DronePwn101

Presented by Andy Doering

Goals:

1_Educate on the fundamentals of drone technology to include signal types, channel features, sensor features, hardware, open source VS proprietary protocols and API.

2_Educate on the basic methodology utilized with exploiting any given UAV

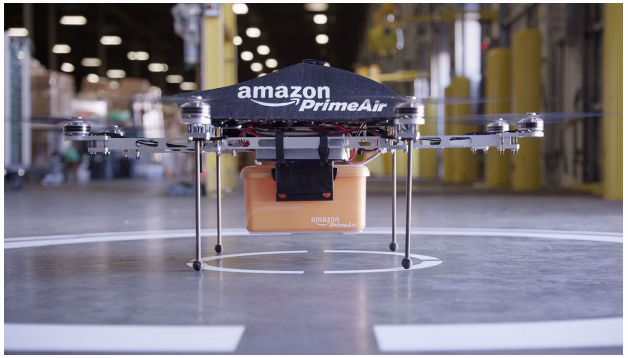
3_Educate on the basics of configuring microcomputers for signal survey and exploitation

4_Expanding on the Existing Technology

5_Demonstrate how to replicate the above technology and features to create a personal unmanned vehicle capable of remote survey and exploitation, and interception.

Drones...

==========



The Technology:

The Basics:

Drones (on average) emit 2 signals

- 2.4GHz = Connections between ground transmitter and the vehicle
- 5.8 GHz = FPV link
- Average connection distance ~ 1000 meters (dB strength variable)

Drone Controller normally has a wifi connection that you connect to via an app
This app handles the transfer of information (sometimes proprietary protocol)

Higher end consumer drones also feature a myriad of on board sensors:

- Altimeter - Altitude
- Pressure Sensor - Improved stability (hovering)
- Accelerometer - detects acceleration
- Magnetometer - compass
- Gyroscope - Detects orientation based off of a static spin axis.

2.4GHz

The frequency most quads use for the connection between the ground transmitter and vehicle (also the frequency that computer wireless networks operate on).

Lower frequency means better penetration for the waves.

The drone receives the signal from the controller, which dictates its movement to the servo motors (each channel in the signal controls a specific function on the drone). The minimum required to pilot a multi-rotor is four channels: throttle (Alti-tutde), yaw (rotation / left or right), pitch (pointed up or down), and roll.

For every flight mode switch, gimbal control, or lighting control, an extra channel is involved. Most flight controllers are going to recommend minimum eight channels.

Each channel has a pinout that is connected to a servo cable.

5.8GHz

Channel used for FPV

Smaller band for more information

Analog video is real-time and requires no image compression and advanced processing (digital is possible but not used due to latency. Recordings and image captures however are 1080p)

Near zero latency between the image captured by the camera and the one viewed by the pilot.

The Protocols:

PWM - Pulse Width Modulation
- Original, older and not used much anymore
- One channel for each Servo
- Analog 1-to-1 broadcast

PCM - Pulse Code Modulation
- Digital
- Can detect signals and correct errors
- PCM is more reliable and less susceptible to interference
- Tends to be more expensive

PPM - Pulse-Position Modulation
- Analog
- Multiple inputs are encoded and transmitted using a single channel
- One signal wire for max of 8 channels

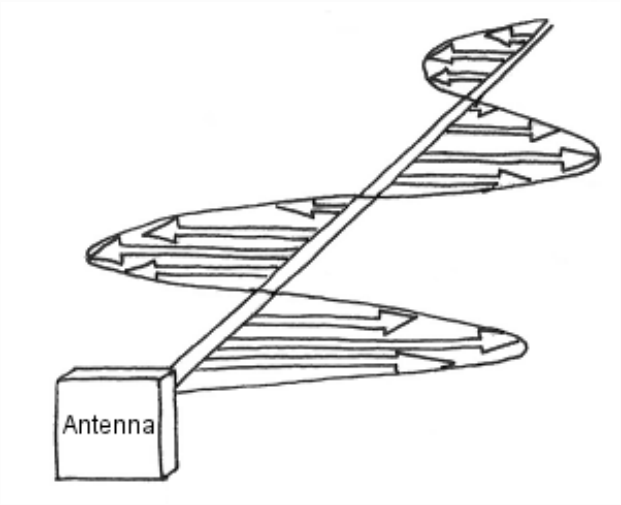
UHF - Ultra High Frequency
- Operate across a range of frequencies
- Uses channel hopping to maintain a strong link for as long as possible.
- Considered a standard for long range applications

Polarization:

==========

Linear
- Single signal formed on a singular plane.
- Can provide extra range as all the energy is focused on a single plane
- Need to ensure that both antennas are aligned to ensure max overlap
- Wifi will typically use linear antennas since the devices are stationary

- Subject to multipath interference: happens when the signal is reflected from object and gets distorted with phase delay, and it interferes with the main signal.

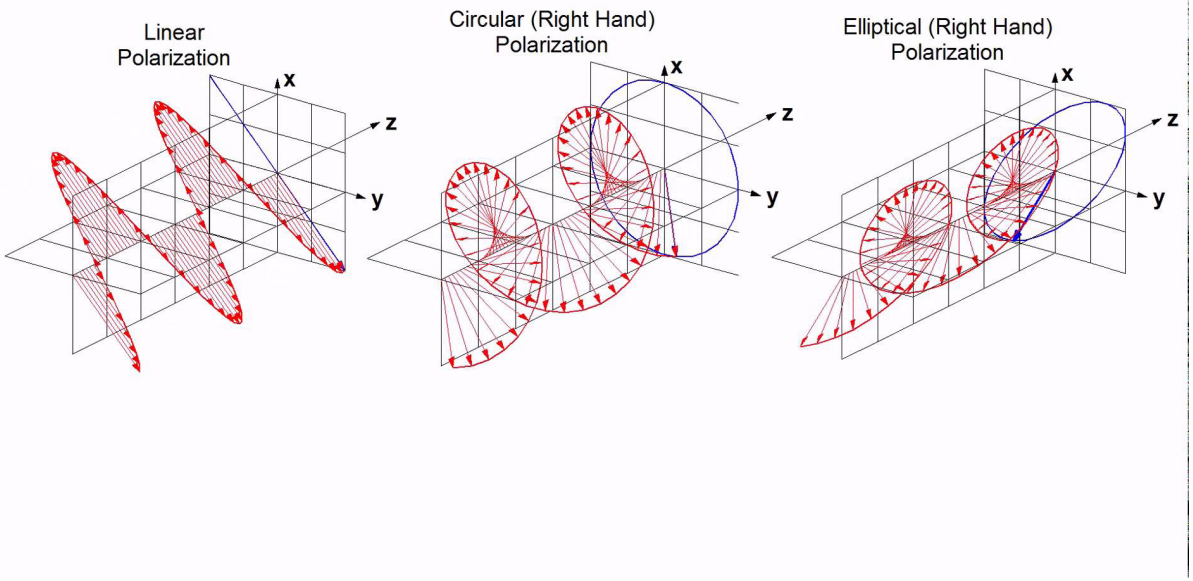


Polarization:

==========

Circular

- Signals are transmitted on both horizontal and vertical planes with a 90 degree phase shift. End result looks like a spinning corkscrew.
- Due to pattern you always get good overlap no matter what angle you are flying at
- Signals always overlap (great coverage)
- Rejects multipath interference
- Left-hand (LHCP) or right-hand (RHCP) / direction the corkscrew spins

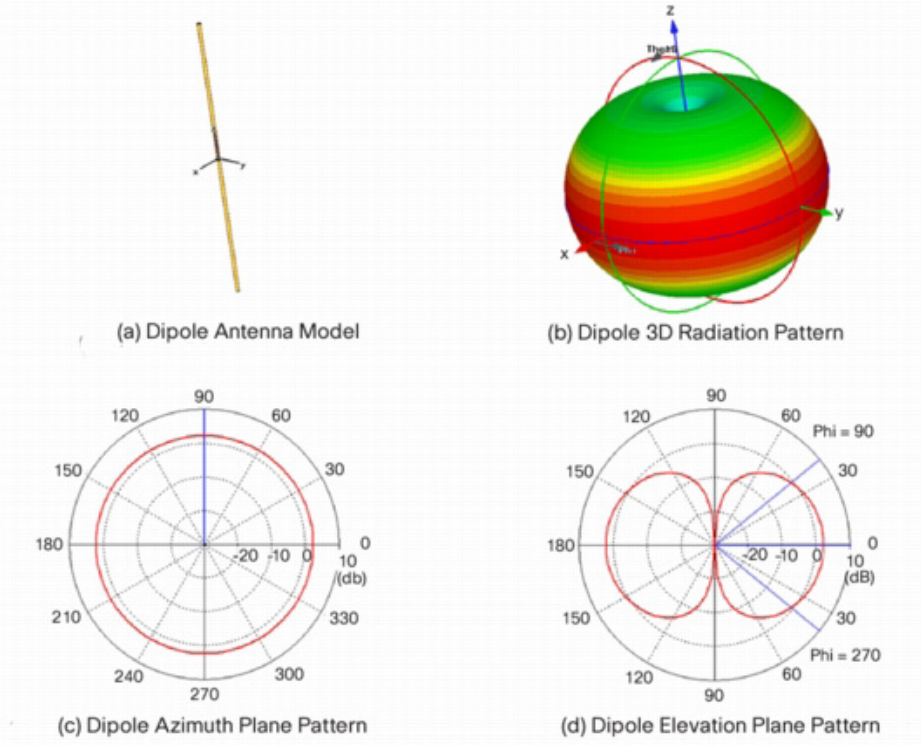


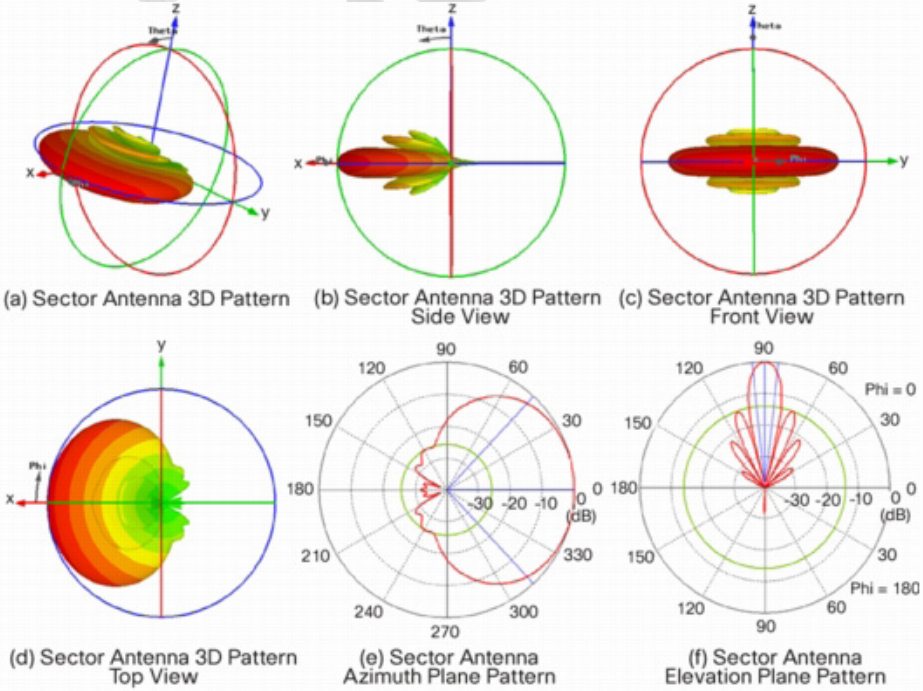
Antennas:

