

Practical Aerial Hacking & Surveillance

Glenn Wilkinson
SensePost

DefCon 2014

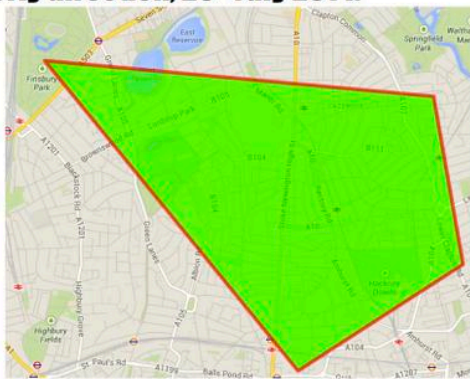


MISSING 'COPTER



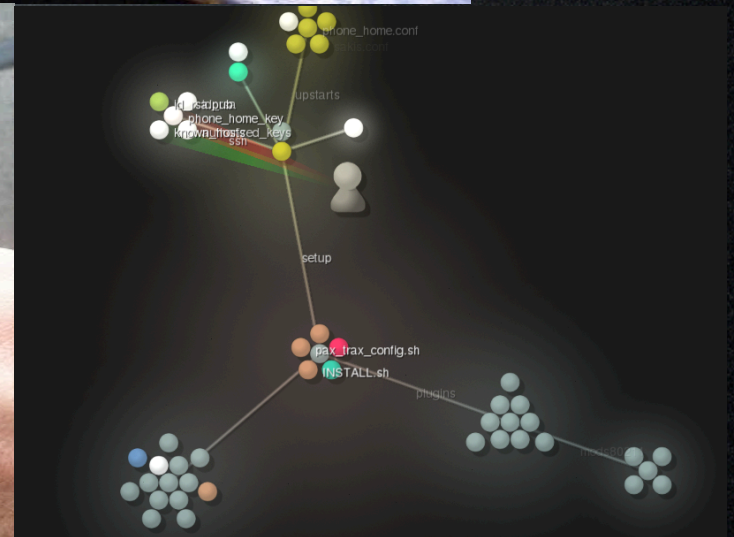
£150 REWARD

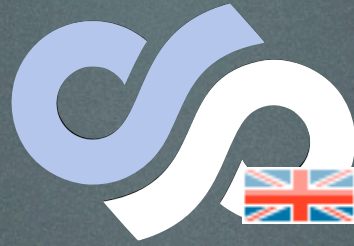
Flew away from Finsbury Park, London in an easterly direction, 26th July 2014.



Map: <http://is.gd/Asm37n>

Contact: foundcopter@gmail.com





SensePost.com



Glenn Wilkinson
@glennzw



@glennzw

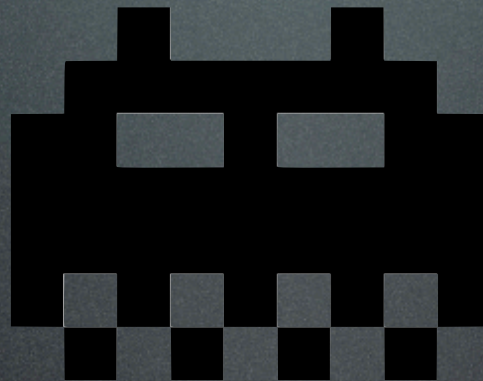

black hat[®]



