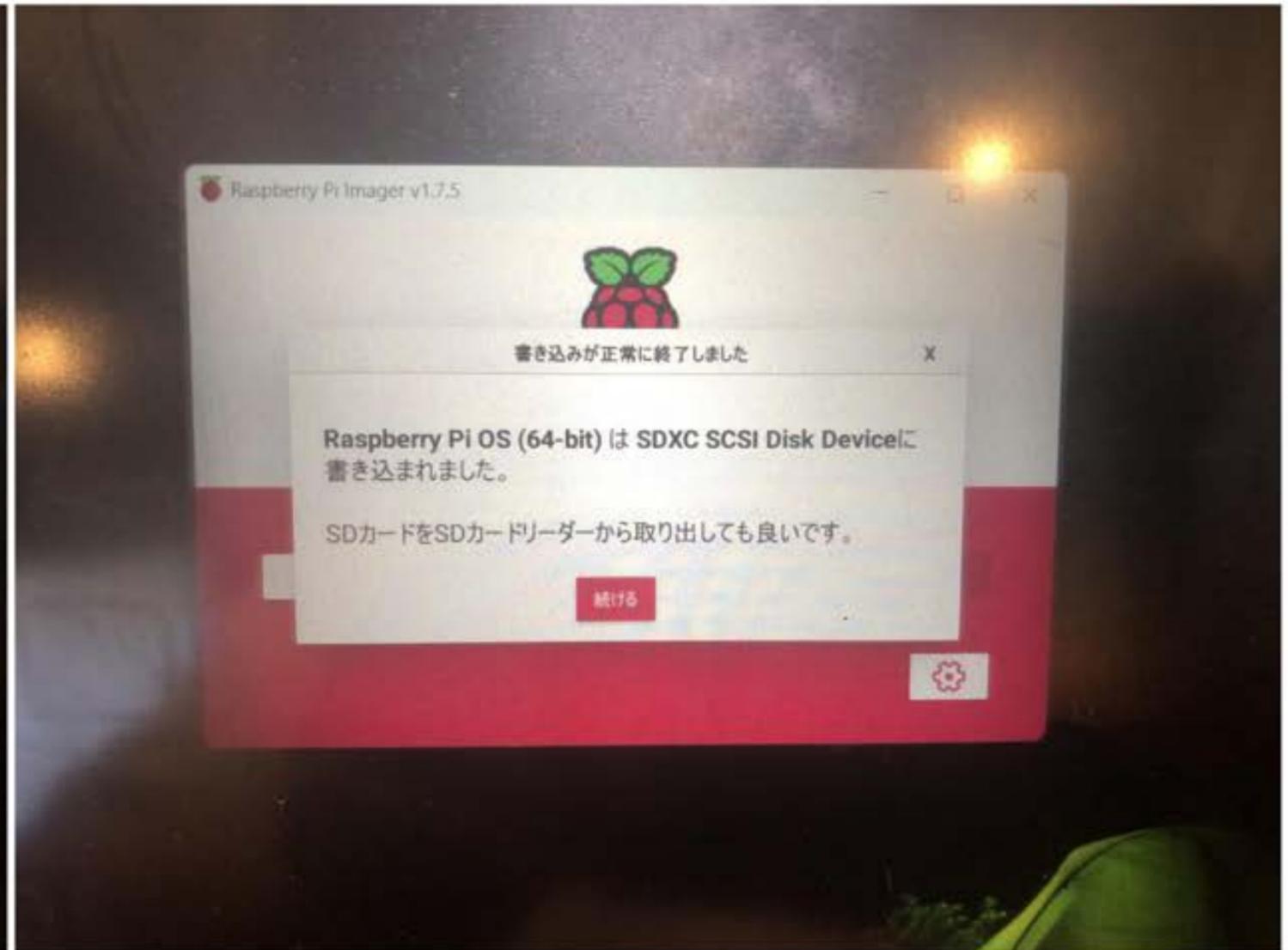
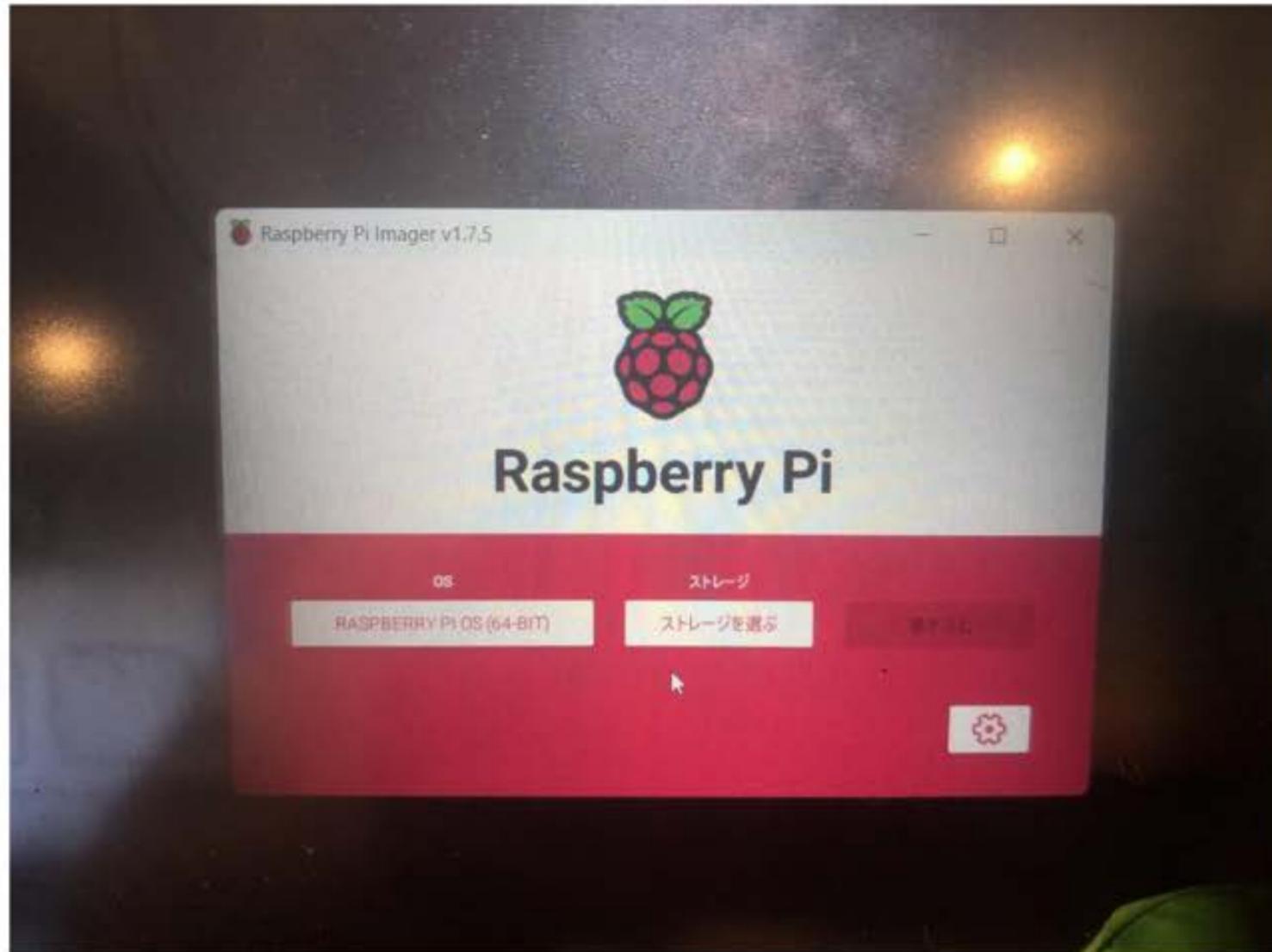
ブラウザでRaspberry Piのホームページに行く <https://www.raspberrypi.com/software/>

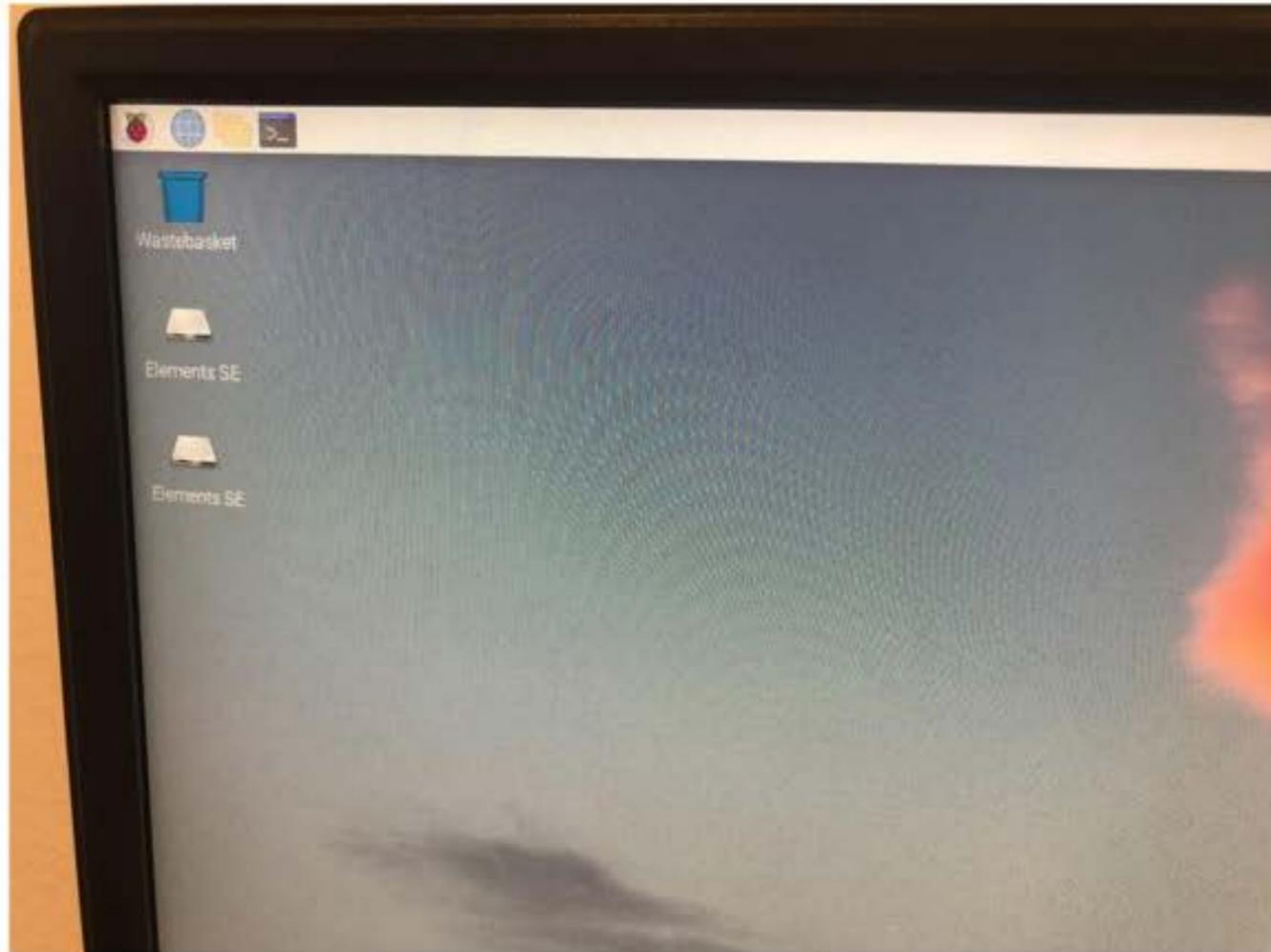
Windows 用のインストーラー (imager)をダウンロードしてインストール。起動。(Windowsを母艦にする場合)

どのOSをいれますか? と選べるので、64Bitの新しいRaspberry Pi OSを選ぶとよいでしょう

で、SDカードへイメージを書き込む







SDカードをさして電源をON。いろいろとアカウントをどうするか、とかパスワード設定しろとか、聞かれたりしますが適当にいれていくと、最終的に画面がたちあがりこうなります

Raspberry Pi 起動

OSをいれたSDカードを起動

Keyboardの設定を変えたほうが僕は使いやすいです（日本語キーボードにしてCtrlとCapsを入れ替える）

管理ツールをNetwork Managerに変更する（とても大事）

[Raspberry Pi OSのWi-Fi設定ツール「Network Manager」の追加 | ラズパイダ \(raspida.com\)](https://raspida.com/network-manager)