==========

<u>Omnidirectional (dipole)</u>
Think lightbulb / donut shape
Emit signal in all directions
More coverage but reduced range

<u>Directional</u>
Think flashlight / cone
Emits signal in one targeted direction
More range but reduced coverage

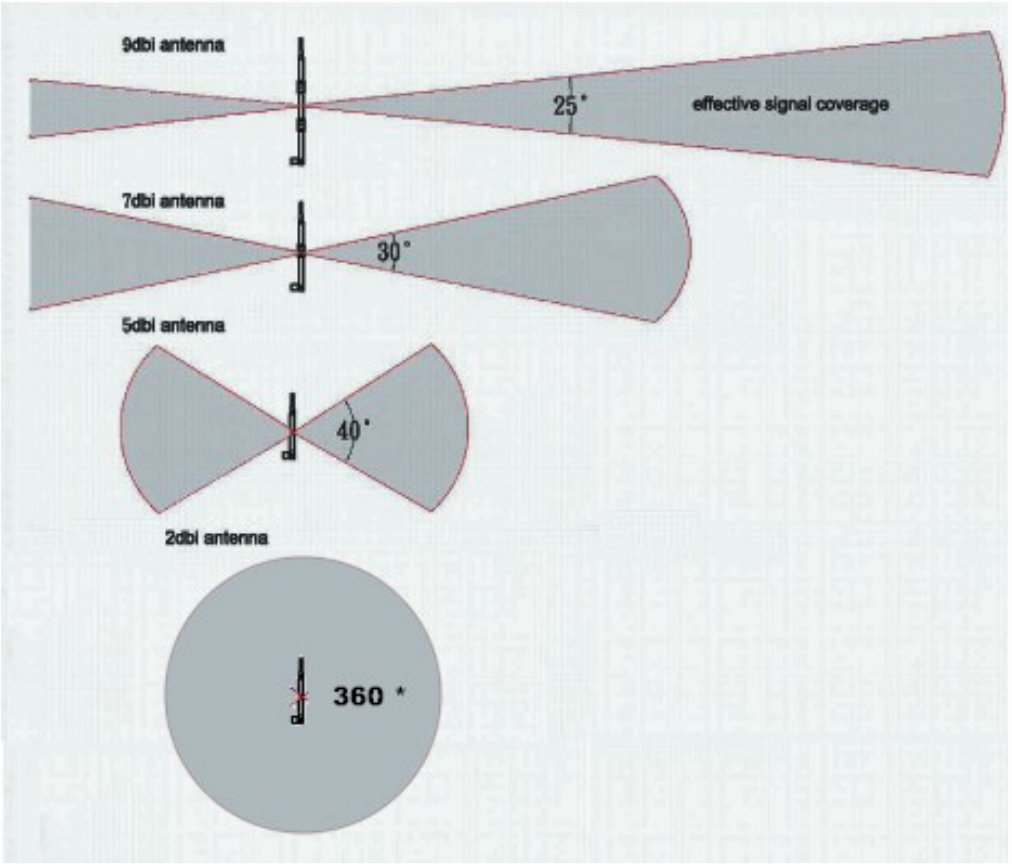


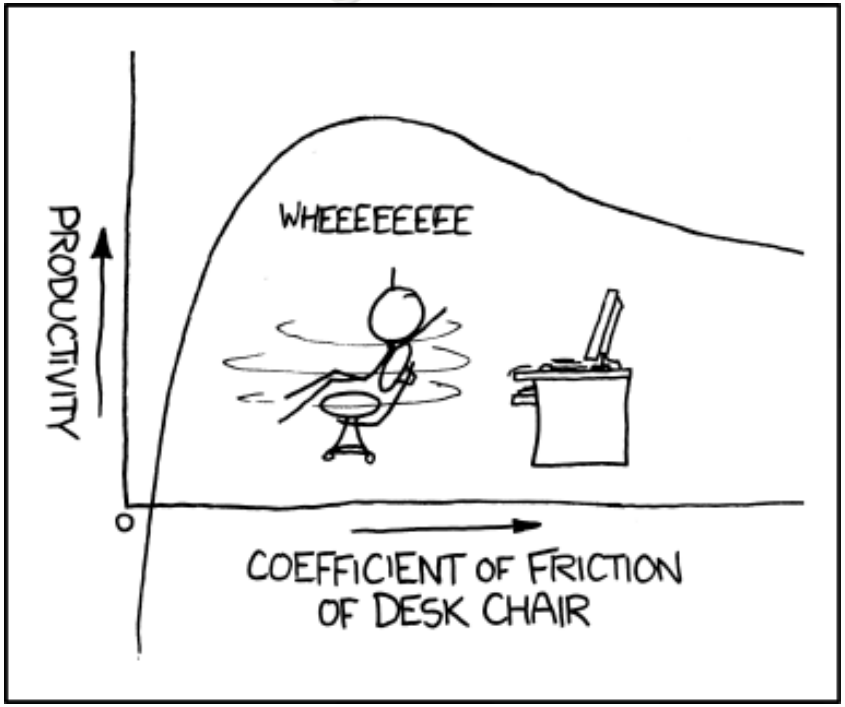


Gain:

==========

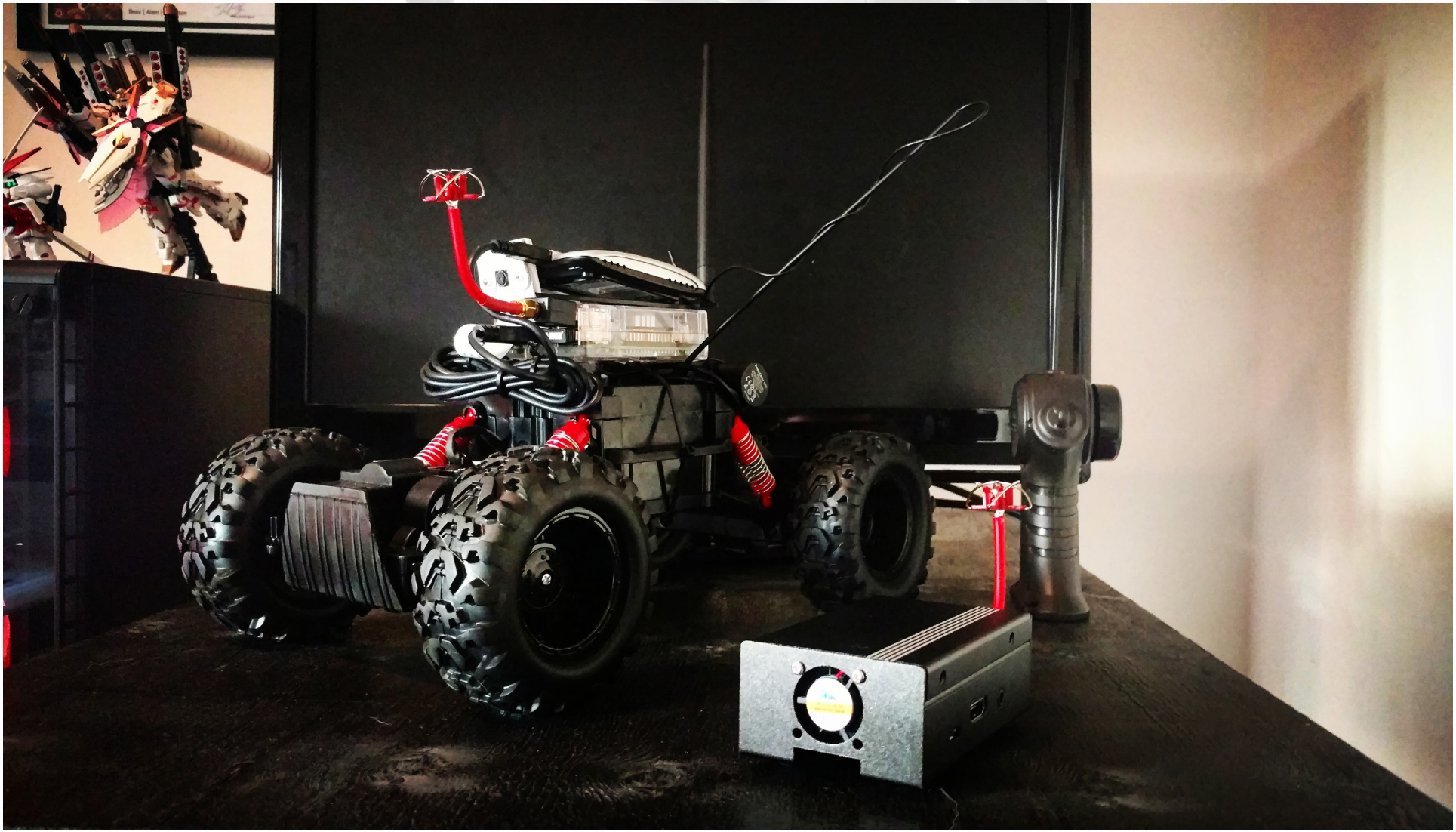
The measure of power of an antenna or transmitter
Measured in decibels (dB)
0db looks like a perfect circle
Increasing the gain will alter the shape of the circle