se~~e~~ure
2013

44CON

ZaCon




iWeb

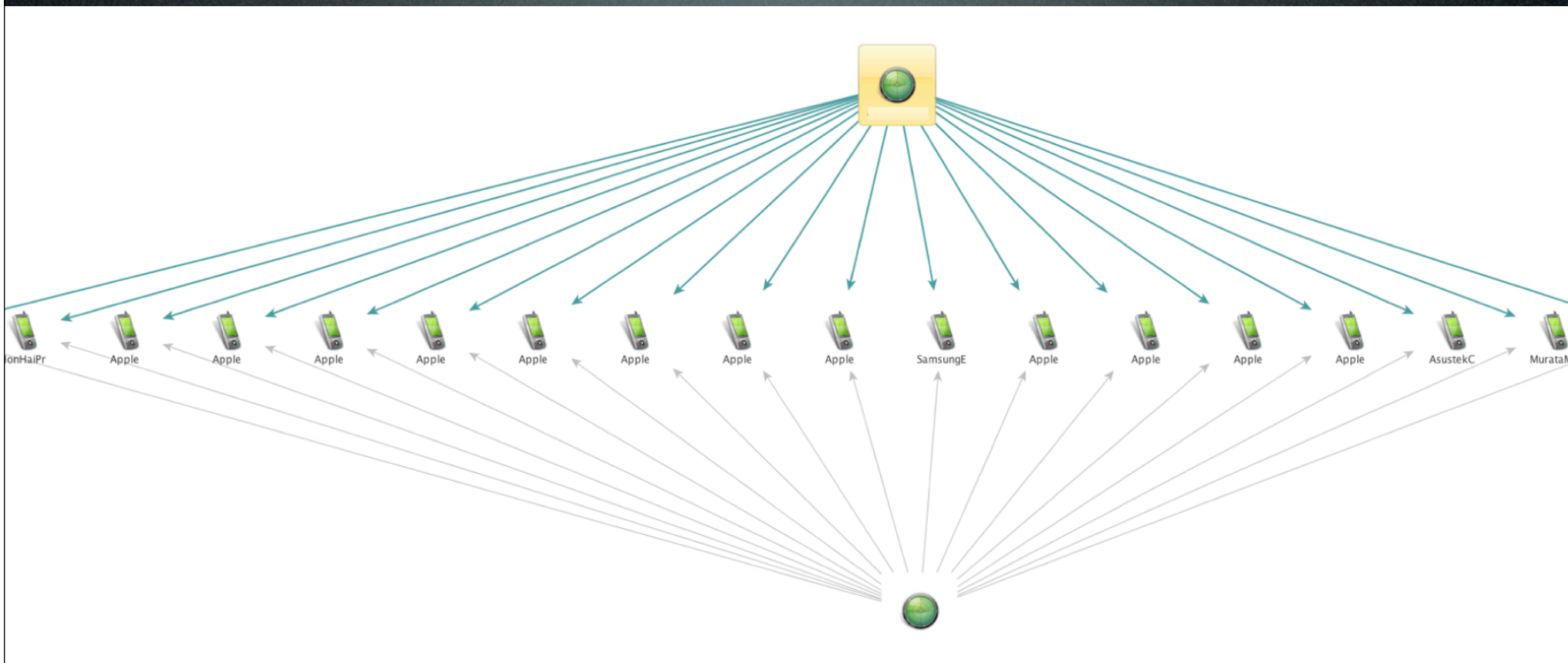


BBC
NEWS

CNN



MOTHERBOARD





Practical Aerial Hacking & Surveillance?

Eyes Over Compton: How Police Spied on a Whole City

A sergeant in the L.A. County Sheriff's Department compared the experiment to Big Brother, even though he went ahead with it willingly. Is your city next?

CIA flew stealth drones into Pakistan to monitor bin Laden house

US Army's A160 Hummingbird drone-copter to don 1.8 gigapixel camera

BY ANDREW MUNCHBACH [@AMUNCHBACH](#)

African firm is selling pepper-spray bullet firing drones

By Leo Kelion



<https://www.eff.org/issues/surveillance-drones>


<https://www.eff.org/deeplinks/2012/01/drones-are-watching-you>

@glennzw

Why we should fight it
(as researchers)

ARE YOU NOT ENTERTAINED?



IS THIS NOT WHY YOU ARE HERE? 