<https://raspida.com/network-manager>

要するにraspi-config というコマンドをたちあげて、ツールを変更してリブートすると

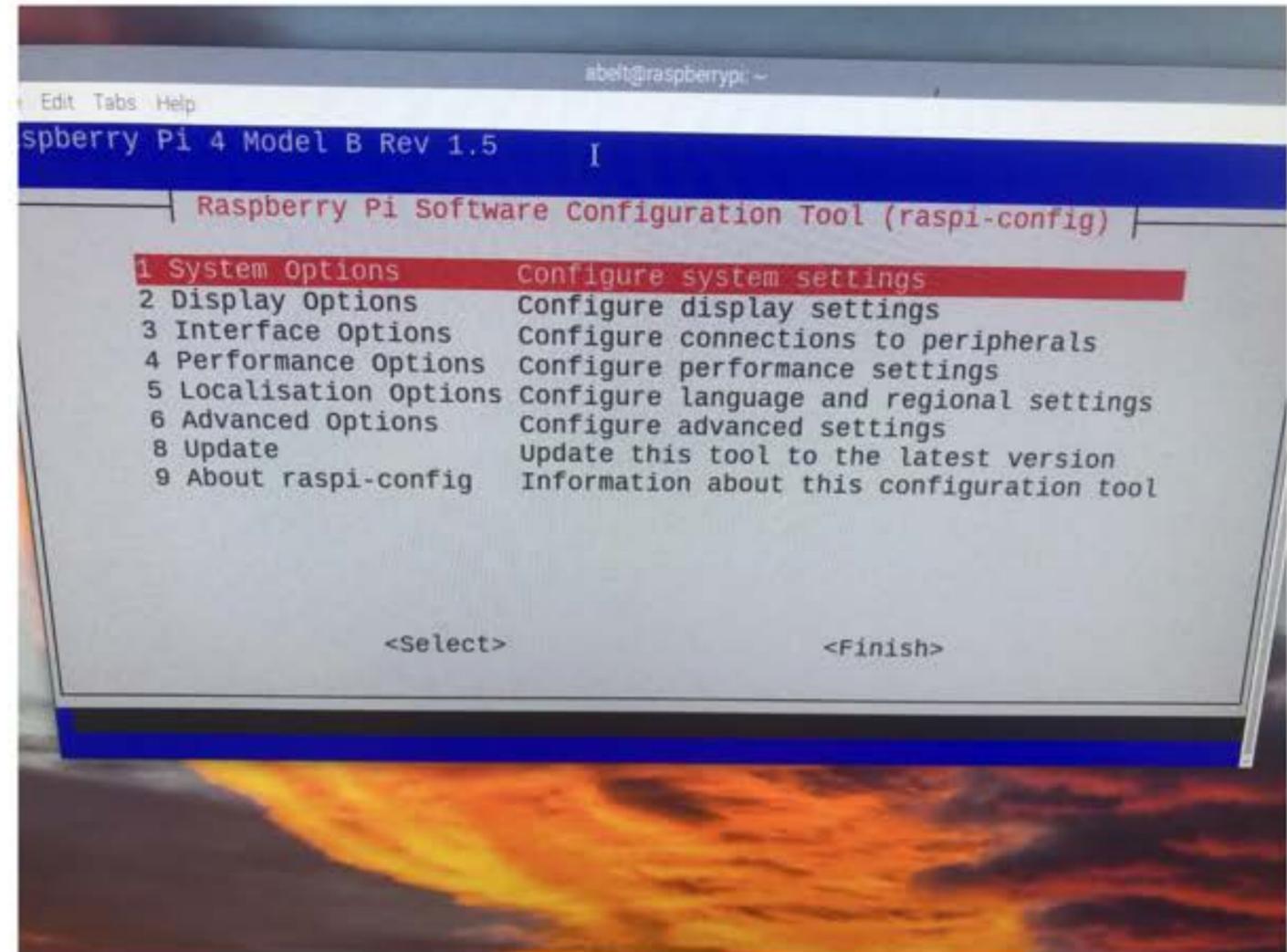
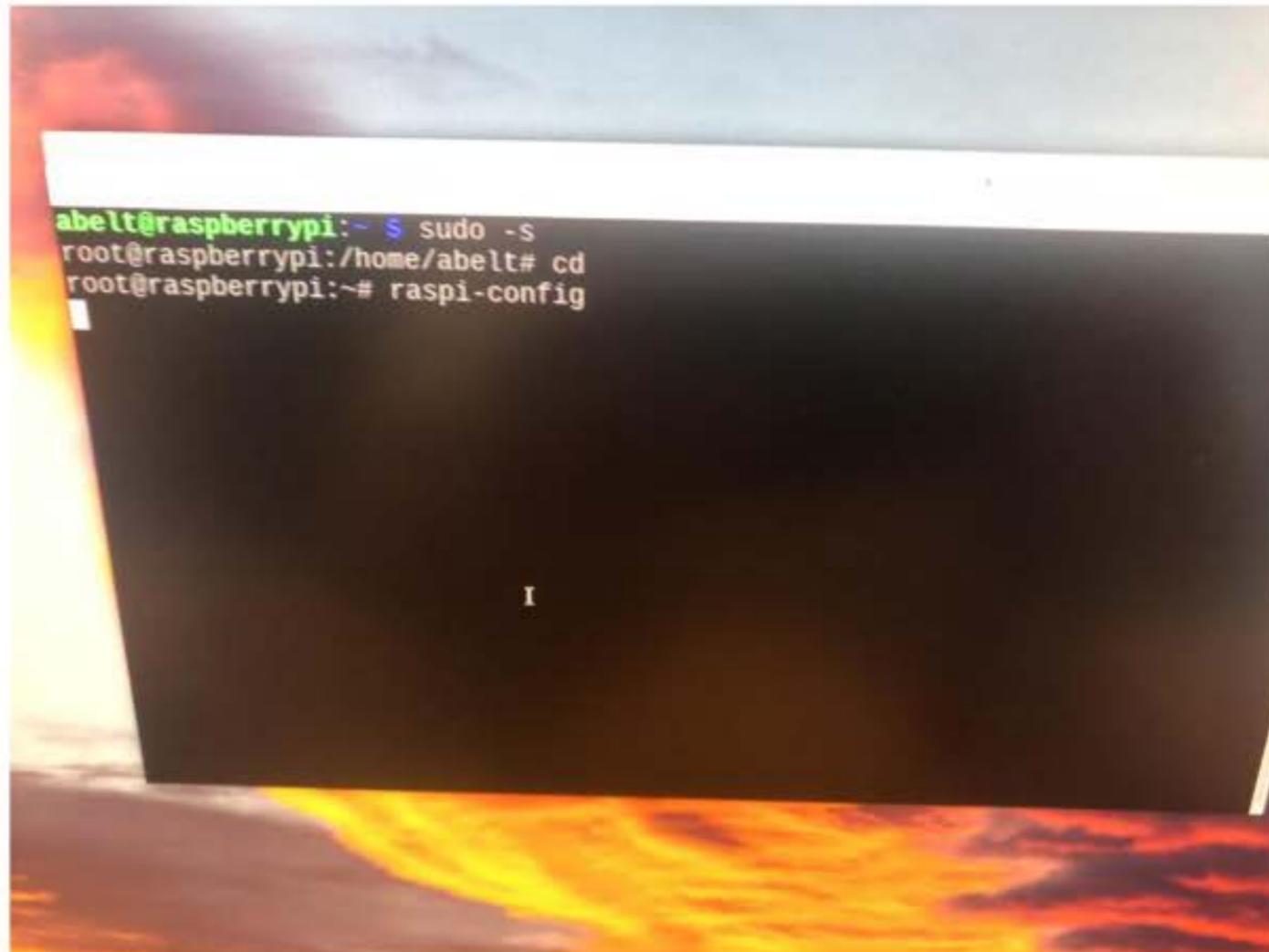
すぐに基地局モードへと設定できてしまう

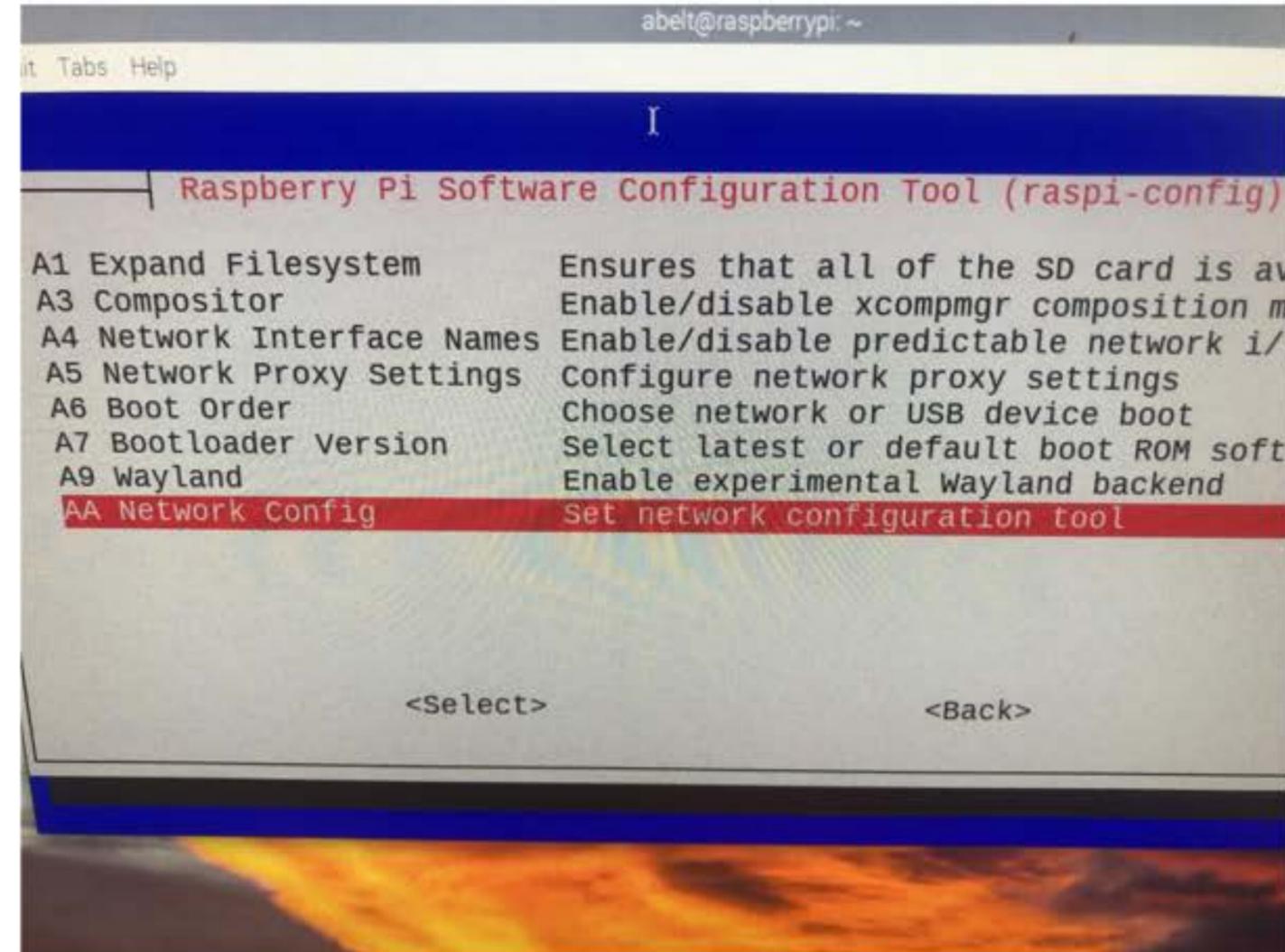
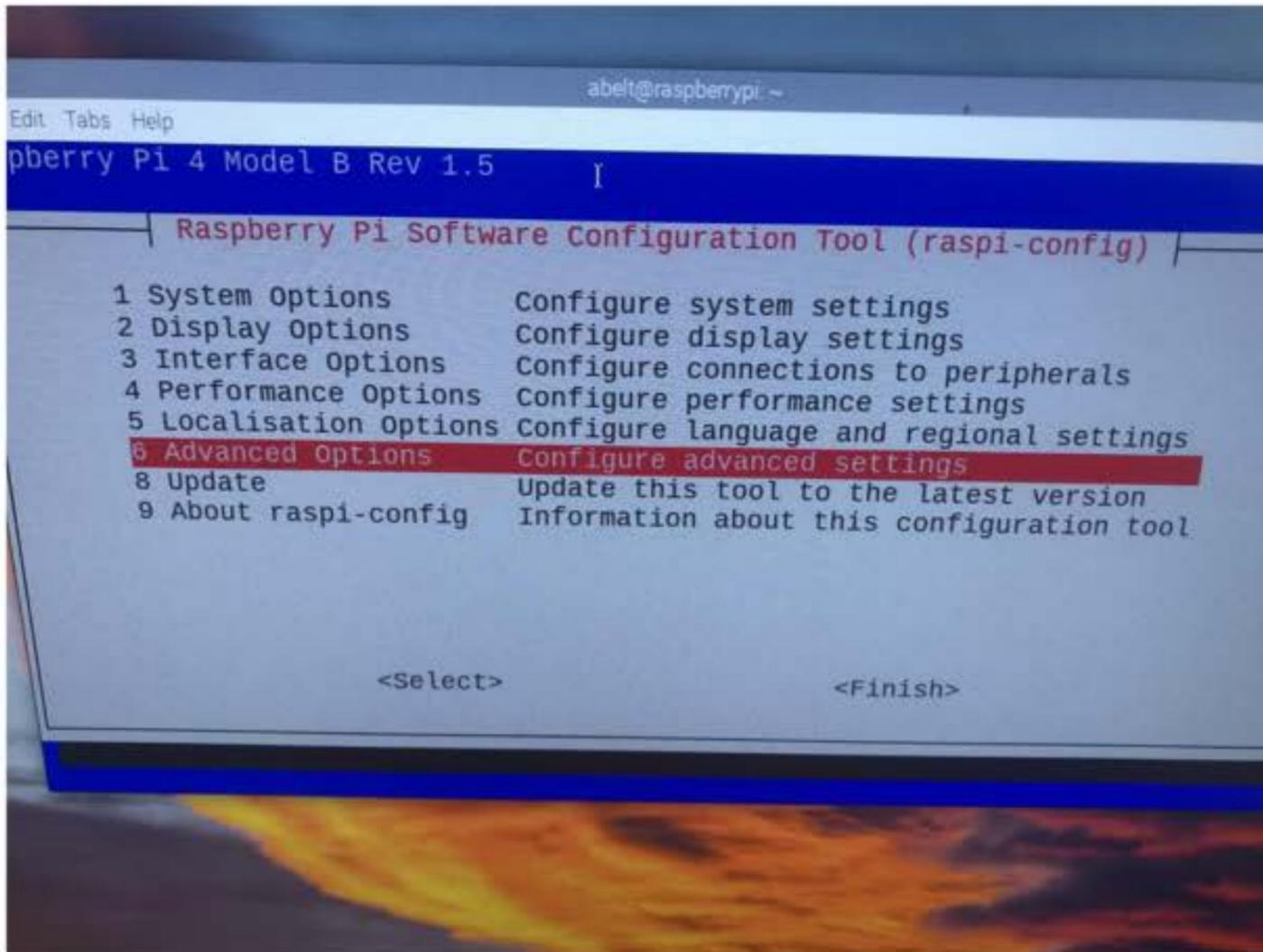
```
abelt@raspberrypi:~$ sudo -s
root@raspberrypi:/home/abelt# vi /etc/default/keyboard
root@raspberrypi:/home/abelt# reboot
```