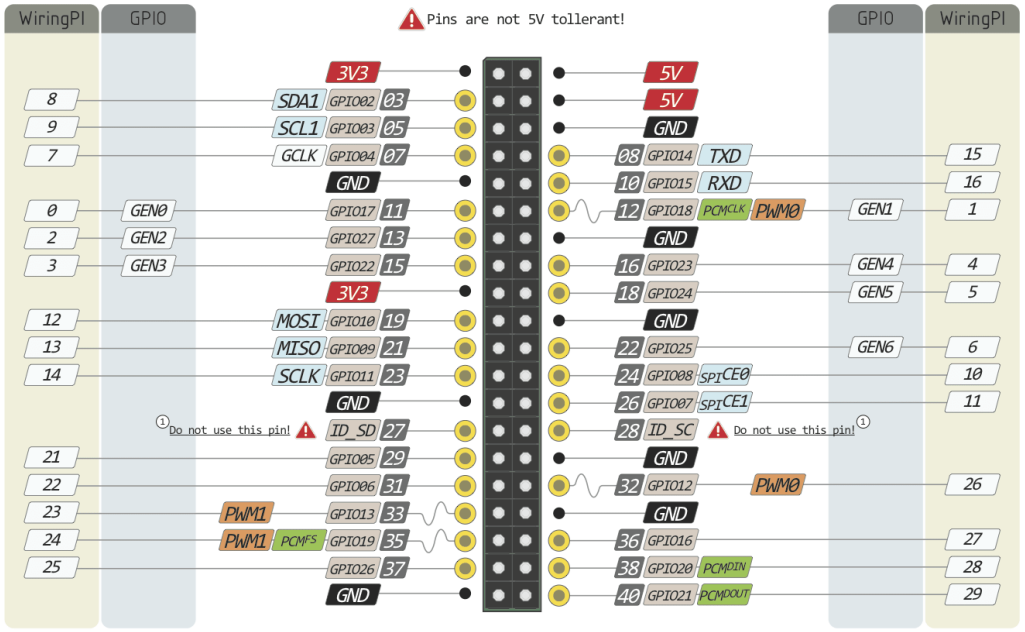
The Build:

==========



RPi pinout

v2 Model B



Legend

- Power
- GND
- Serial Pin
- PCM Audio
- PWM
- IO Pin
- Physical Pin
- Port Name
- PWM Pin

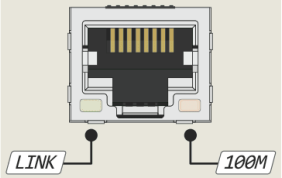
① These pins are reserved for ID EEPROM

At boot time this I2C interface will be interrogated to look for an EEPROM that identifies the attached board and allow automagic setup of the GPIOs (and optionally, Linux drivers).

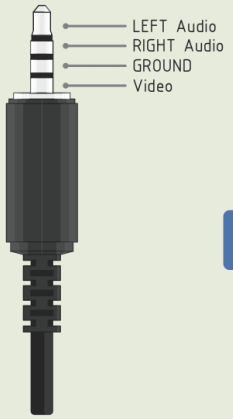
DO NOT USE these pins for anithing other than attaching an I2C ID EEPROM. Leave unconnected if ID EEPROM not required.

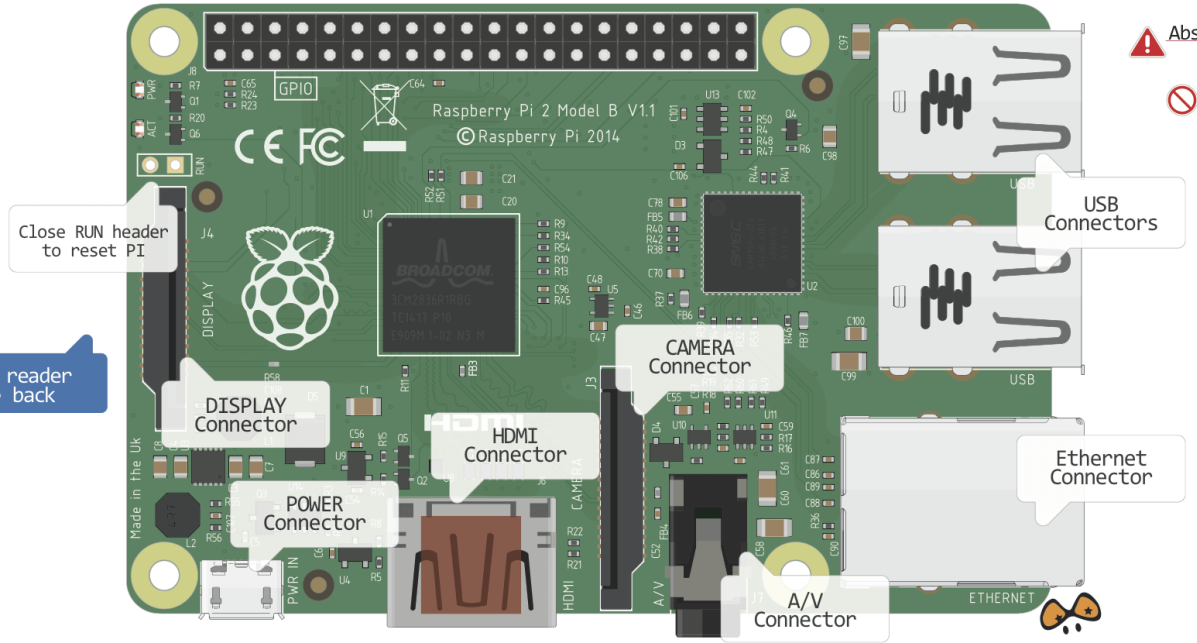
⚠ The PWM pin available on the GPIO header is shared with the Audio system

ETHERNET Connector



AUDIO/VIDEO Connector



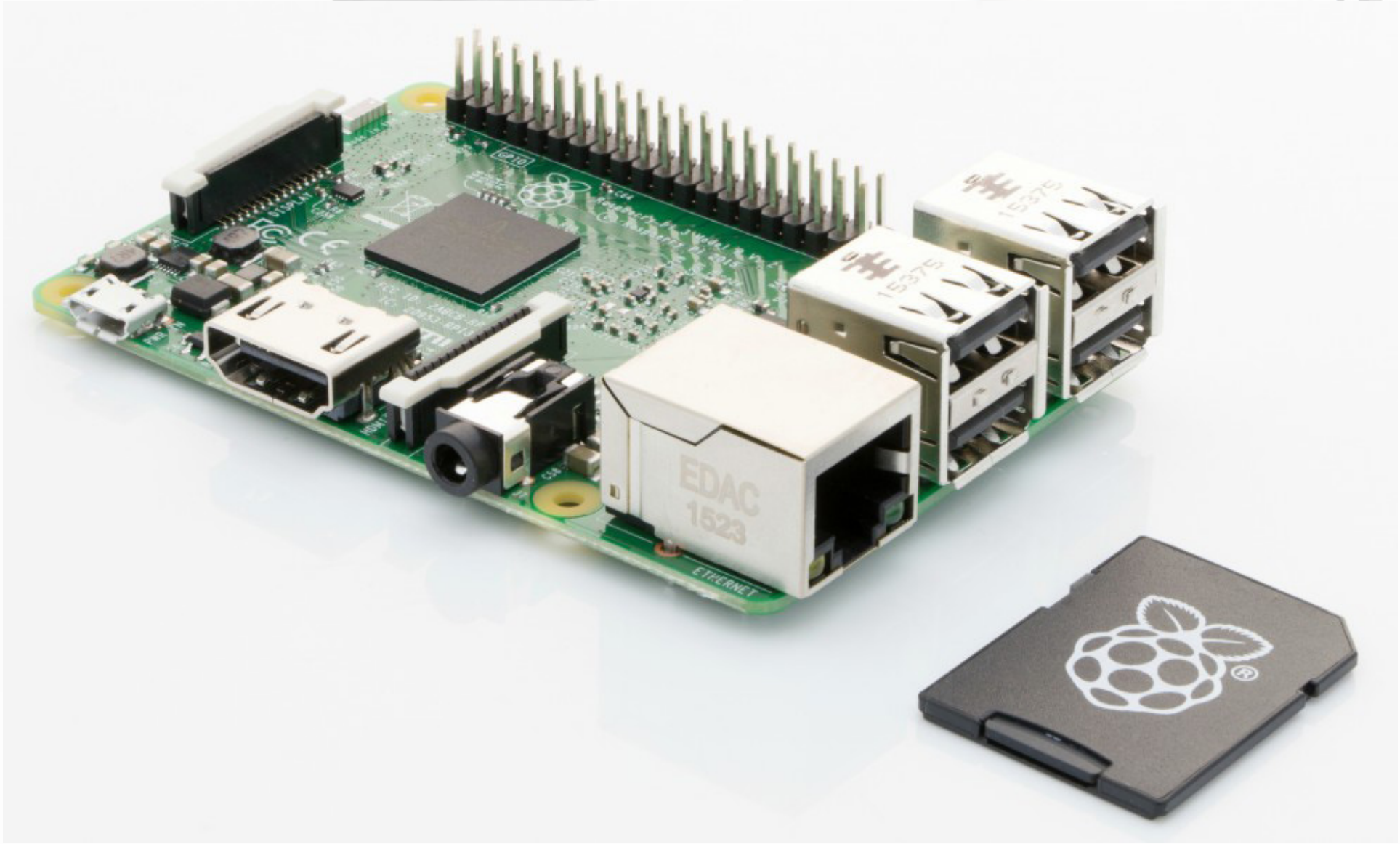


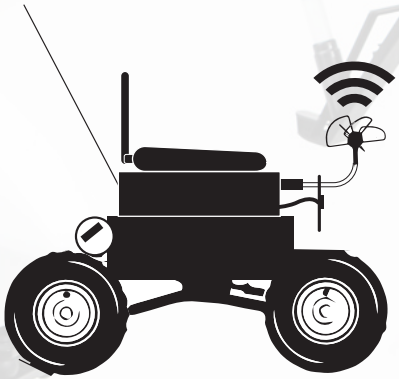
⚠ Absolute MAX per pin 16mA recommended 8mA