44CON 2013
HTTP://44CON.COM
@44CON

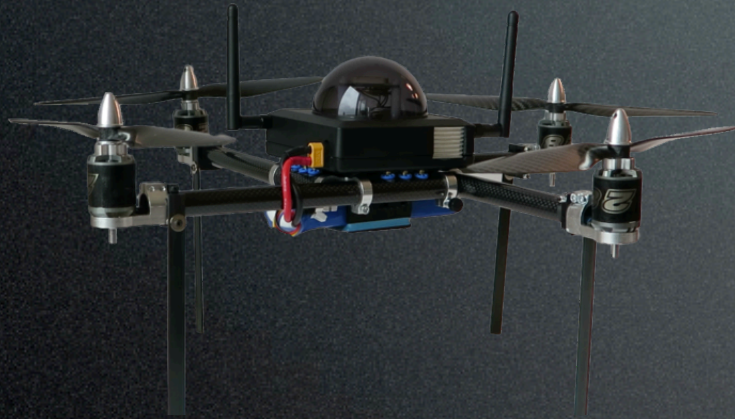
Overview

1. Aerial Platform
2. Ground control / automation
3. Hacking / surveilling payload
4. A methodology

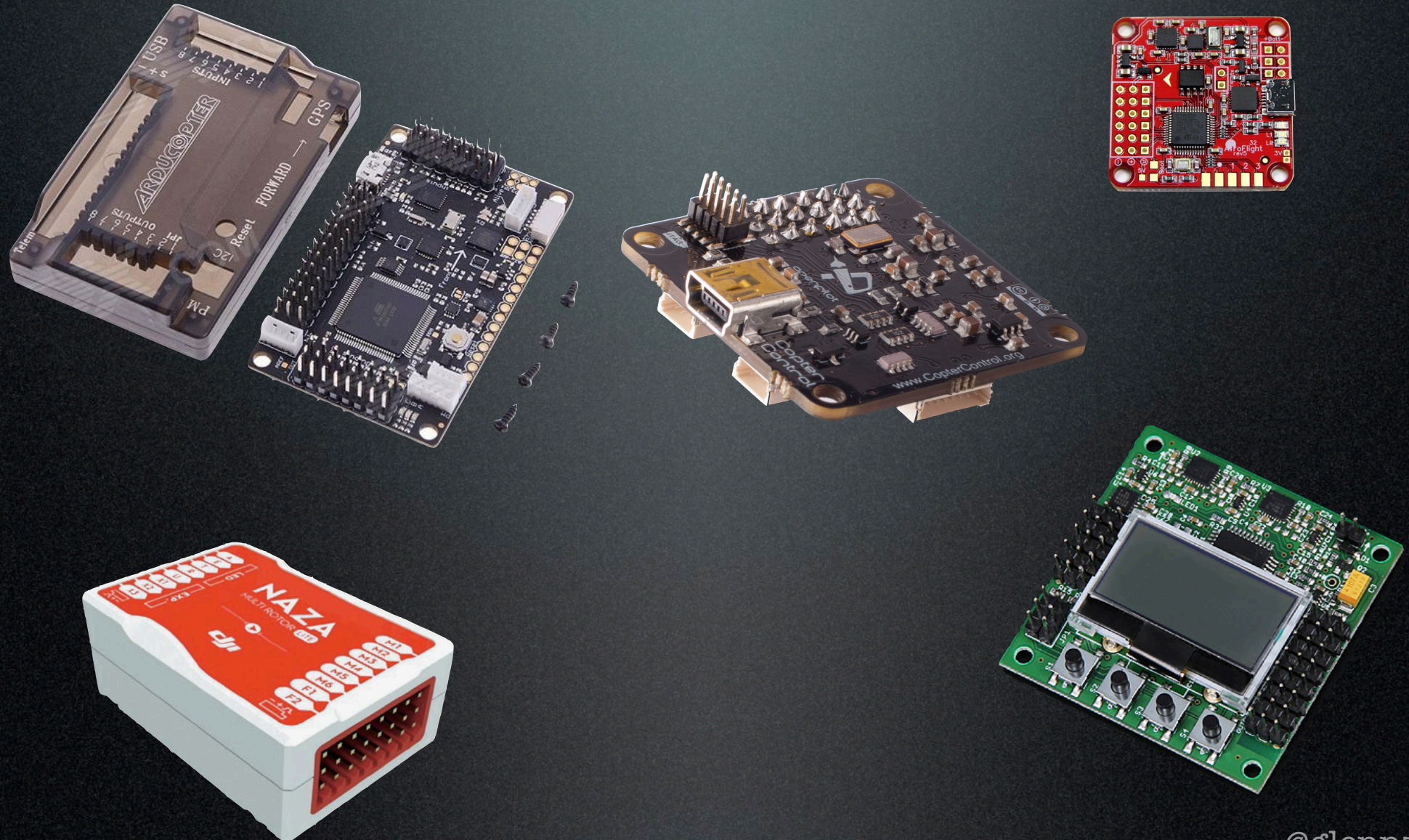
1. Aerial Platform

- Multi-rotor vs Fixed wing
- Flight controller
- Cameras
- GPS

Wing vs Multi-rotor



Flight Controller



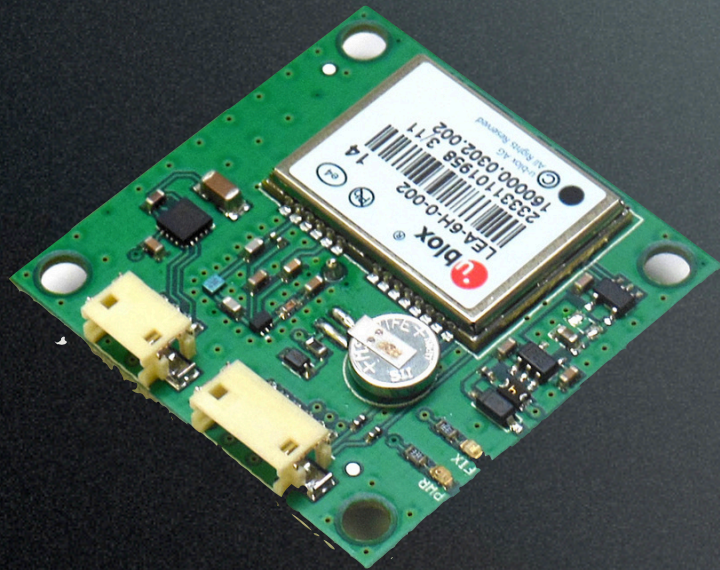
Cameras



Cameras



GPS



Other considerations

- Battery
- ESC
- Motors / propellers

Form Factor Practicality



2. Ground Control / Automation



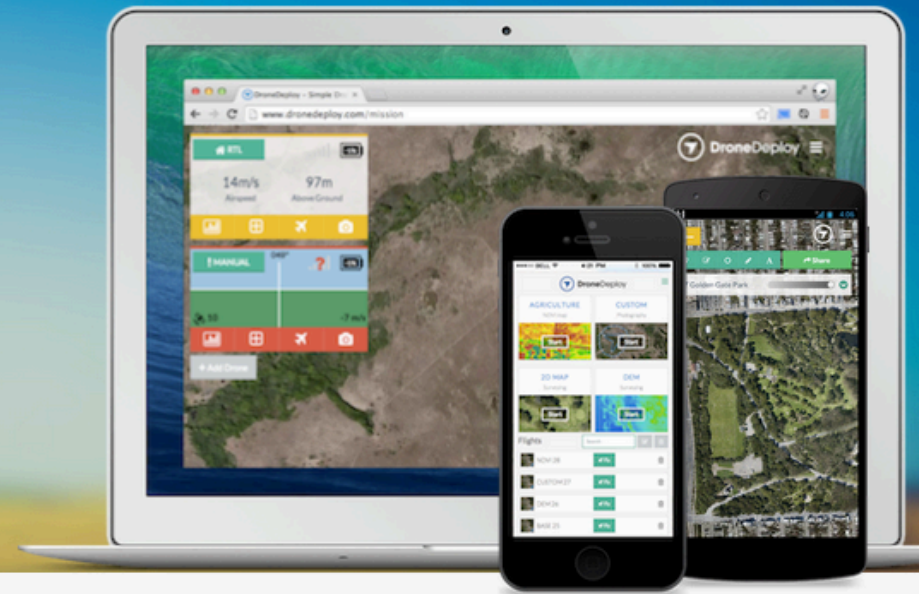
The screenshot displays the QGroundControl interface. The main map shows an aerial view of a city with a red mission plan consisting of several waypoints connected by lines. A red aircraft icon is positioned at one of the waypoints. The right-hand panel contains system status for two MAVs: MAV 001 is in 'READY MODE' with a throttle of 90%, and MAV 220 is in 'LOCKED MODE' with a throttle of 0%. Below this is a 'Horizontal Situation Indicator' (HSI) showing a heading scale and a red aircraft icon. The bottom panel features a 'Mission Plan' console with a list of waypoints: 0 (TakeOff), 1 (Navigate), 2 (Loiter Time), 3 (Ret. to Launch), and 4 (Land). Each waypoint includes fields for mode, frame, latitude, longitude, altitude, and heading. The console also includes buttons for 'Save WPs', 'Load WPs', and 'Send'.