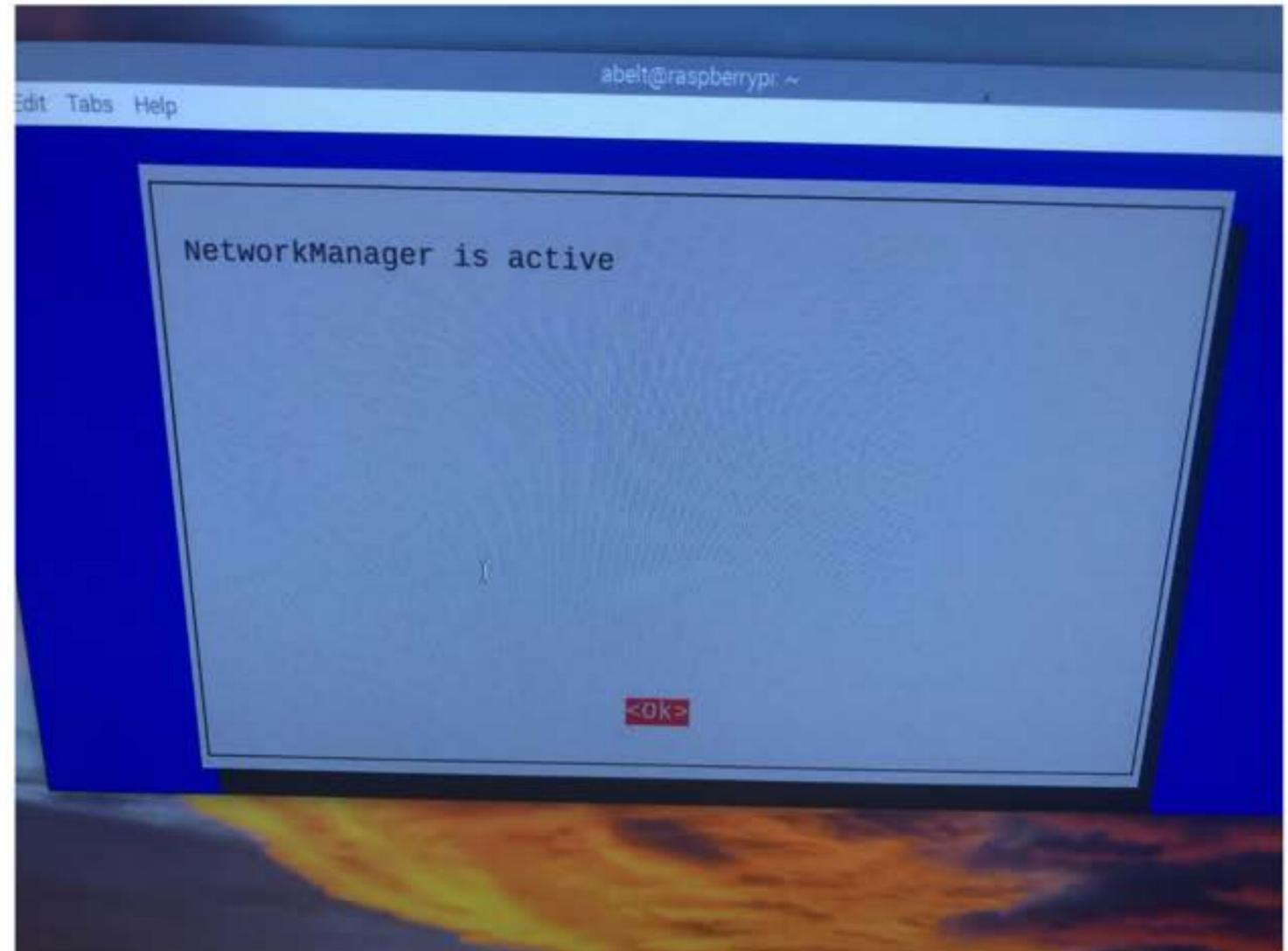
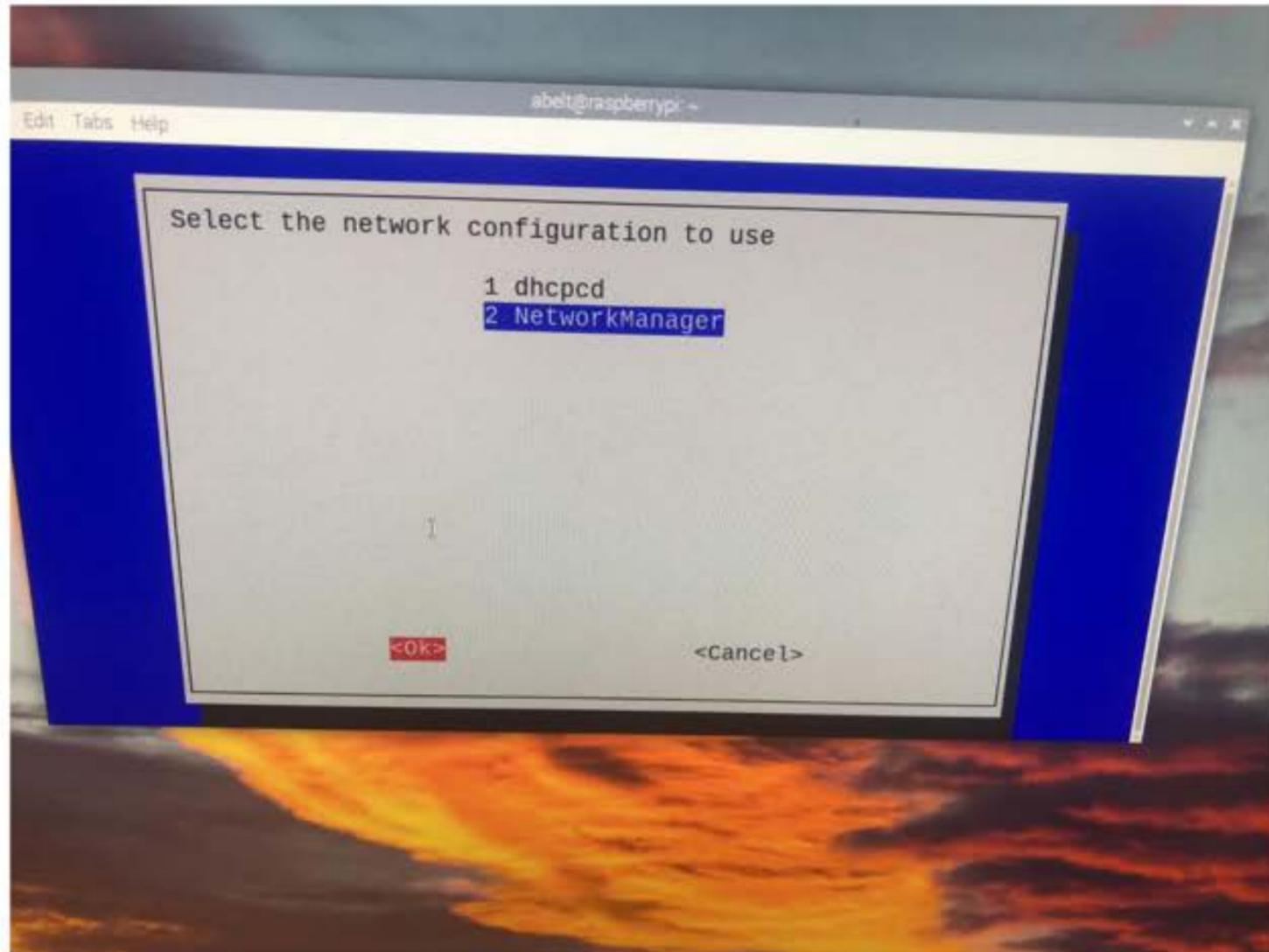
```
# KEYBOARD CONFIGURATION FILE
# Consult the keyboard(5) manual page.

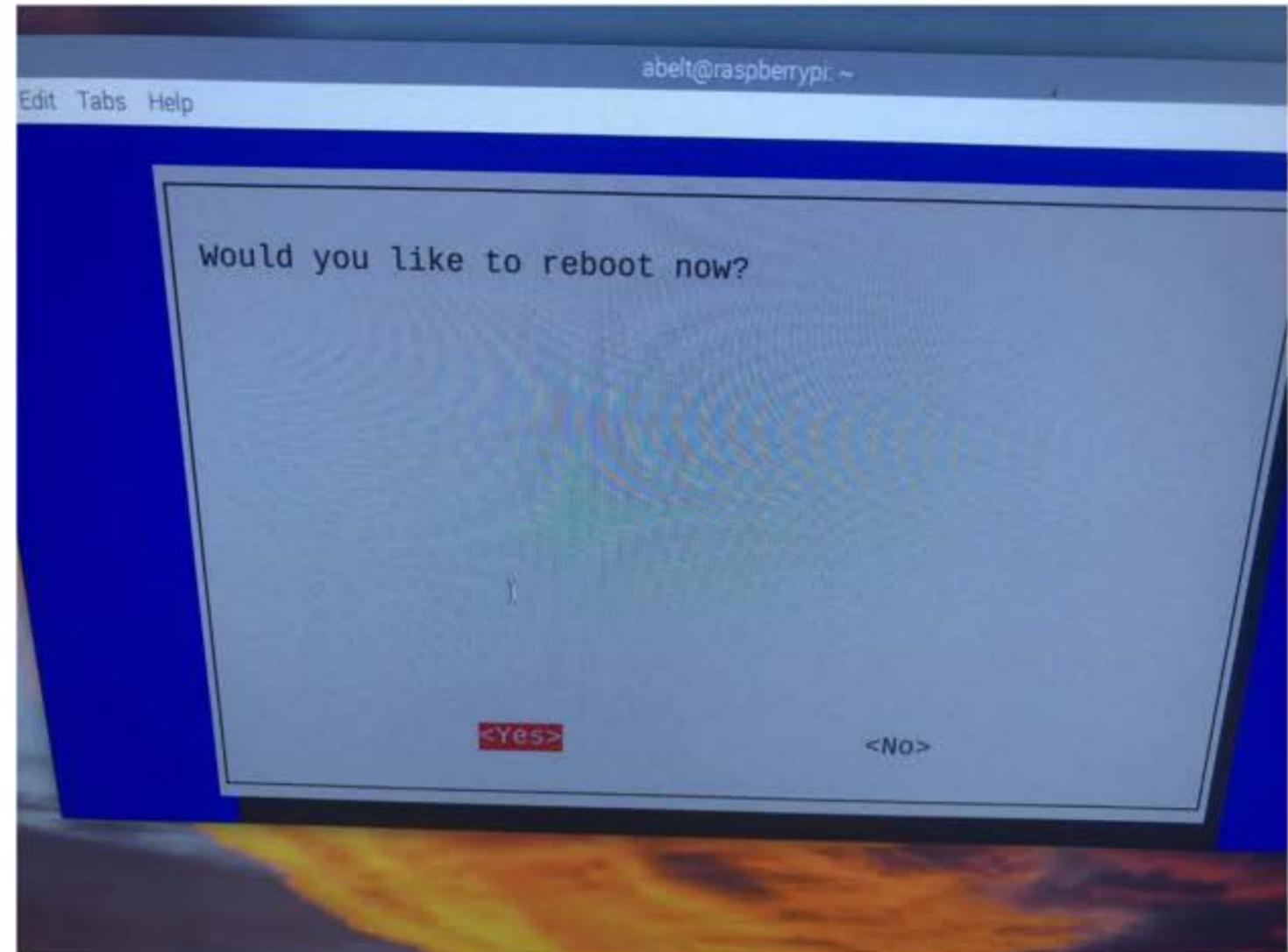