🚫 Absolute MAX 50mA for entire package

bq
www.bq.com

25 JUN 2015
ver 1 rev 0


EDAC
1523
ETHERNET



Pi 1
DHCP / Authentication server (hostapd) and iptables.
These act as a wireless access point (with WPA2 authentication)

This Pi is facilitates your connection to the drone by acting as the intermediary between you and the drone

This modular build allows for a multitude of device capabilities including running Kali and Tor on the pi. Alternate builds could include an antenna directly plugged into the laptop, as well as control of the vehicle via ArduPilot and additional hardware

Pi 2
Hosts apache web server and runs Rpi-Cam-Web-Interface which runs as a client to RaspiMJPEG

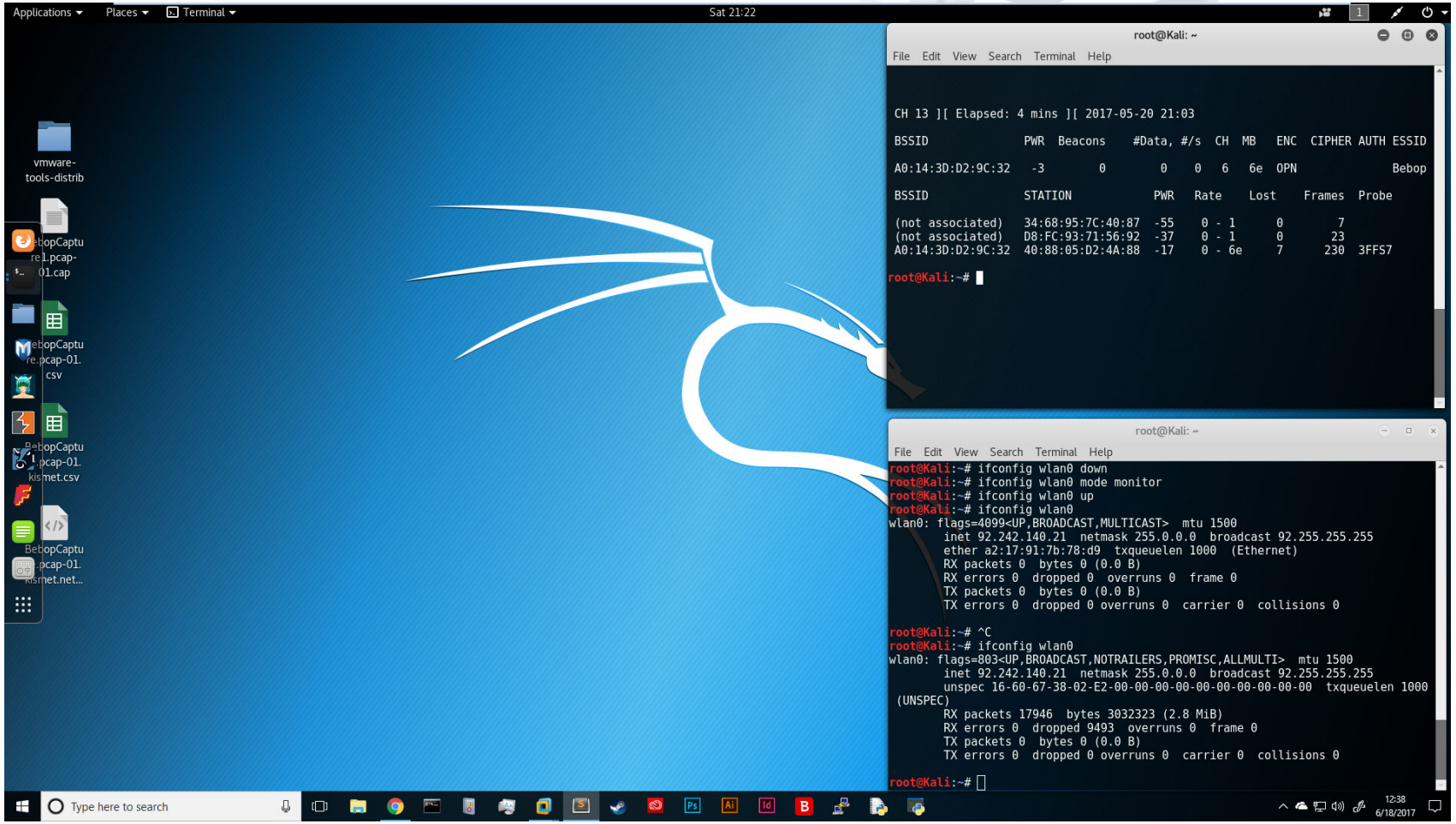
Facilitate live video streams to an HTML page (offering extreme flexibility in viewing platform)

DHCP / Authentication server (hostapd) and iptables.

ALFA AWUS036H Antenna

Exploring the filesystem:

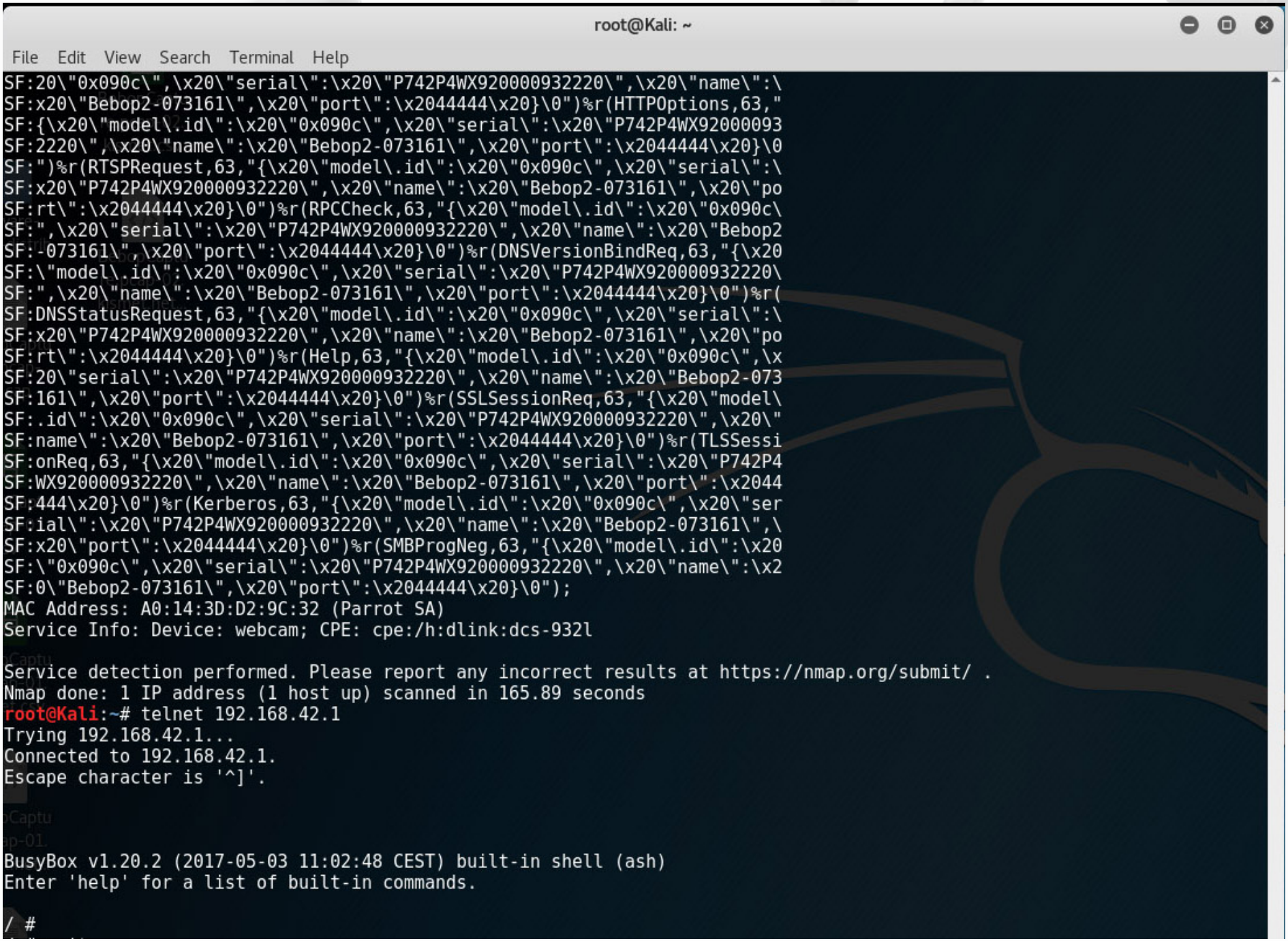
==========

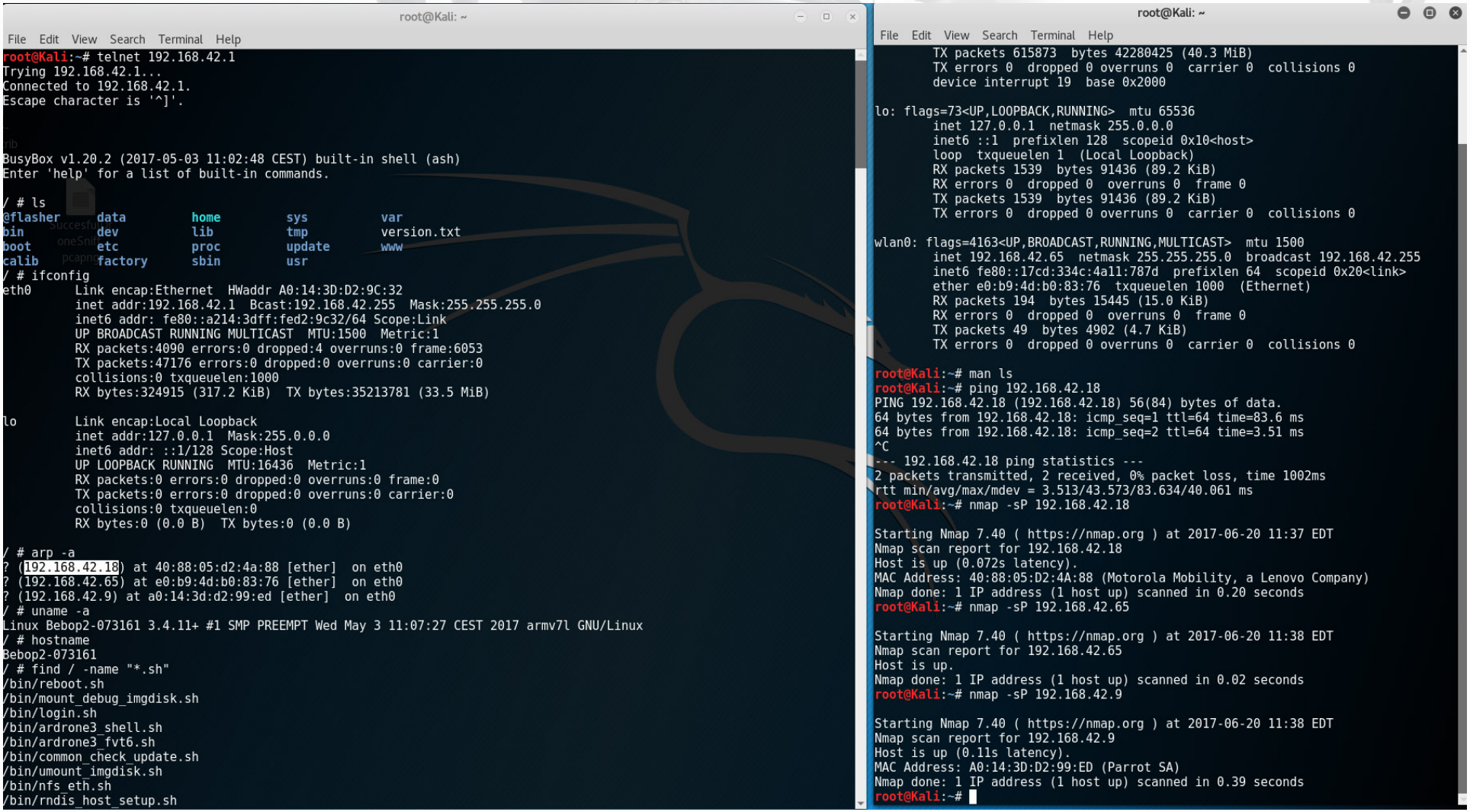


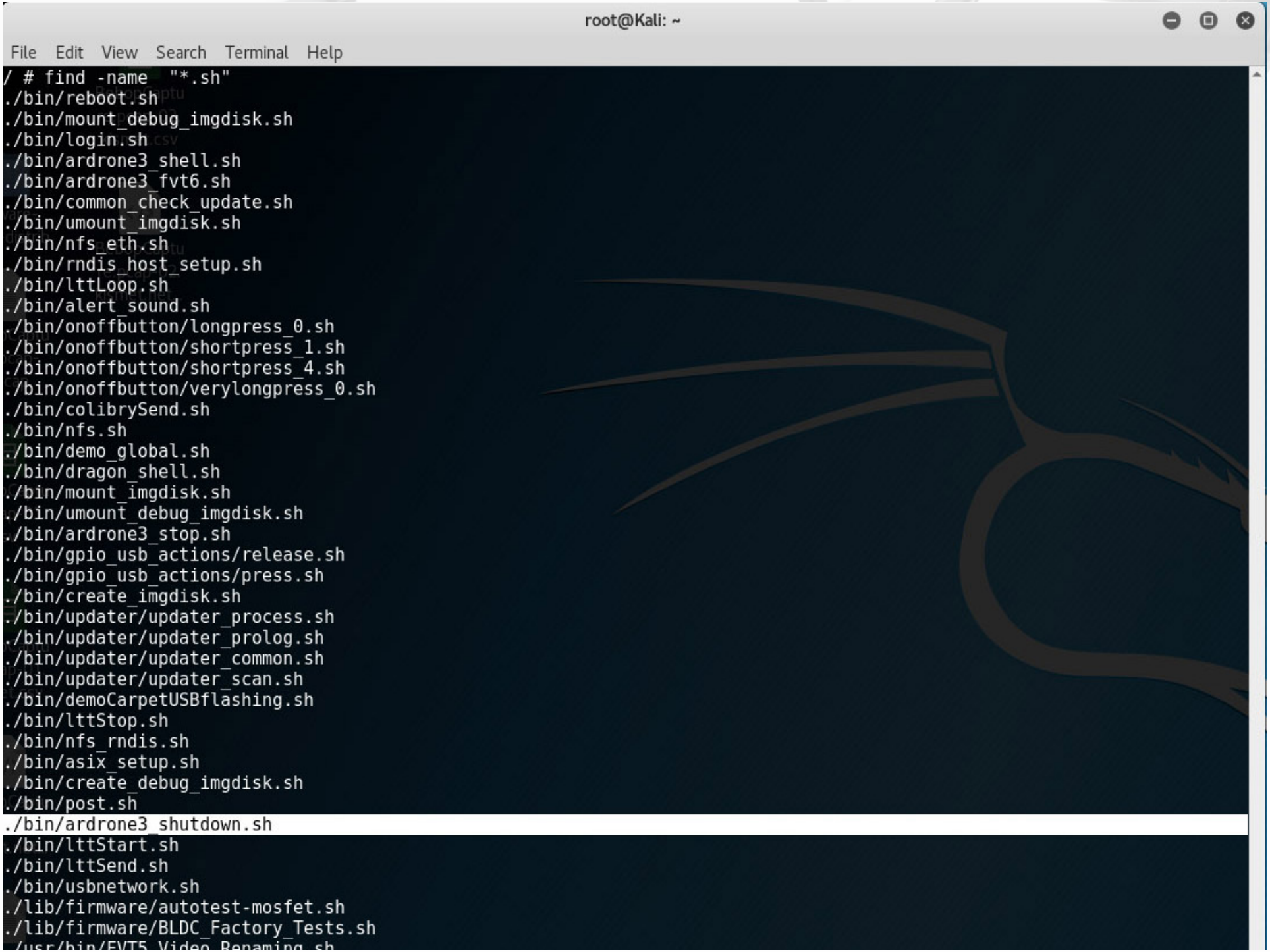
root@Kali: ~

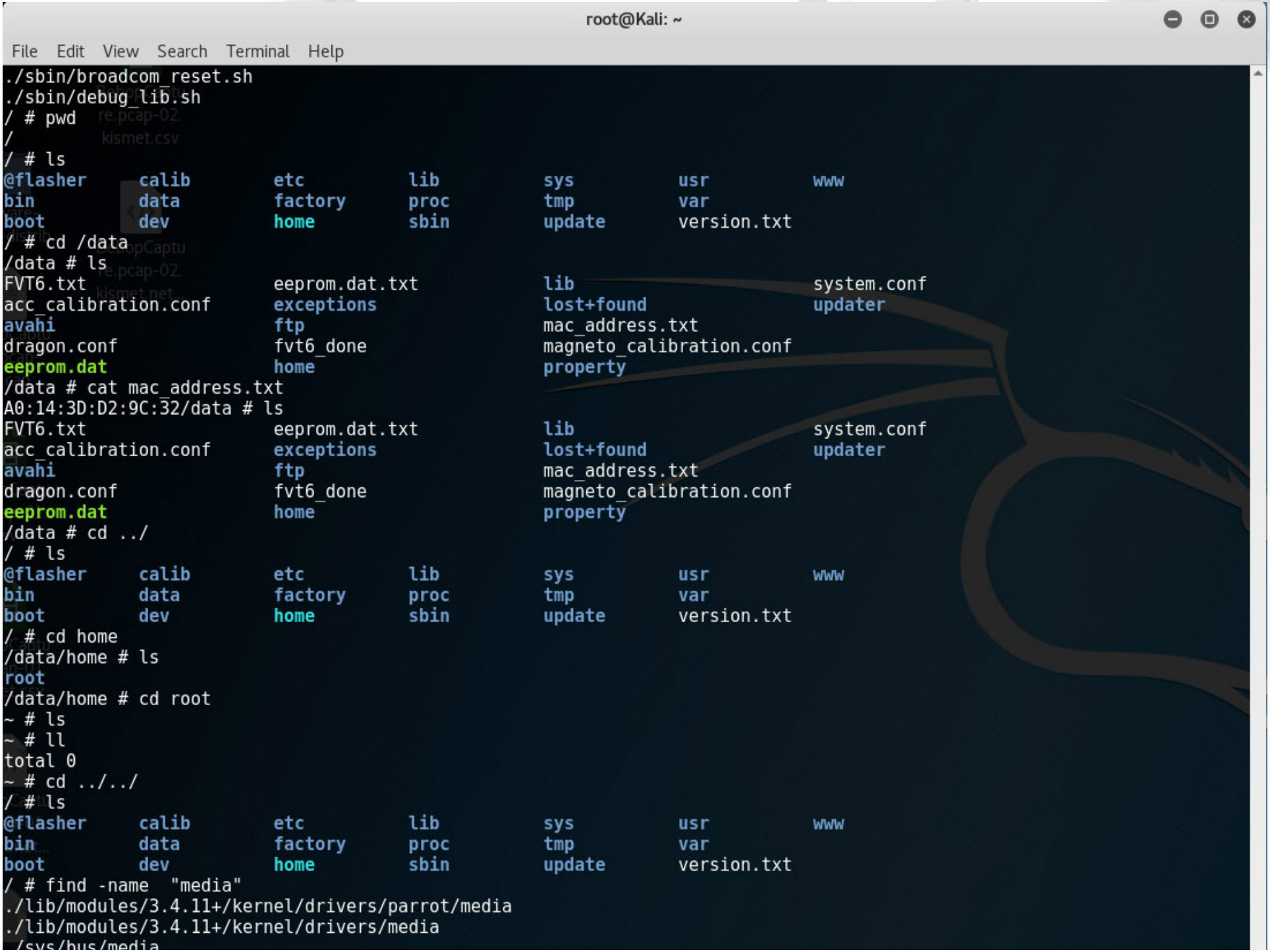
File Edit View Search Terminal Help

```
Host is up (0.019s latency).
Not shown: 65528 closed ports
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              BusyBox ftpd (D-Link DCS-932L IP-Cam camera)
23/tcp    open  telnet
51/tcp    open  ftp              BusyBox ftpd (D-Link DCS-932L IP-Cam camera)
61/tcp    open  ftp              BusyBox ftpd (D-Link DCS-932L IP-Cam camera)
9050/tcp  open  tor-socks?
44444/tcp open  cognex-dataman?
44445/tcp open  unknown
3 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprint
s at https://nmap.org/cgi-bin/submit.cgi?new-service :
```