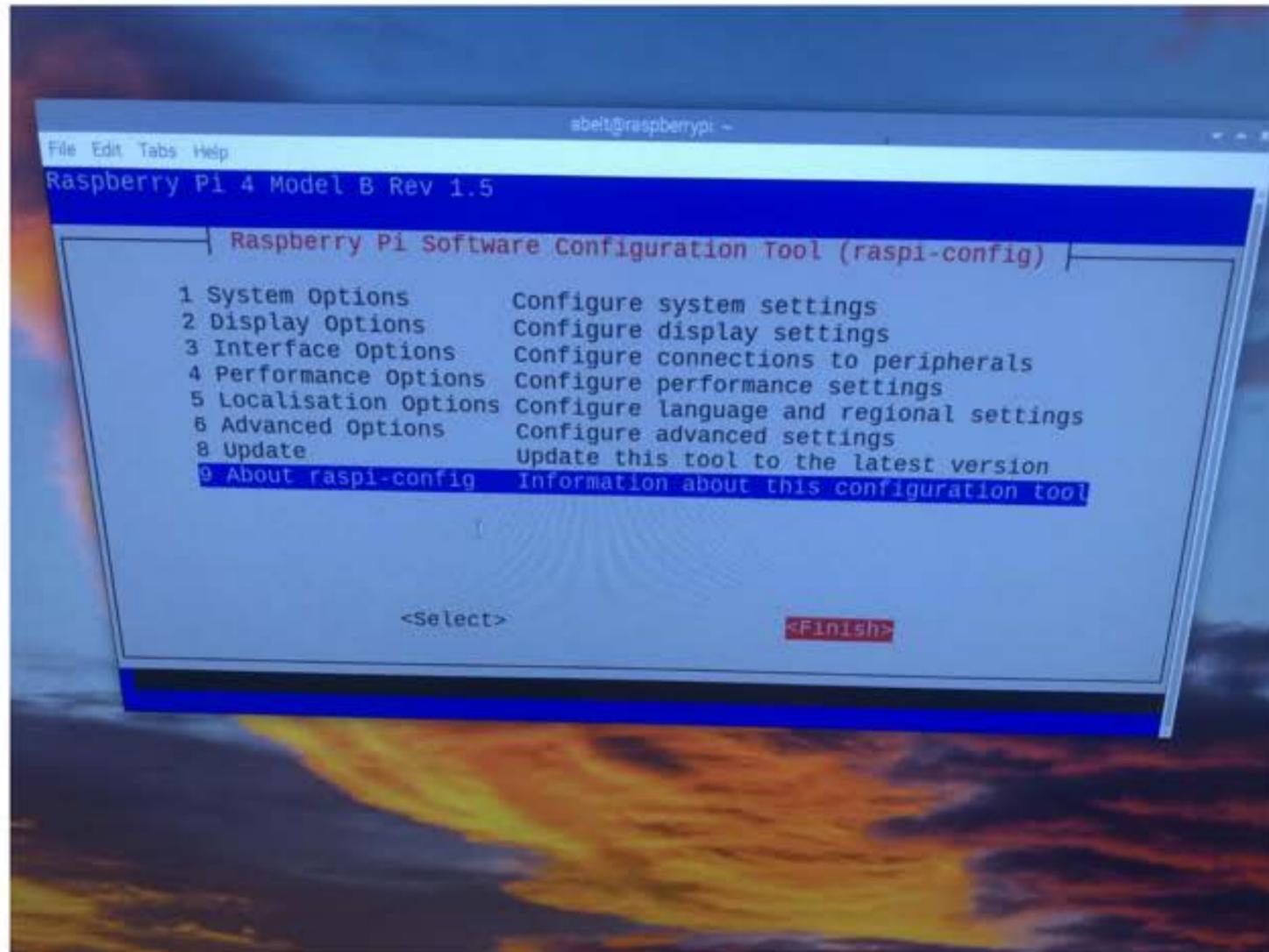
XKBMODEL="jp106"
XKBLayout="j"
XKBVARIANT=""
XKBOPTIONS="ctrl:swapcaps"

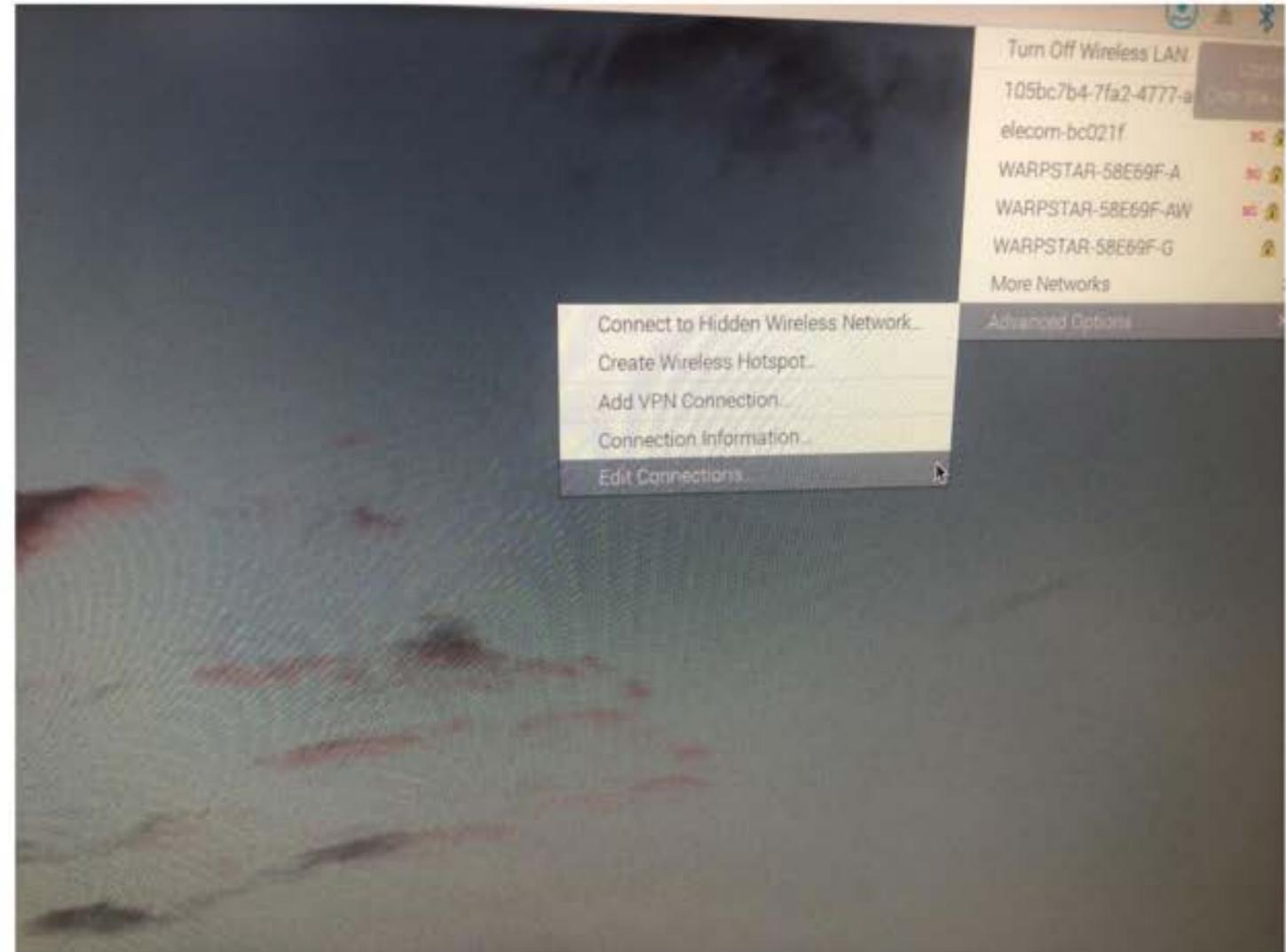
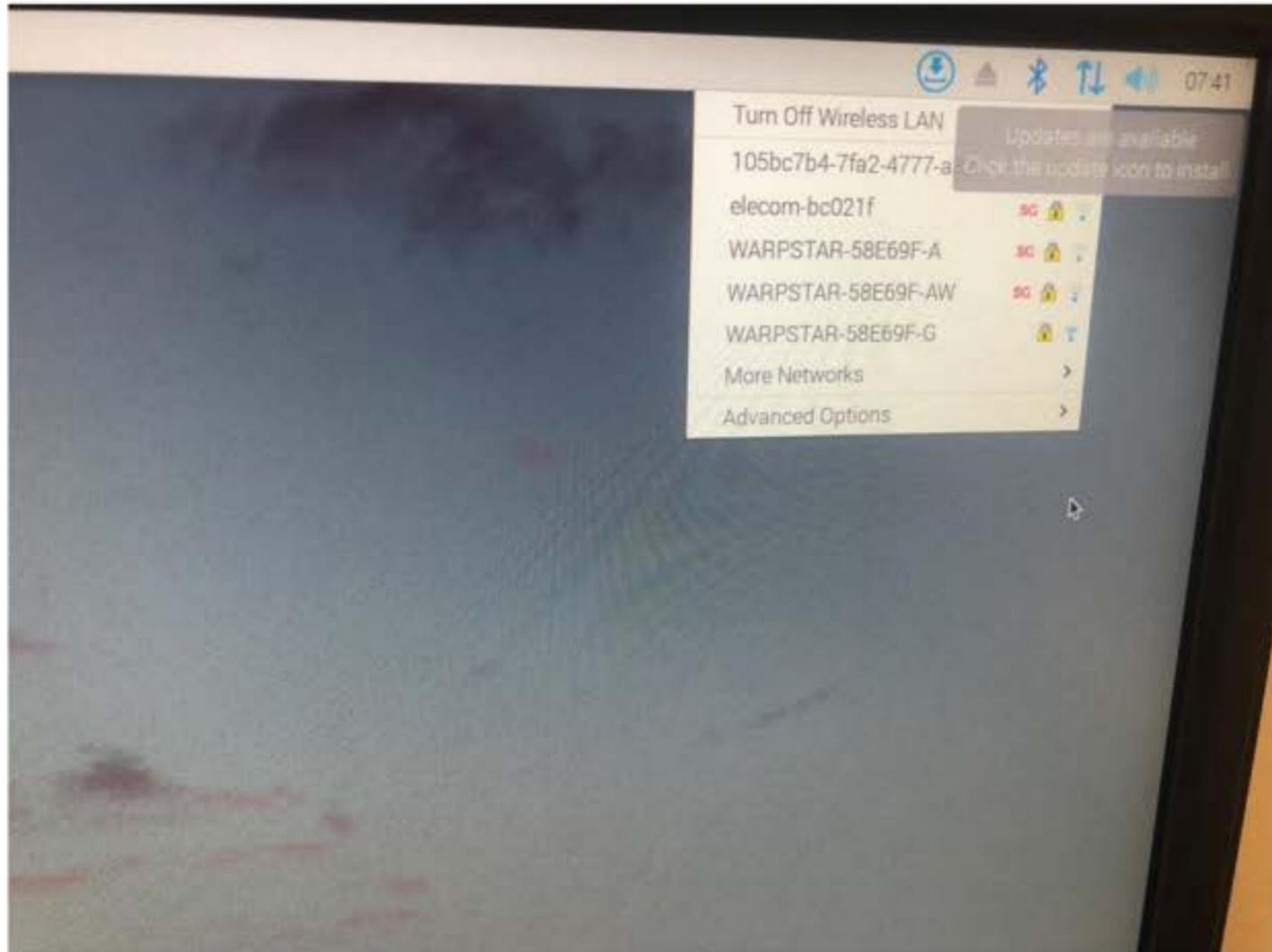
BACKSPACE="guess"
```