root@Kali: ~
File Edit View Search Terminal Help
SF:20\"0x090c\",\x20\"serial\":\x20\"P742P4WX920000932220\",\x20\"name\":\
SF:x20\"Bebop2-073161\",\x20\"port\":\x2044444\x20}\0")%r(HTTPOptions,63,"
SF:{\x20\"model\.id\":\x20\"0x090c\",\x20\"serial\":\x20\"P742P4WX92000093
SF:2220\",\x20\"name\":\x20\"Bebop2-073161\",\x20\"port\":\x2044444\x20}\0
SF:")%r(RTSPRequest,63,"{\x20\"model\.id\":\x20\"0x090c\",\x20\"serial\":\
SF:x20\"P742P4WX920000932220\",\x20\"name\":\x20\"Bebop2-073161\",\x20\"po
SF:rt\":\x2044444\x20}\0")%r(RPCCheck,63,"{\x20\"model\.id\":\x20\"0x090c\
SF:",\x20\"serial\":\x20\"P742P4WX920000932220\",\x20\"name\":\x20\"Bebop2
SF:-073161\",\x20\"port\":\x2044444\x20}\0")%r(DNSVersionBindReq,63,"{\x20
SF:\"model\.id\":\x20\"0x090c\",\x20\"serial\":\x20\"P742P4WX920000932220\
SF:",\x20\"name\":\x20\"Bebop2-073161\",\x20\"port\":\x2044444\x20}\0")%r(
SF:DNSStatusRequest,63,"{\x20\"model\.id\":\x20\"0x090c\",\x20\"serial\":\
SF:x20\"P742P4WX920000932220\",\x20\"name\":\x20\"Bebop2-073161\",\x20\"po
SF:rt\":\x2044444\x20}\0")%r(Help,63,"{\x20\"model\.id\":\x20\"0x090c\",\x
SF:20\"serial\":\x20\"P742P4WX920000932220\",\x20\"name\":\x20\"Bebop2-073
SF:161\",\x20\"port\":\x2044444\x20}\0")%r(SSLSessionReq,63,"{\x20\"model\
SF:.id\":\x20\"0x090c\",\x20\"serial\":\x20\"P742P4WX920000932220\",\x20\"
SF:name\":\x20\"Bebop2-073161\",\x20\"port\":\x2044444\x20}\0")%r(TLSSessi
SF:onReq,63,"{\x20\"model\.id\":\x20\"0x090c\",\x20\"serial\":\x20\"P742P4
SF:WX920000932220\",\x20\"name\":\x20\"Bebop2-073161\",\x20\"port\":\x2044
SF:444\x20}\0")%r(Kerberos,63,"{\x20\"model\.id\":\x20\"0x090c\",\x20\"ser
SF:ial\":\x20\"P742P4WX920000932220\",\x20\"name\":\x20\"Bebop2-073161\",\
SF:x20\"port\":\x2044444\x20}\0")%r(SMBProgNeg,63,"{\x20\"model\.id\":\x20
SF:\"0x090c\",\x20\"serial\":\x20\"P742P4WX920000932220\",\x20\"name\":\x2
SF:0\"Bebop2-073161\",\x20\"port\":\x2044444\x20}\0");
MAC Address: A0:14:3D:D2:9C:32 (Parrot SA)
Service Info: Device: webcam; CPE: cpe:/h:dlink:dcs-932l
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 165.89 seconds
root@Kali:~# telnet 192.168.42.1
Trying 192.168.42.1...
Connected to 192.168.42.1.
Escape character is '^]'.
BusyBox v1.20.2 (2017-05-03 11:02:48 CEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
/ #


root@Kali: ~
File Edit View Search Terminal Help
root@Kali:~# telnet 192.168.42.1
Trying 192.168.42.1...
Connected to 192.168.42.1.
Escape character is '^]'.
BusyBox v1.20.2 (2017-05-03 11:02:48 CEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.
/ # ls
@flasher data home sys var
bin dev lib tmp version.txt
boot etc proc update www
calib factory sbin usr
/ # ifconfig
eth0 Link encap:Ethernet HWaddr A0:14:3D:D2:9C:32
inet addr:192.168.42.1 Bcast:192.168.42.255 Mask:255.255.255.0
inet6 addr: fe80::a214:3dff:fed2:9c32/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:4090 errors:0 dropped:4 overruns:0 frame:6053
TX packets:47176 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:324915 (317.2 KiB) TX bytes:35213781 (33.5 MiB)
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
/ # arp -a
? (192.168.42.18) at 40:88:05:d2:4a:88 [ether] on eth0
? (192.168.42.65) at e0:b9:4d:b0:83:76 [ether] on eth0
? (192.168.42.9) at a0:14:3d:d2:99:ed [ether] on eth0
/ # uname -a
Linux Bebop2-073161 3.4.11+ #1 SMP PREEMPT Wed May 3 11:07:27 CEST 2017 armv7l GNU/Linux
/ # hostname
Bebop2-073161
/ # find / -name "*.sh"
/bin/reboot.sh
/bin/mount_debug_imgdisk.sh
/bin/login.sh
/bin/ardrone3_shell.sh
/bin/ardrone3_fvt6.sh
/bin/common_check_update.sh
/bin/umount_imgdisk.sh
/bin/nfs_eth.sh
/bin/rndis_host_setup.sh
root@Kali: ~
File Edit View Search Terminal Help
TX packets 615873 bytes 42280425 (40.3 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
device interrupt 19 base 0x2000
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1 (Local Loopback)
RX packets 1539 bytes 91436 (89.2 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1539 bytes 91436 (89.2 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 192.168.42.65 netmask 255.255.255.0 broadcast 192.168.42.255
inet6 fe80::17cd:334c:4a11:787d prefixlen 64 scopeid 0x20<link>
ether e0:b9:4d:b0:83:76 txqueuelen 1000 (Ethernet)
RX packets 194 bytes 15445 (15.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 49 bytes 4902 (4.7 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
root@Kali:~# man ls
root@Kali:~# ping 192.168.42.18
PING 192.168.42.18 (192.168.42.18) 56(84) bytes of data.
64 bytes from 192.168.42.18: icmp_seq=1 ttl=64 time=83.6 ms
64 bytes from 192.168.42.18: icmp_seq=2 ttl=64 time=3.51 ms
^C
--- 192.168.42.18 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 3.513/43.573/83.634/40.061 ms
root@Kali:~# nmap -sP 192.168.42.18
Starting Nmap 7.40 (https://nmap.org) at 2017-06-20 11:37 EDT
Nmap scan report for 192.168.42.18
Host is up (0.072s latency).
MAC Address: 40:88:05:D2:4A:88 (Motorola Mobility, a Lenovo Company)
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@Kali:~# nmap -sP 192.168.42.65
Starting Nmap 7.40 (https://nmap.org) at 2017-06-20 11:38 EDT
Nmap scan report for 192.168.42.65
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
root@Kali:~# nmap -sP 192.168.42.9
Starting Nmap 7.40 (https://nmap.org) at 2017-06-20 11:38 EDT
Nmap scan report for 192.168.42.9
Host is up (0.11s latency).
MAC Address: A0:14:3D:D2:99:ED (Parrot SA)
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
root@Kali:~#


root@Kali: ~
File Edit View Search Terminal Help
/ # find -name "*.sh"
./bin/reboot.sh
./bin/mount_debug_imgdisk.sh
./bin/login.sh
./bin/ardrone3_shell.sh
./bin/ardrone3_fvt6.sh
./bin/common_check_update.sh
./bin/umount_imgdisk.sh
./bin/nfs_eth.sh
./bin/rndis_host_setup.sh
./bin/lttLoop.sh
./bin/alert_sound.sh
./bin/onoffbutton/longpress_0.sh
./bin/onoffbutton/shortpress_1.sh
./bin/onoffbutton/shortpress_4.sh
./bin/onoffbutton/verylongpress_0.sh
./bin/colibrySend.sh
./bin/nfs.sh
./bin/demo_global.sh
./bin/dragon_shell.sh
./bin/mount_imgdisk.sh
./bin/umount_debug_imgdisk.sh
./bin/ardrone3_stop.sh
./bin/gpio_usb_actions/release.sh
./bin/gpio_usb_actions/press.sh
./bin/create_imgdisk.sh
./bin/updater/updater_process.sh
./bin/updater/updater_prolog.sh
./bin/updater/updater_common.sh
./bin/updater/updater_scan.sh
./bin/demoCarpetUSBflashing.sh
./bin/lttStop.sh
./bin/nfs_rndis.sh
./bin/asix_setup.sh
./bin/create_debug_imgdisk.sh
./bin/post.sh
./bin/ardrone3_shutdown.sh
./bin/lttStart.sh
./bin/lttSend.sh
./bin/usbnetwork.sh
./lib/firmware/autotest-mosfet.sh
./lib/firmware/BLDC_Factory_Tests.sh

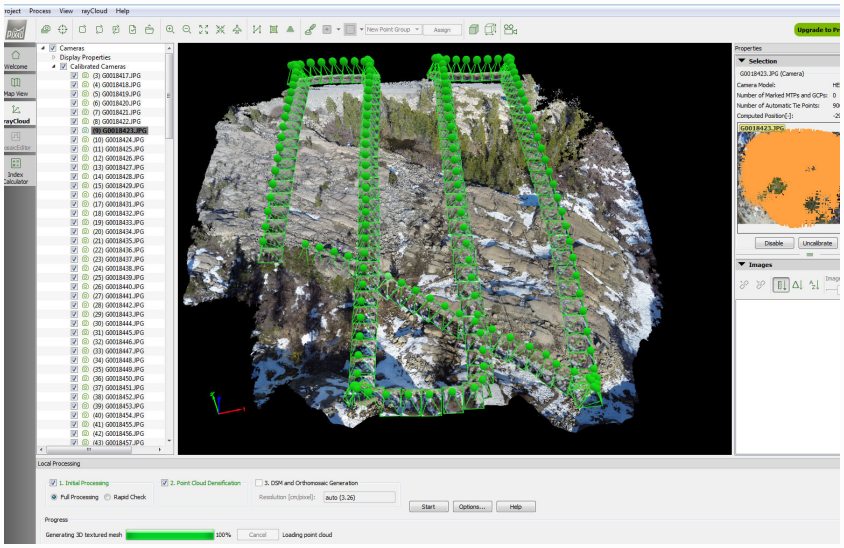

root@Kali: ~
File Edit View Search Terminal Help
./sbin/broadcom_reset.sh
./sbin/debug_lib.sh
/ # pwd
/
/ # ls
@flasher calib etc lib sys usr www
bin data factory proc tmp var
boot dev home sbin update version.txt
/ # cd /data
/data # ls
FVT6.txt eeprom.dat.txt lib system.conf
acc_calibration.conf exceptions lost+found updater
avahi ftp mac_address.txt
dragon.conf fvt6_done magneto_calibration.conf
eeprom.dat home property
/data # cat mac_address.txt
A0:14:3D:D2:9C:32/data # ls
FVT6.txt eeprom.dat.txt lib system.conf
acc_calibration.conf exceptions lost+found updater
avahi ftp mac_address.txt
dragon.conf fvt6_done magneto_calibration.conf
eeprom.dat home property
/data # cd ../
/ # ls
@flasher calib etc lib sys usr www
bin data factory proc tmp var
boot dev home sbin update version.txt
/ # cd home
/data/home # ls
root
/data/home # cd root
~ # ls
~ # ll
total 0
~ # cd ../../
/ # ls
@flasher calib etc lib sys usr www
bin data factory proc tmp var
boot dev home sbin update version.txt
/ # find -name "media"
./lib/modules/3.4.11+/kernel/drivers/parrot/media
./lib/modules/3.4.11+/kernel/drivers/media
./sys/bus/media

Taking it a step further:

==========

3D Modeling - Intended for use in Architecture Surveying

- Drag and drop a GEO Bounding Box which gives the drone the area to survey
- Drone automatically flies around the bounding box taking pictures from a myriad of angles
- Drone automatically returns home and lands.
- Info is stored in ‘the cloud’ and processed where it is turned into a 3D rendered model
- From here you are capable of viewing stats on aspects like length, height, surface measurements, etc.

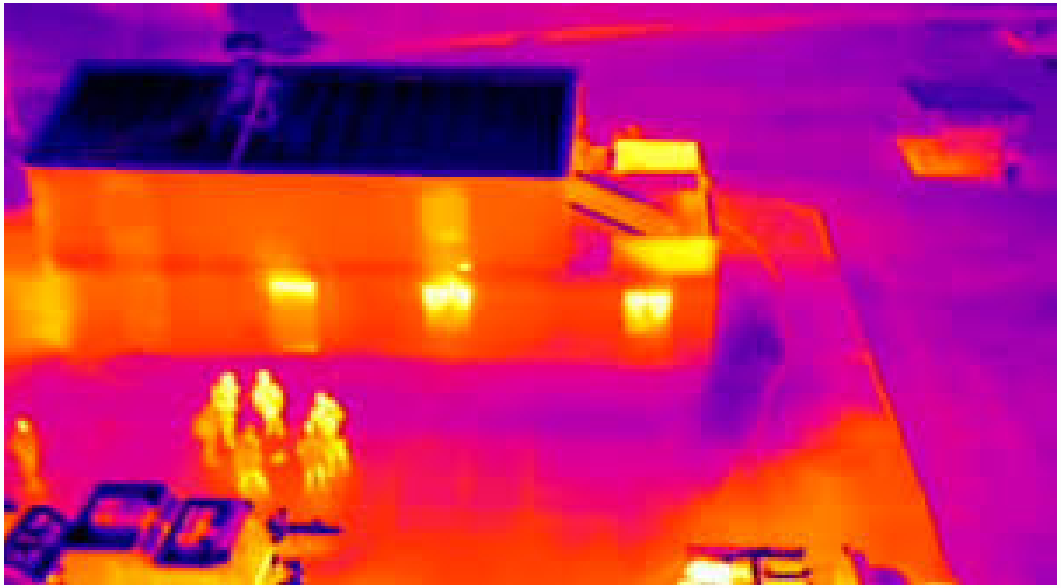


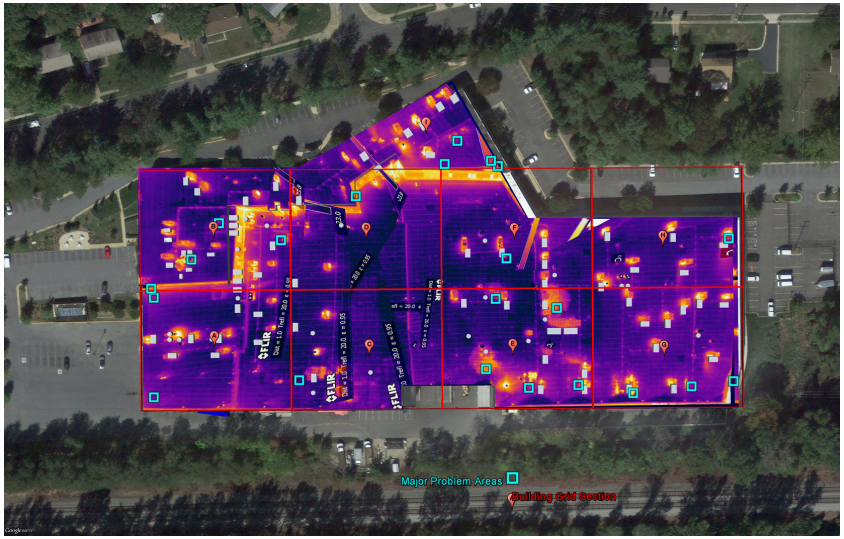
Taking it a step further:

==========

Thermal Cameras - Intended for use in Energy Auditing

- Temperature sensitivity of 0.05 °C
- Variety of palettes and alarm (security) modes, which can be combined with a visible spectrum camera





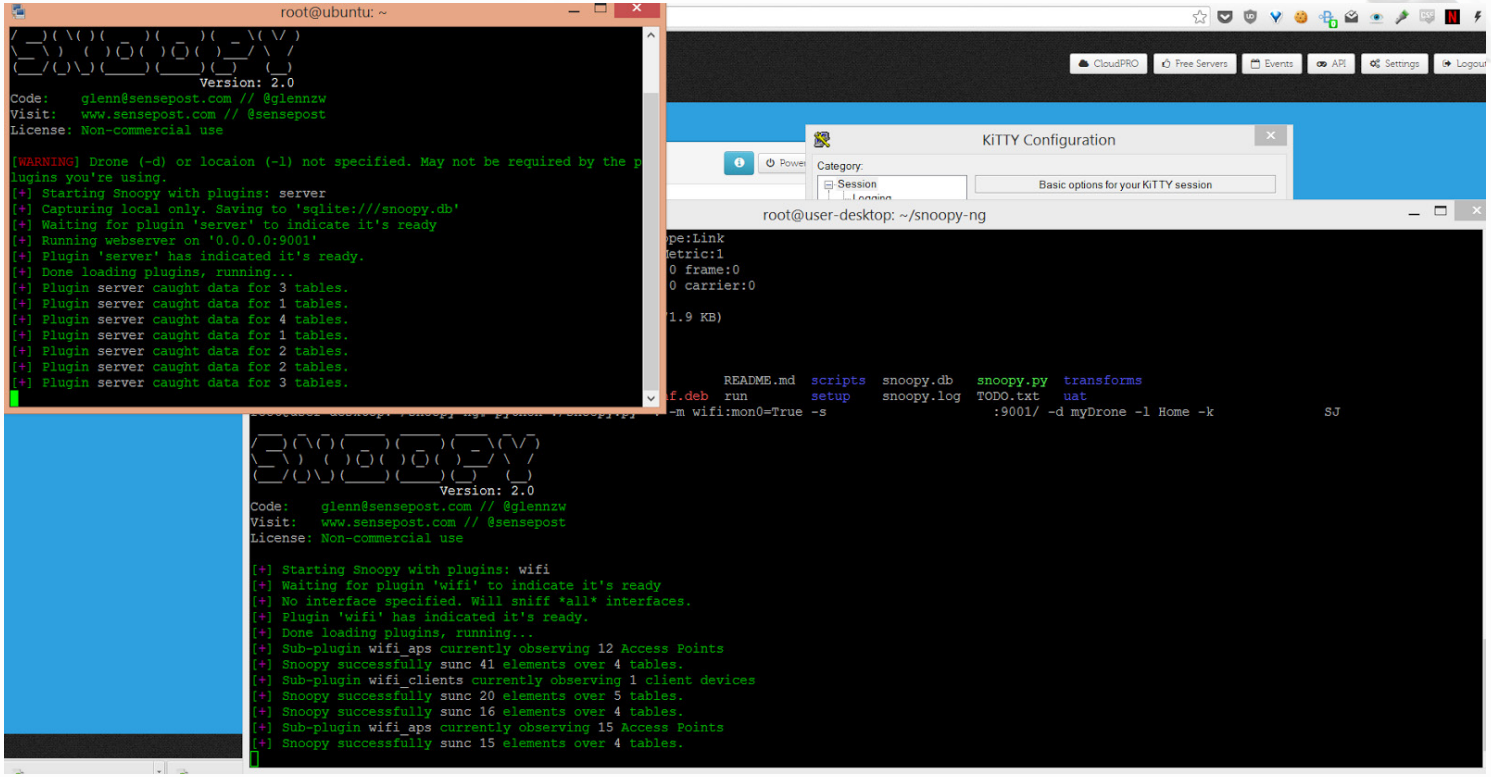
Taking it a step further:

==========

Snoopy + Wigle.net

SNOOPY

- Distributed tracking and profiling framework.
- Performs the following two functions:
    - Collect Probe SSIDs from nearby wireless devices.
    - Offer a Rogue Access Point for nearby wireless devices to connect to.