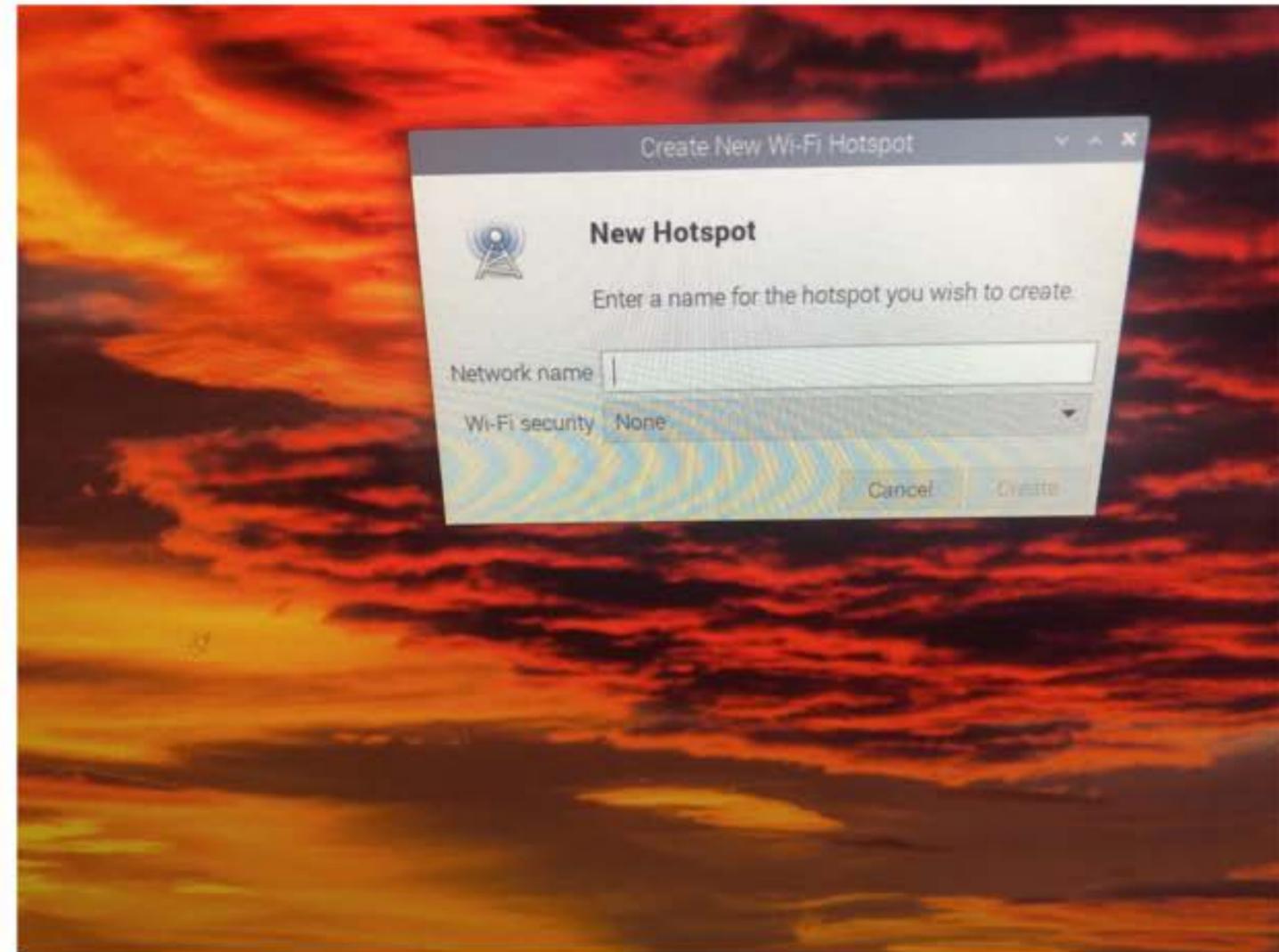
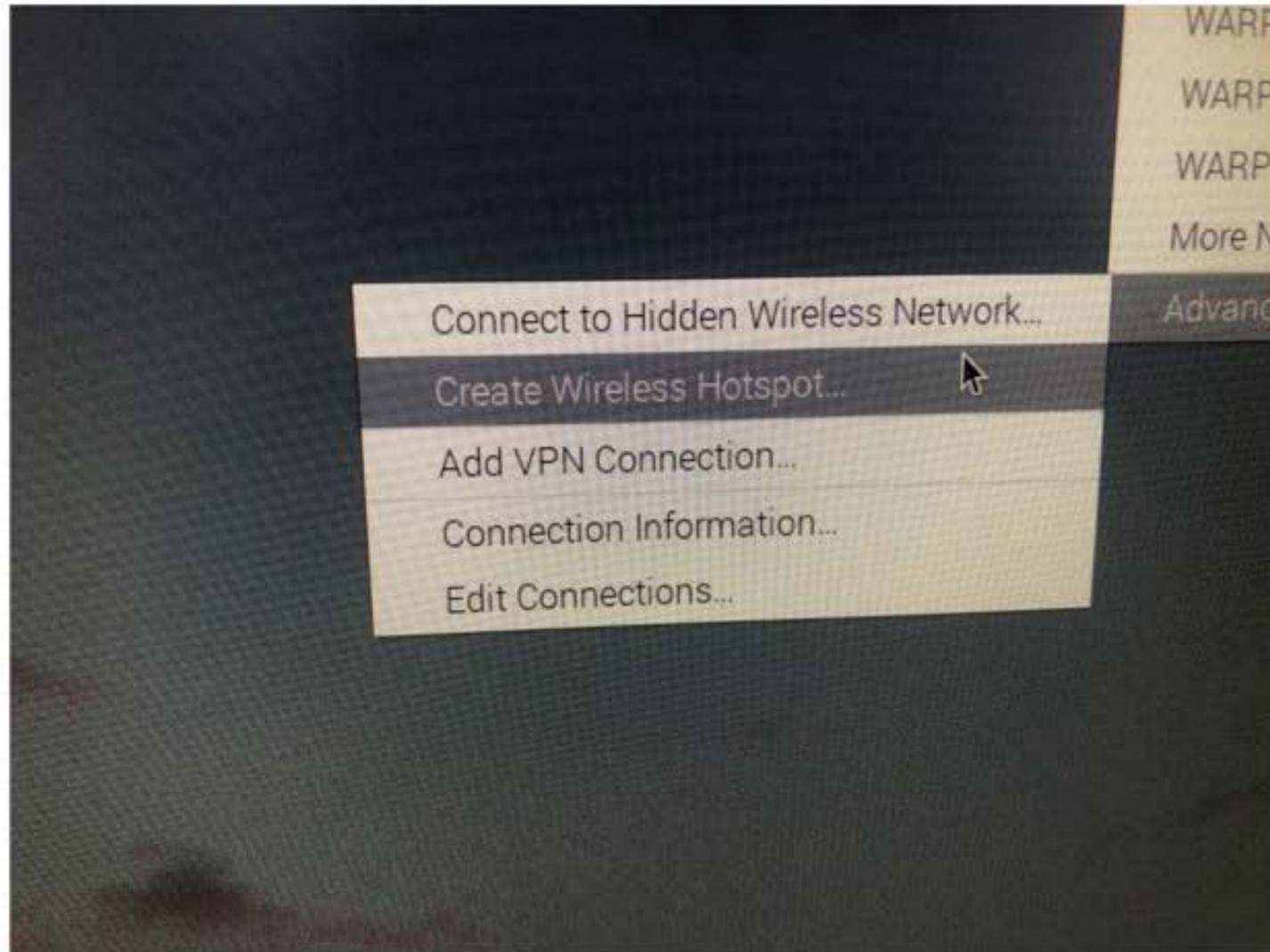


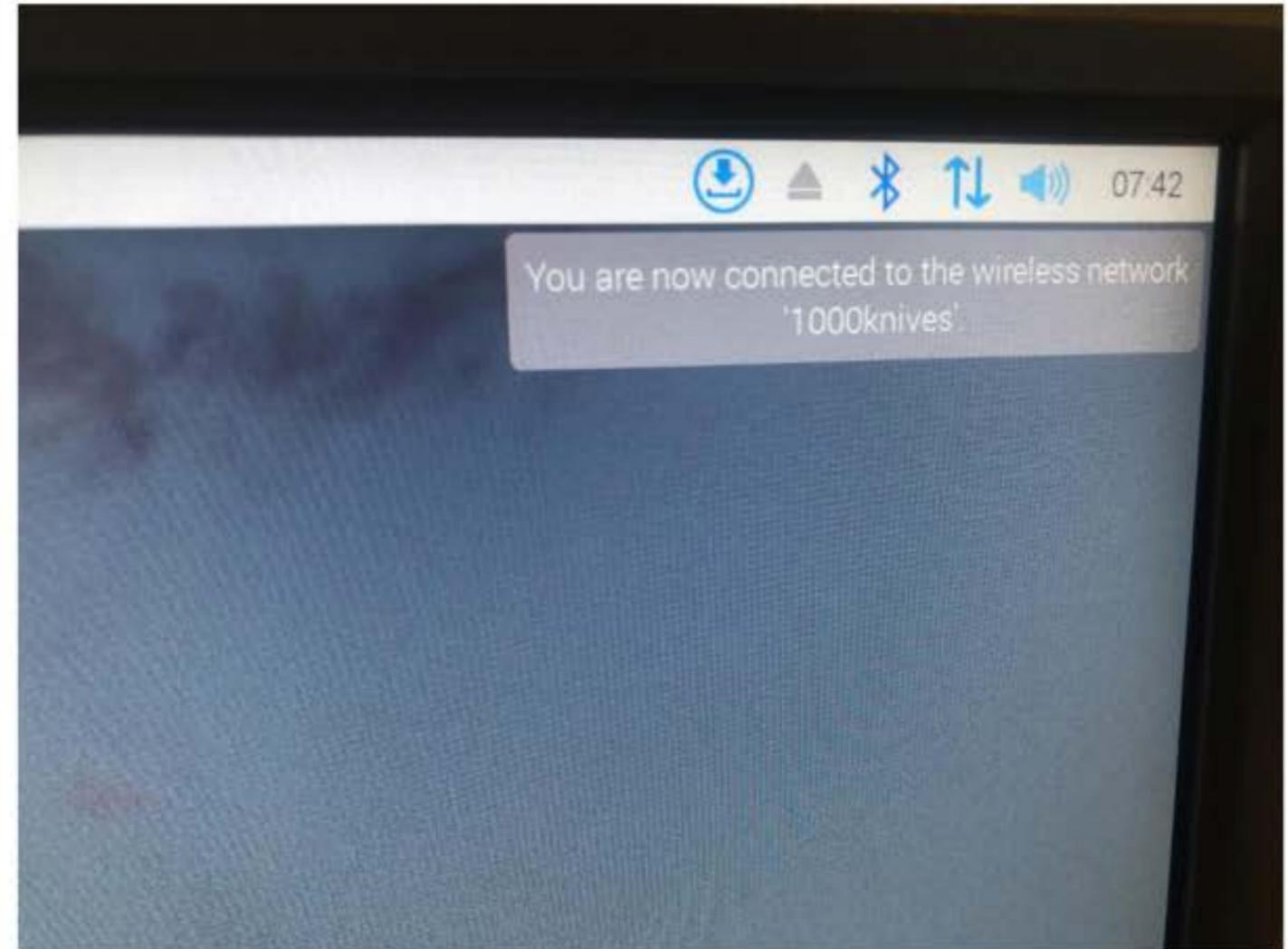








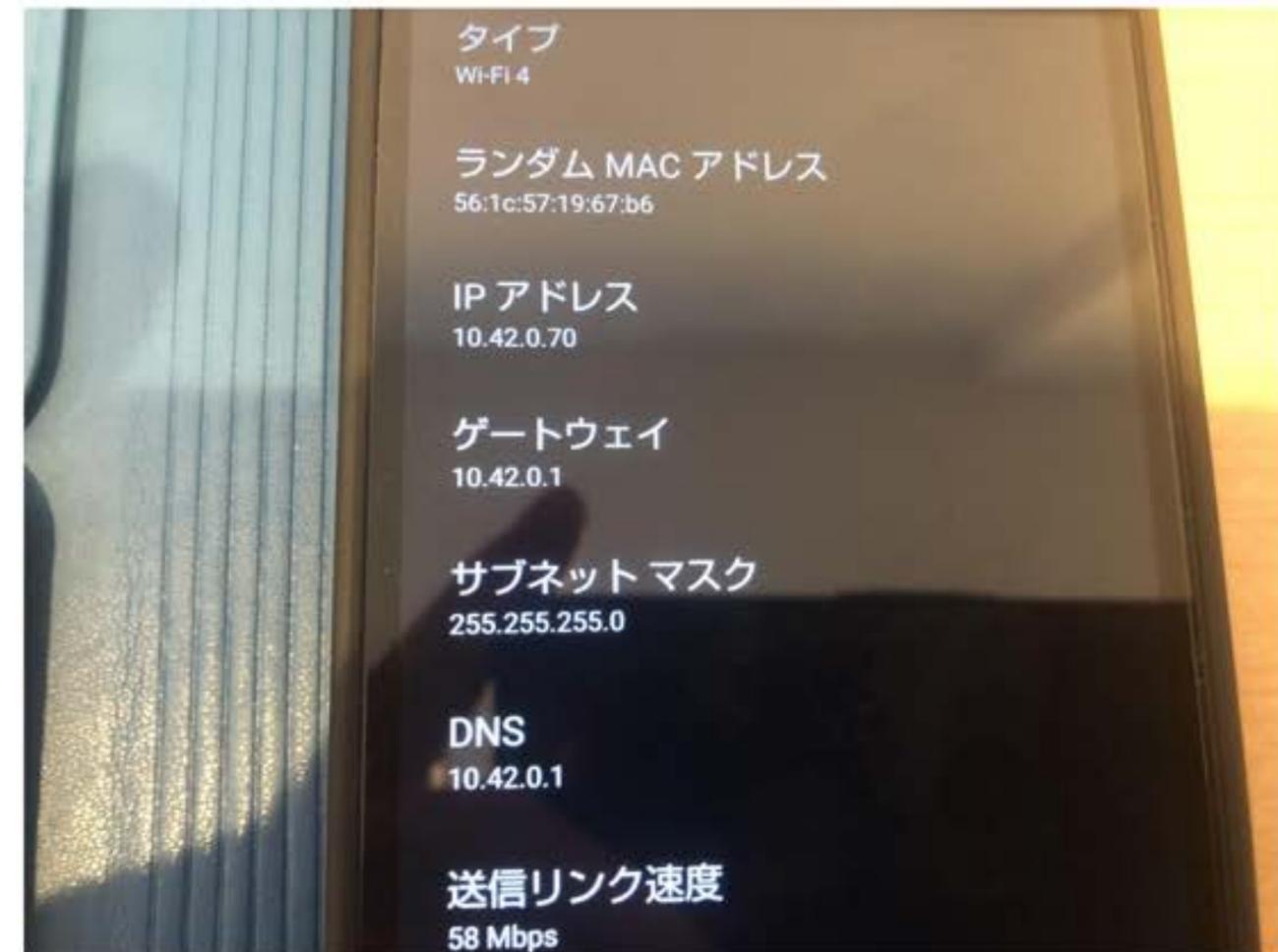




調べたい対象をつなげる

調査用の無線LANができれば、調査対象の機器をそこにつなげて動作するようにしましょう

調査対象のアプリケーションが動作することも確認すること



Wireshark、Whois、Tracerouteを入れる

ターミナルからsudo -sしてRootになって

```
apt install wireshark
```

```
apt install whois
```

```
apt install traceroute
```

こんだけいれとけばとりあえずの調査ができます

Wiresharkがパケットをつかまえるツールです

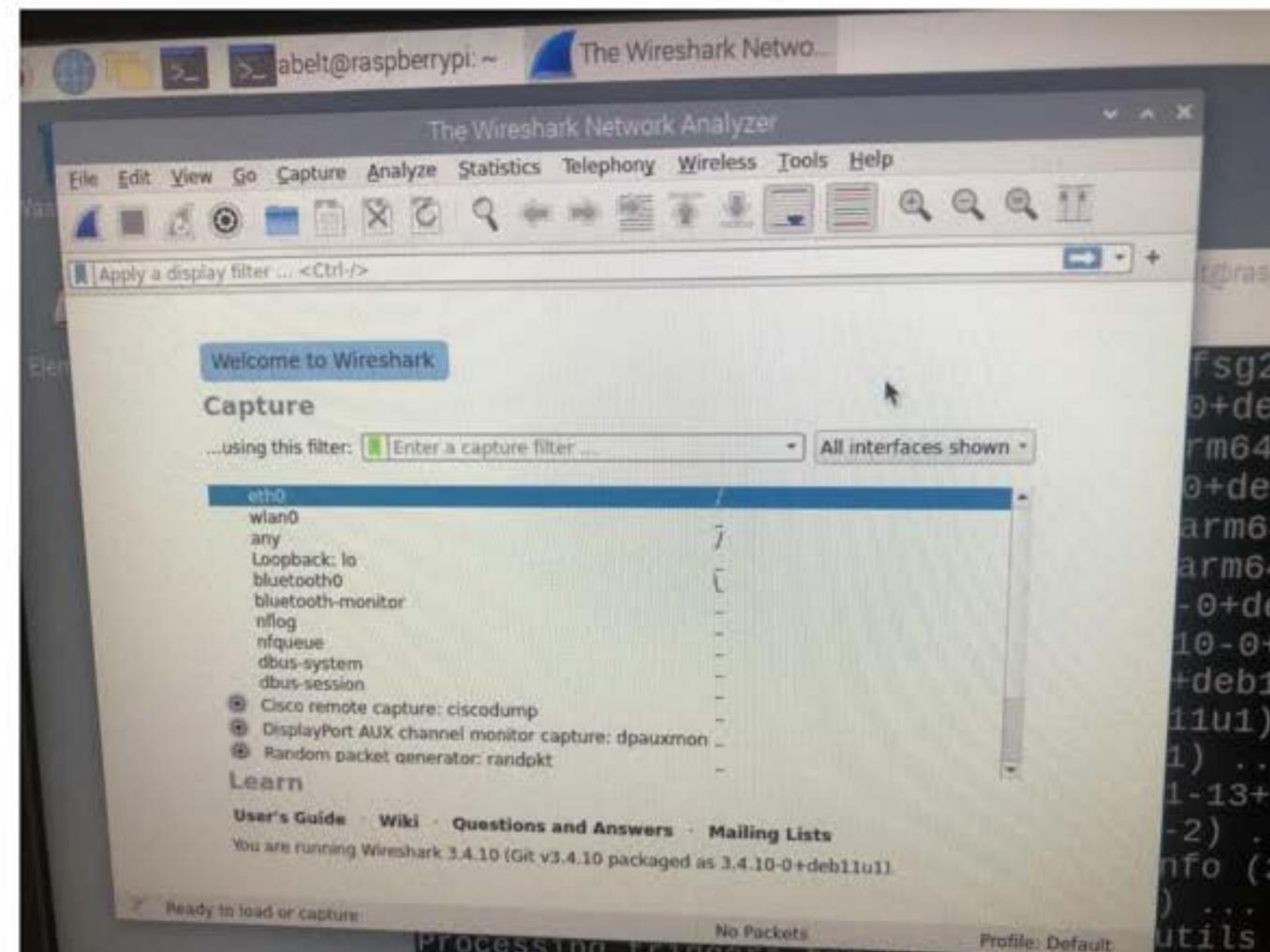
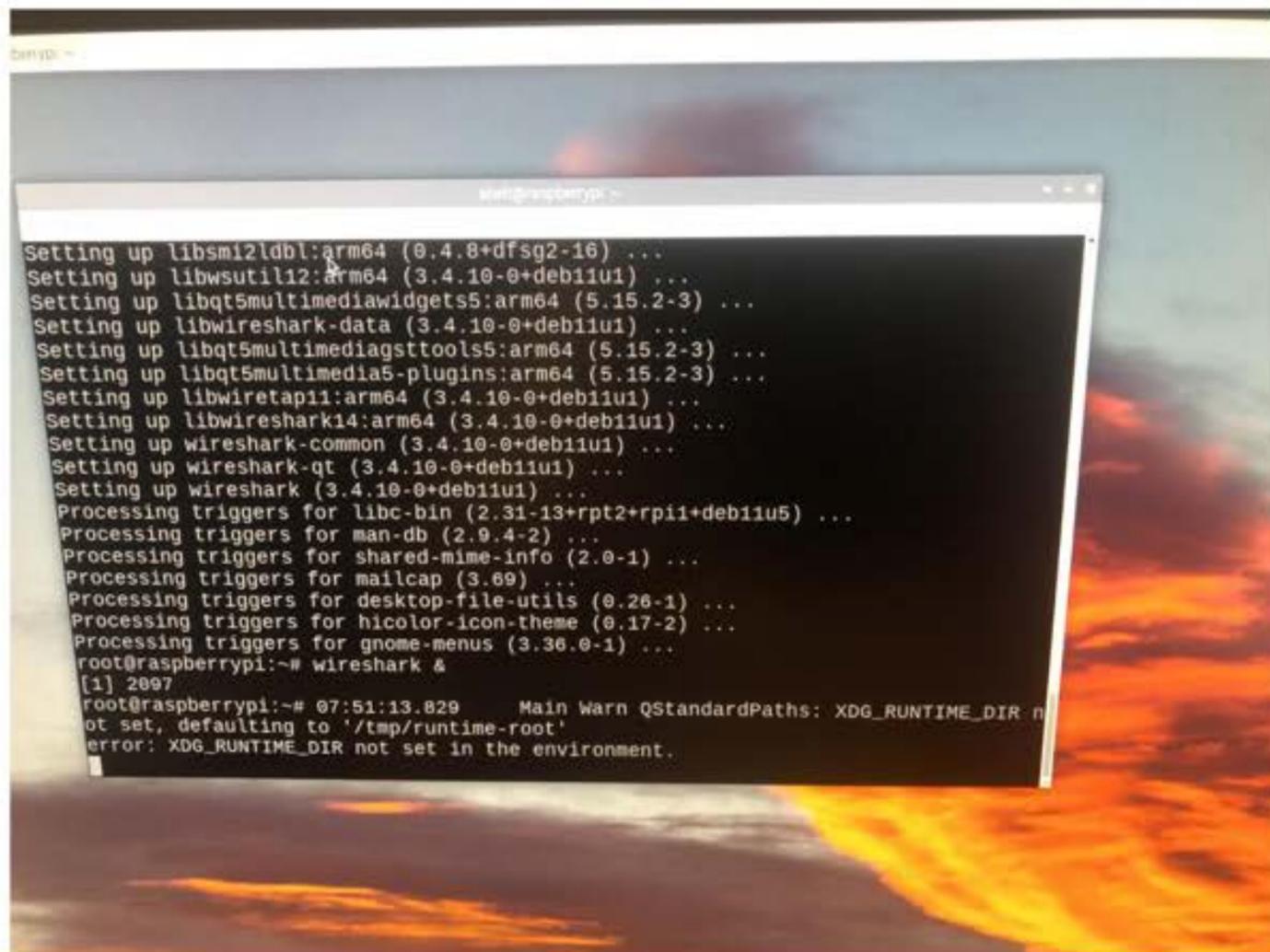
Wiresharkをつかってパケットを捕まえます