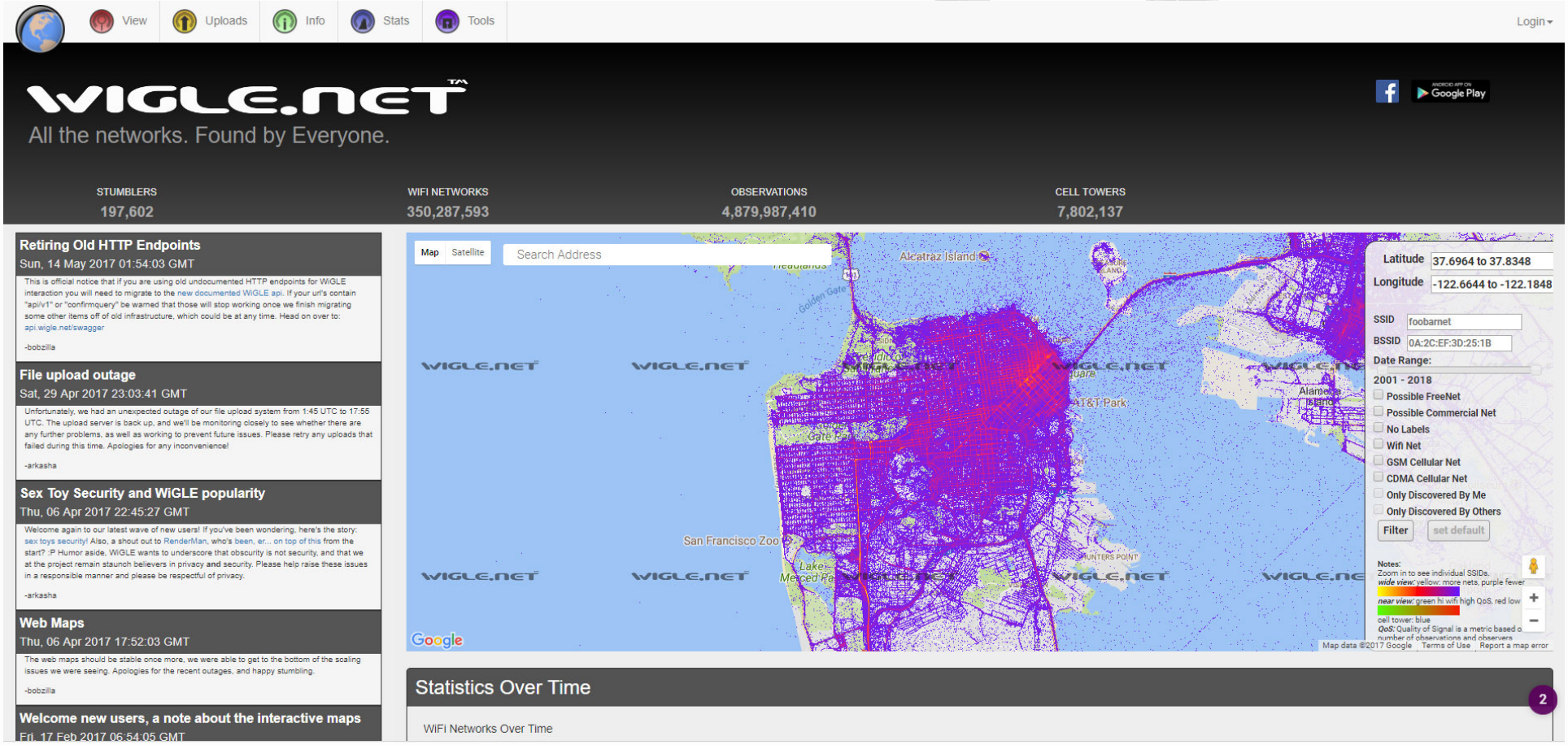
Taking it a step further:

==========

Snoopy + Wigle.net

Wigle

- “We consolidate location and information of wireless networks world-wide to a central database...applications that can map, query and update the database via the web. “

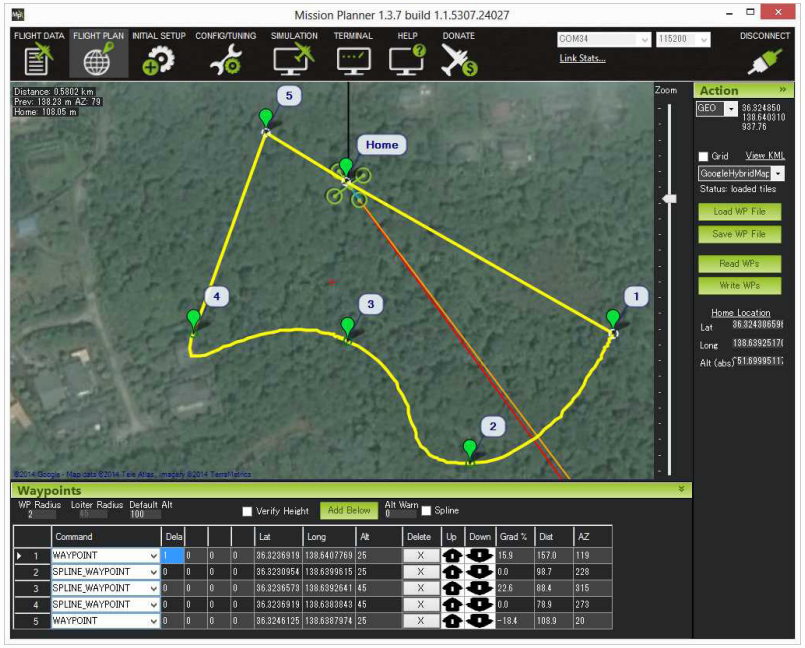


Taking it a step further:

==========

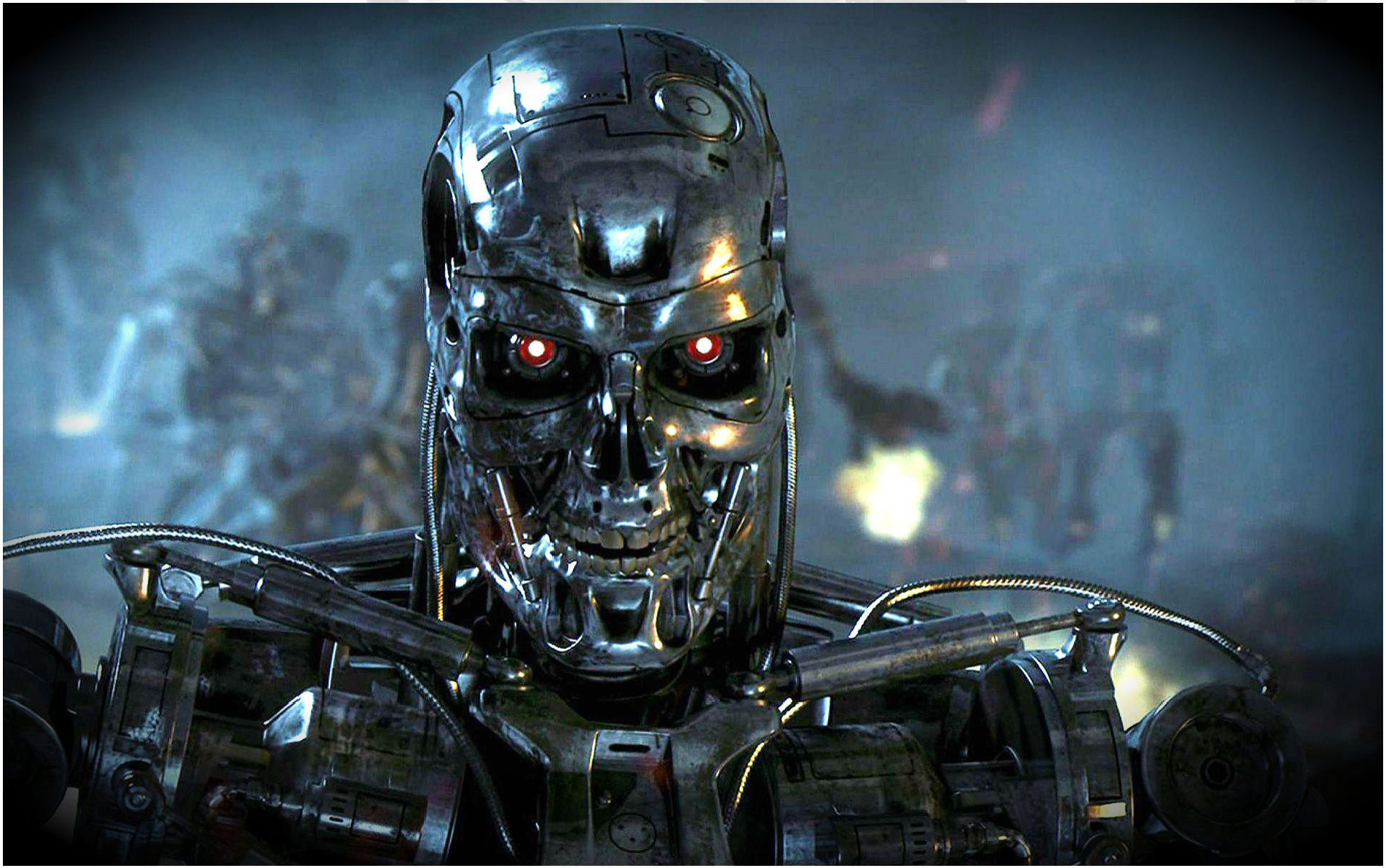
ArduPilot // Full Automation

- “Fully autonomous complex missions which can be programmed through a number of compatible software ground stations. The entire package is designed to be safe, feature rich, open-ended for custom applications, and is increasingly easy to use even for the novice.”



Well then...

==========



The Methodology:

==========

Research Drone
Look for forums / blogs
LOTS of reverse engineering info available online
User manuals, tech specs, open source research

Investigate SDKs / APIs
Look for features / bugs (chipsets in particular)

Choose Attack Type
Deatuh
Packet Spoofing / GPS redirection
Packet Spoofing / Reassociation
GPS Jamming
RF Jamming / Forced Landing
RF Cracking
Man in the Middle VIA Chip Duplication
Survey and Exploitation
Data Exfiltration