どのインターフェースから採取するか

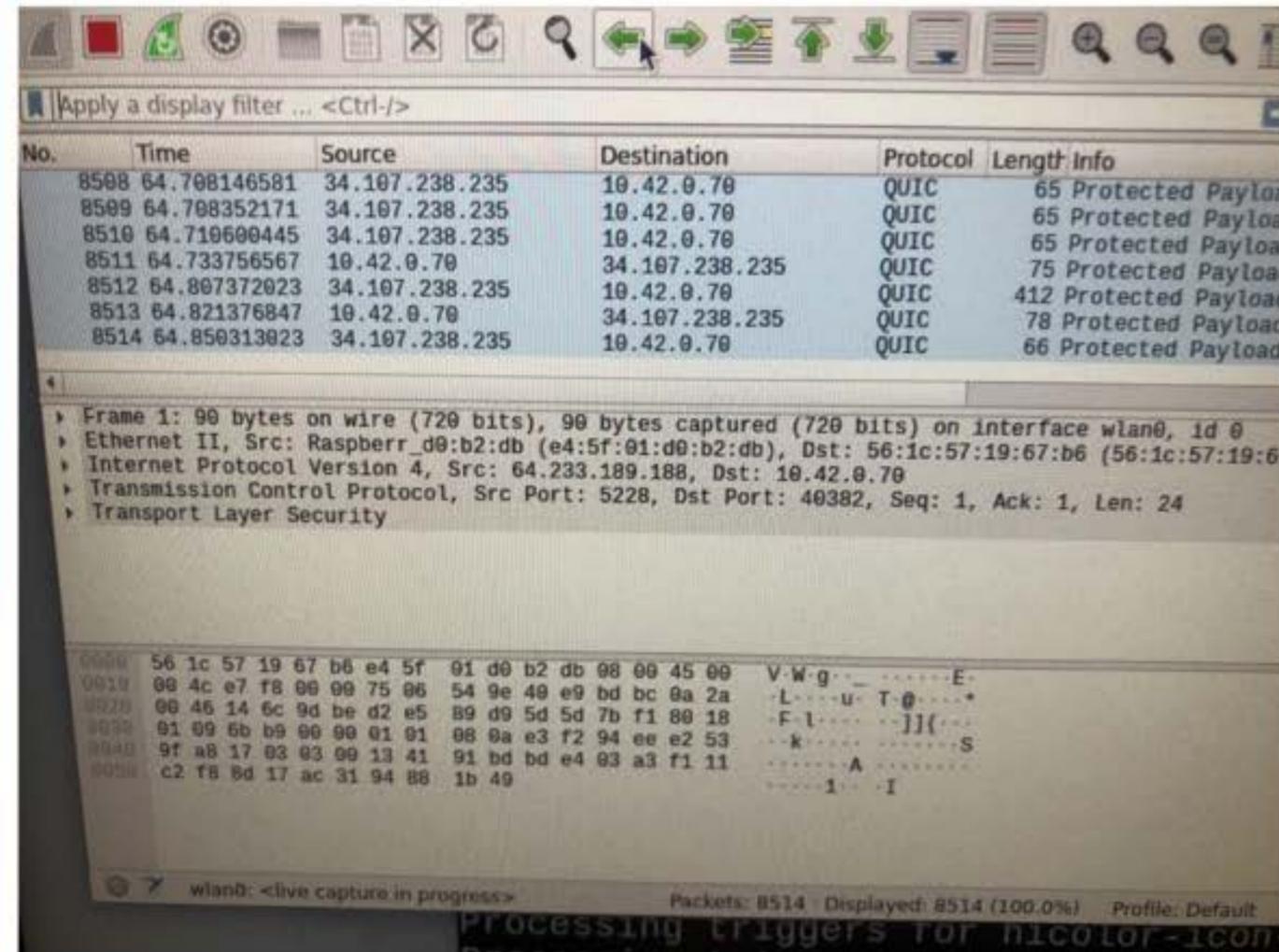
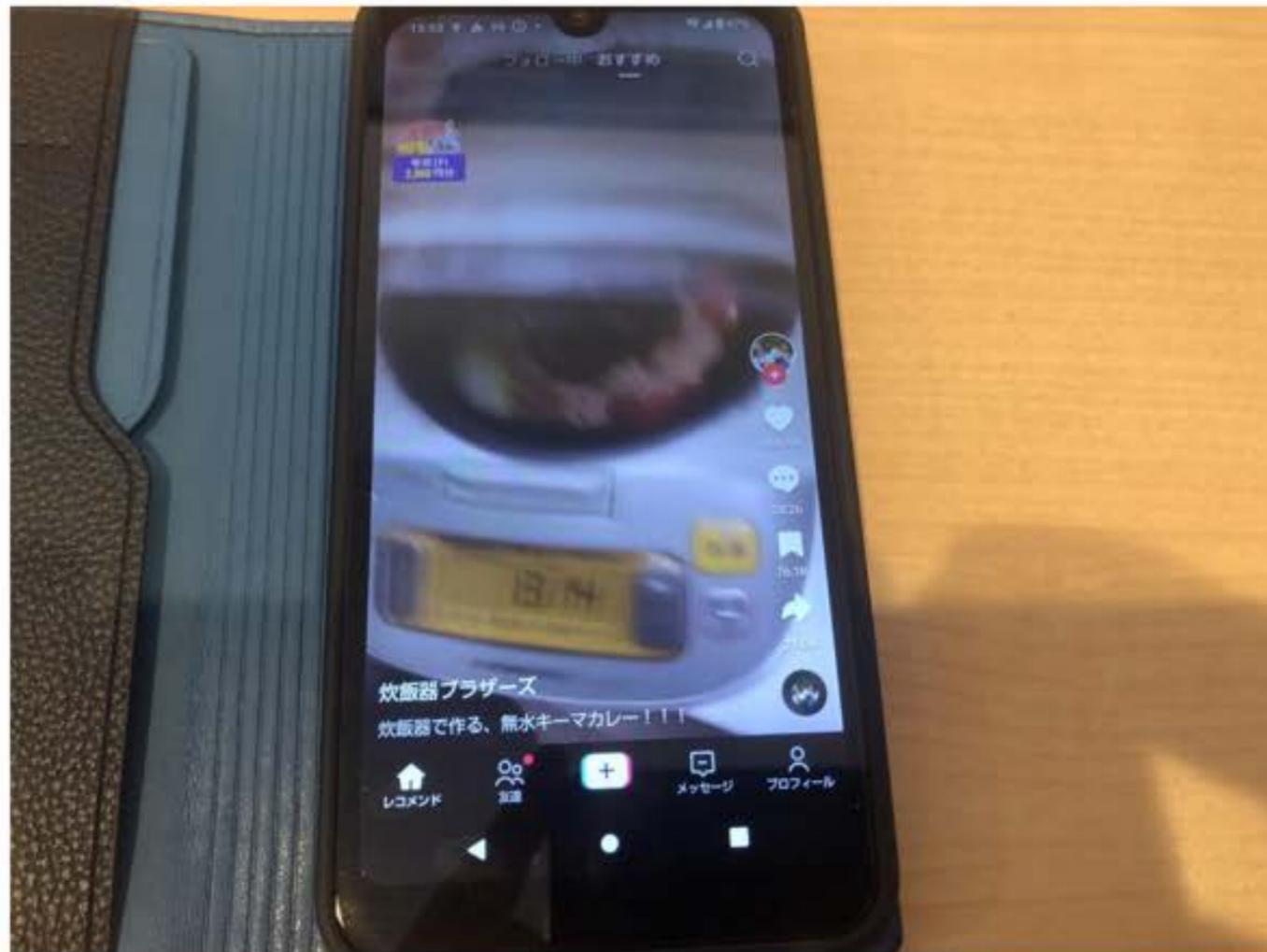
条件付けもできる

採取したパケットをファイルに記録することもできる

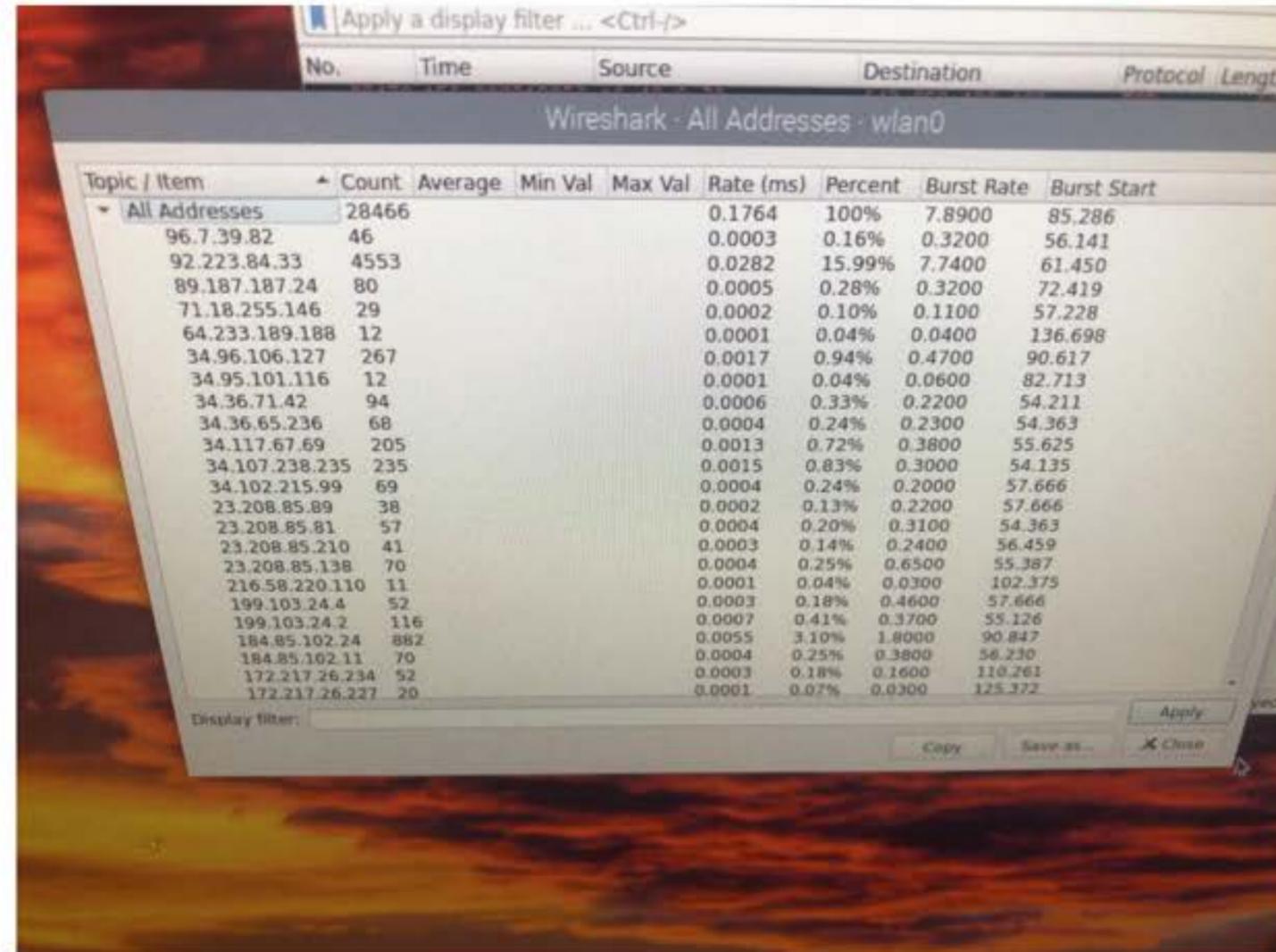
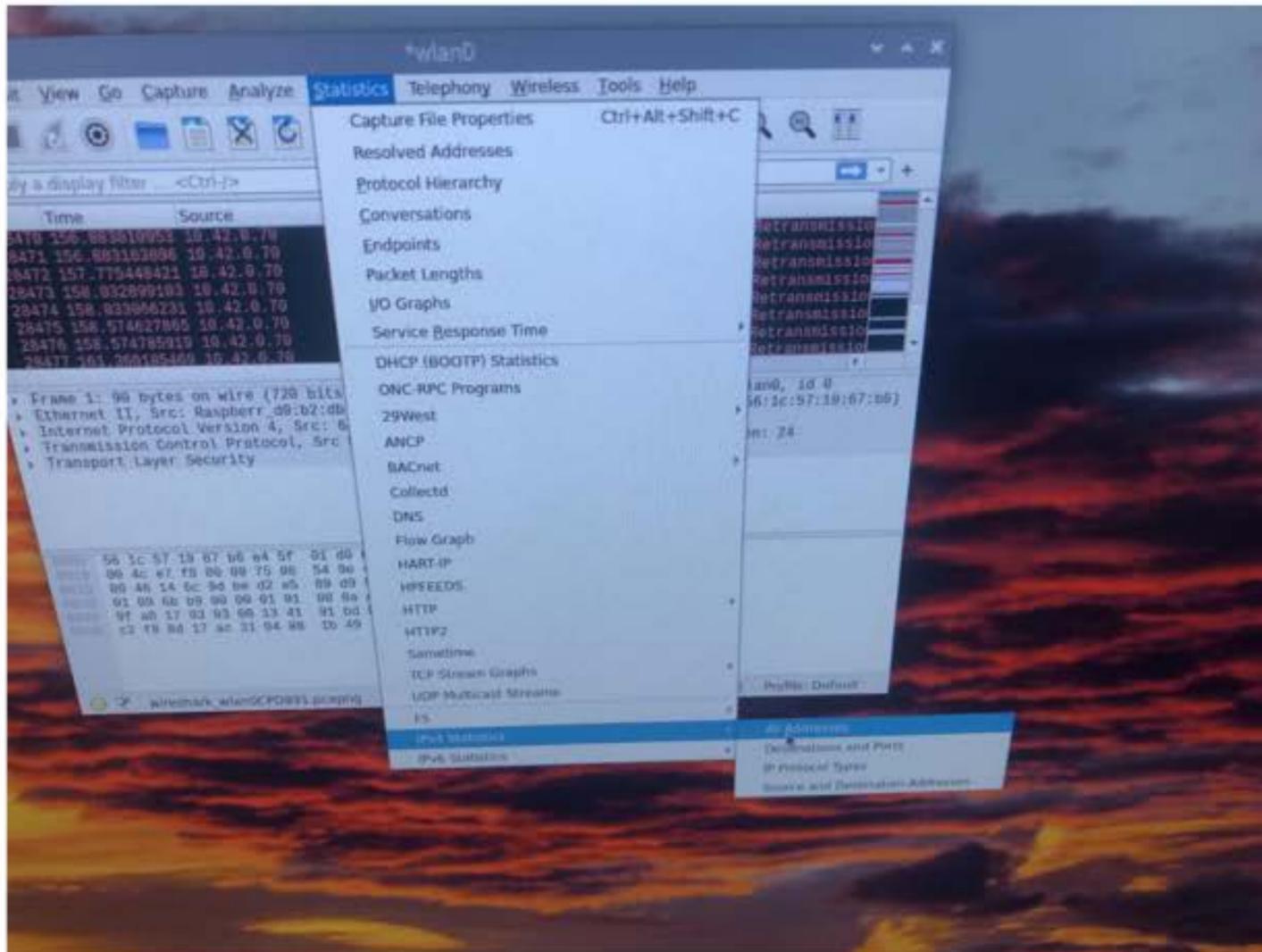
パケット自体の解析も可能



sudo -s して apt install wireshark したら wireshark & してたちあげると、GUIがたちあがってきます。入カインターフェースを wlan0 にして、左上の青い波のボタンをおすとパケットキャプチャーがはじまります。あ、メニューから出力先を外付けHDDのファイル指定したりしておいてもいいですよ



調査対象のスマホでTikTok起動！すると、右のようにパケットが流れているのがどんどん表示されていきます。ほとんどQUICだなあ。。。中身わかりませんねえ。



パケットのダンプをストップ（赤いボタンを押すと止まります）して、タブからStatisticsのところ例えばIPv4 address を選ぶと、右のように、使われているIPv4アドレスがリストされ、何個（Count）とんできたか、とかが表示されます。これでどこと通信してるのかが一目瞭然です

whois は、IPアドレスがだれのものなのかを調べます



IPアドレスは払いだされるときに「誰がもってるか」を登録する必要があります

whoisコマンドを使うと、どこの誰がそのIPアドレスの保有者なのかわかります

でも、固定IPアドレス1個とか8個とかを例えばOCNから払い出してもらったりしても外のデータベースから見ると、OCNが持っているようにみえるだけです。個人の方は安心してください。日本では、裁判所の令状がないとIPアドレスの開示はできないようになっています。これは憲法に定める通信の秘密に起因することですので非常に大事に守られています（ただし、児童ポルノに関するときは、児童の人権のほうが通信の秘密より優先されるためにちょっと違う扱いが行われます）

```

If you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#
root@raspberrypi:~#
root@raspberrypi:~# whois 184.85.102.9
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#
NetRange:      184.84.0.0 - 184.87.255.255
CIDR:          184.84.0.0/14
NetName:       AKAMAI
NetHandle:     NET-184-84-0-0-1
Parent:        NET184 (NET-184-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      Akamai Technologies, Inc. (AKAMAI)
Organization: Akamai Technologies, Inc. (AKAMAI)
RegDate:       2010-03-03
Updated:       2012-03-02
Ref:           https://rdap.arin.net/registry/ip/184.84.0.0
OrgName:       Akamai Technologies, Inc.

```

```

@raspberrypi:~# whois 71.18.255.144
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#
NetRange:      71.18.0.0 - 71.18.255.255
CIDR:          71.18.0.0/16
NetName:       BYTED
NetHandle:     NET-71-18-0-0-1
Parent:        NET71 (NET-71-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      Bytedance Inc. (BYTED)
Organization:  Bytedance Inc. (BYTED)
RegDate:       2021-12-16
Updated:       2021-12-16
Ref:           https://rdap.arin.net/registry/ip/71.18.0.0
OrgName:       Bytedance Inc.
OrgId:         BYTED
Address:       3000 El Camino Real Building 2 Suite 400
City:          Palo Alto
StateProv:    CA
PostalCode:   94300
Country:       US
RegDate:       2018-08-09
Updated:       2021-11-18

```

Akamaiと通信してるなあ。。。動画のCDNはAkamaiなのかしらん。。。で、やっぱりByteDance社と通信はしてるんですね。あたりまえですが。ByteDance、シリコンバレーのPalo Altoの住所でアドレス取得してますね。3000 ElCamino Real, Palo Alto, CAだと。。。だいたいあの辺かあ。。。中国の会社なんですけどね

[ByteDance - Wikipedia](#) 「ByteDance (バイトダンス、**簡体字**: 字节跳动; **繁体字**: 字節跳動) は、[動画共有サービスTikTok](#)などを運営する**中華人民共和國**のテクノロジー企業。」

Tracerouteでパケットがどこを通るかわかります

Tracerouteをつかうと、パケットがどこを通過して目的地につくかがわかります

注目すべきは途中のIPアドレスと、相手に届くまでの時間です

相手に届くまでの時間をみると、相手が地球上でどれくらい離れたところにいるのかがわかります

途中のIPアドレスをみているとどの業者がサービスをだしているかのヒントがわかります

```

you see inaccuracies in the results, please report at
https://www.arin.net/resources/registry/whois/inaccuracy_rep
copyright 1997-2023, American Registry for Internet Numbers,

root@raspberrypi:~# traceroute 147.160.176.65
traceroute to 147.160.176.65 (147.160.176.65), 30 hops max, 60 bytes
 1 gateway.xa.example.com (192.168.1.1)  0.675 ms  0.490 ms  0.3
 2 180.8.126.202 (180.8.126.202)  4.065 ms  153.128.214.26 (153.1
 23 ms 180.8.126.162 (180.8.126.162)  4.462 ms
 3 180.8.126.201 (180.8.126.201)  3.591 ms  7.864 ms  180.8.126.15
 69) 4.453 ms
 4 218.43.253.194 (218.43.253.194)  4.345 ms  4.174 ms  5.159 ms
 5 27.86.45.1 (27.86.45.1)  5.719 ms  27.85.228.37 (27.85.228.37)
 6.120.9 (27.86.120.9)  6.461 ms
 6 106.139.193.21 (106.139.193.21)  5.209 ms  27.86.46.89 (27.86.46.
 5 27.85.227.121 (27.85.227.121)  5.536 ms
 7 oteJIN301.int-gw.kddi.ne.jp (27.86.32.2)  4.229 ms  4.615 ms  4.5
 8 111.108.2.206 (111.108.2.206)  4.576 ms  4.365 ms  4.397 ms
 9 * * *
10 147.160.176.46 (147.160.176.46)  4.456 ms  147.160.176.22 (147.160.

```

```

15 ms *
147.160.176.33 (147.160.176.33)  6.040 ms *  5.780 ms
* 147.160.176.40 (147.160.176.40)  4.969 ms *
3 * 147.160.176.33 (147.160.176.33)  4.920 ms *
4 147.160.176.45 (147.160.176.45)  4.668 ms * 147.160.176.47
9.555 ms
25 147.160.176.1 (147.160.176.1)  5.583 ms  147.160.176.33 (147
18 ms 4.876 ms
26 * 147.160.176.50 (147.160.176.50)  4.535 ms *
27 147.160.176.33 (147.160.176.33)  4.963 ms * 4.817 ms
28 * * *
29 * * *
30 147.160.176.52 (147.160.176.52)  4.692 ms * 147.160.176.51 (14
5.131 ms
root@raspberrypi:~#

```

```

#
NetRange: 147.160.176.0 - 147.160.191.255
CIDR: 147.160.176.0/20
NetName: BYTED
NetHandle: NET-147-160-176-0-1
Parent: NET147 (NET-147-0-0-0-0)
NetType: Direct Allocation
OriginAS:
Organization: Bytedance Inc. (BYTED)
RegDate: 2019-06-27
Updated: 2019-06-27
Ref: https://rdap.arin.net/registry/ip/147.160.176.0

OrgName: Bytedance Inc.
OrgId: BYTED
Address: 3000 El Camino Real Building 2 Suite 400
City: Palo Alto
StateProv: CA
PostalCode: 94306
Country: US

```

OCNからTracerouteしたら、大手町でKDDIさんに飛び込んですぐ直後にByteDance社のアドレス帯に入ります
 RTTが5msしかない、ってことは、物理的には都内にあると推察できます
 # 途中のIPアドレスとのRTTとほとんど差がないことからわかります

すなわちByteDance社は都内にもサーバーを置いている可能性が高いですね

そこから先はわかりません

というわけで今回TikTokをみてみたのですが

今回調べてみたときにわかった通信先は

Google (認証など?)

Akamai (どうやら動画をCDNで流しているみたい)

ByteDance (TikTokの会社)

のようです。

ByteDance社は、シリコンバレーのPalo Altoに住所をもってそこがアドレスの登録地になっていますが、TracerouteするとKDDIさんやSoftBankさんの直近にサーバーがあるようで、RTTからみると国内に通信先をもっているとおもわれます

ByteDance社の「なか」がどうなってるかはわかりませんが、TikTokアプリが直接外国と通信している様子はありませんでした。

また、ほとんどの通信がQUICになっていて暗号化されているため何を通信しているのかは簡単にうかがいすることはできませんでした

いったんまとめ

今回は、Raspberry Pi を無線LANルーターにして、パケットを見る手順をまとめてみました
Wiresharkのさらなる使い方については、調べてみていただければ幸いです

この機材があればいろいろなアプリやIoT機器などがどのような通信をしているかを調査することができます

QUICの中身を解析するには末端のアプリ側のコード解析などが必要になりますので、OSSでないかぎり、非常に難しいです。逆アセンブルしないといけませんからね。

そこから先はまた別のお話というわけで。

今回はいったんここまでとさせていただきます

**ご清聴ありがとうございました
とおもいきや。。。おまけ**

Raspberry Pi OSがよくできてるわけですよ

今回調査してみてよくわかったのですが、

Ubuntu は、いろいろと入っていて逆にルーターにしにくい

Debianは、ちゃんとNetwork Managerの使い方を勉強すれば非常につかやすい。GUI抜きでもいけるので、組み込みルーターにするには最適ではないかとおもわれる

ですが、今回Raspberry Pi OSがとても使いやすいのがわかりまして。コレ、Debianをもとにしているのですが、

このRaspberry Pi OSが、普通のノートPCでうごけばいいのになあ。。。っておもったら、

ああ、ありますね。PC用。

でもさ。Raspberry Pi だと持ち運べないしなあ。。

Raspberry Pi とってもいいんだけど、持ち運びはちょっと難しいんですよね
意外と電源容量使うので、携帯電話用のモバイルバッテリーだと足りないし
画面とキーボードとマウスもつけるので、手軽にちょこちょこっていうわけにはいかない

[Best Raspberry Pi Laptop in 2023 \(pcguide.com\)](https://www.pcguidance.com/raspberry-pi-laptop/)

Raspberry Pi Laptop っていうのも確かにあるんですけどね(´▽`)

あるやん。PC用（あとMacも）のOS

[Raspberry Pi Desktop for PC and Mac – Raspberry Pi](https://www.raspberrypi.com/software/raspberry-pi-desktop/)

<https://www.raspberrypi.com/software/raspberry-pi-desktop/>

Raspberry Pi Desktop for PC and Mac

Debian with Raspberry Pi Desktop is our operating system for PC and Mac. It provides the Raspberry Pi OS desktop, as well as most of the recommended software that comes with Raspberry Pi OS, for any PC or Apple Mac computer.

じゃあ、ちょっと古いのとか中古のノートPCでよくね？



ノートPCでやれば

電源の問題なし

ディスプレイとキーボード、マウスもついてる

WiFiインターフェースもある！

Ethernetもある！

ネットワーク遊びするにはこっちのほうがいろいろといいんじゃないかしら

どうせやるなら携帯電話のインターフェースが欲しい



ノートPCにSIM刺せるやつありますよね

携帯電話モデムがついてるやつ

あれをうまくやると、携帯電話回線を「上流」にすることもできるんじゃない??

ええ。できちゃうんですよね。。。

でもそのやり方については今回は時間切れ。またの機会とさせていただければ幸いです





ご清聴ありがとうございました