<http://www.qgroundcontrol.org/>

Cloud Control for Drones

A Simple Web-Based Mission Planner

Join the Explorer Program



www.DroneDeploy.com

@glennzw

3. Payload



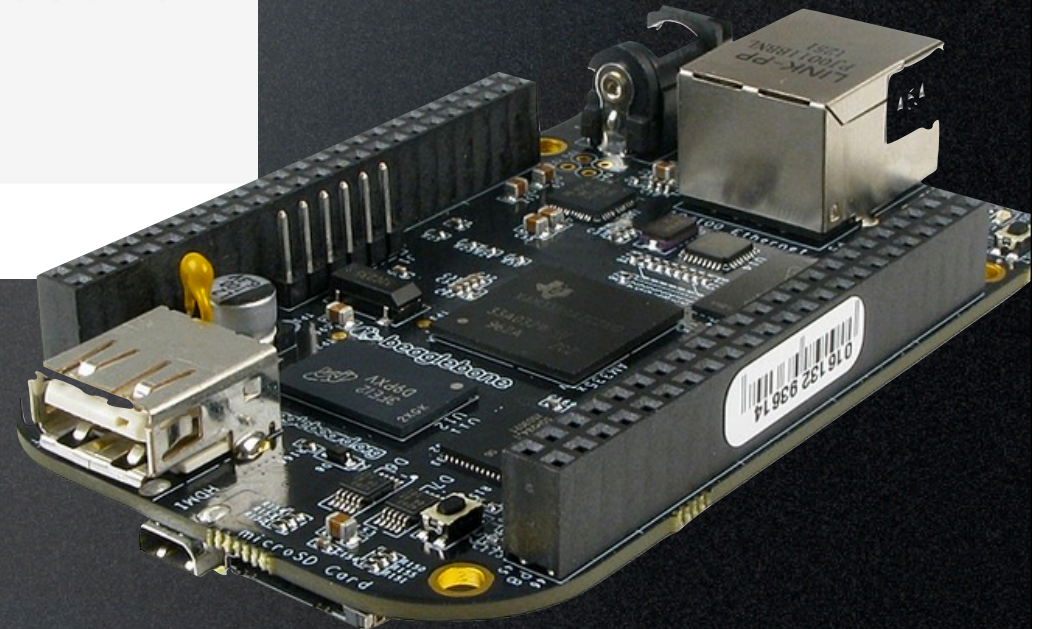
SensePost presents:

```
/$$$$$$
/$$_ $$
| $$ \_/ /$$$$$$$$ /$$$$$$$ /$$$$$$$ /$$$$$$$ /$$ /$$
| $$$$$$ | $$_ $$ /$$_ $$ /$$_ $$ /$$_ $$ | $$ | $$
\___ $$ | $$ \ $$ | $$ \ $$ | $$ \ $$ | $$ \ $$ | $$ | $$
/$$ \ $$ | $$ | $$ | $$ | $$ | $$ | $$ | $$ | $$ | $$
| $$$$$$/ | $$ | $$ | $$$$$$/ | $$$$$$/ | $$$$$$/ | $$$$$$
\___/ |_/ \_/ \___/ \___/ | $$_ / \___ $
| $$ /$$ | $$
| $$ | $$$$$$/
|_/ \_/
```

Version: 2.0

Code: glenn@sensepost.com // @glennzw
Visit: www.sensepost.com // @sensepost
License: Non-commercial use

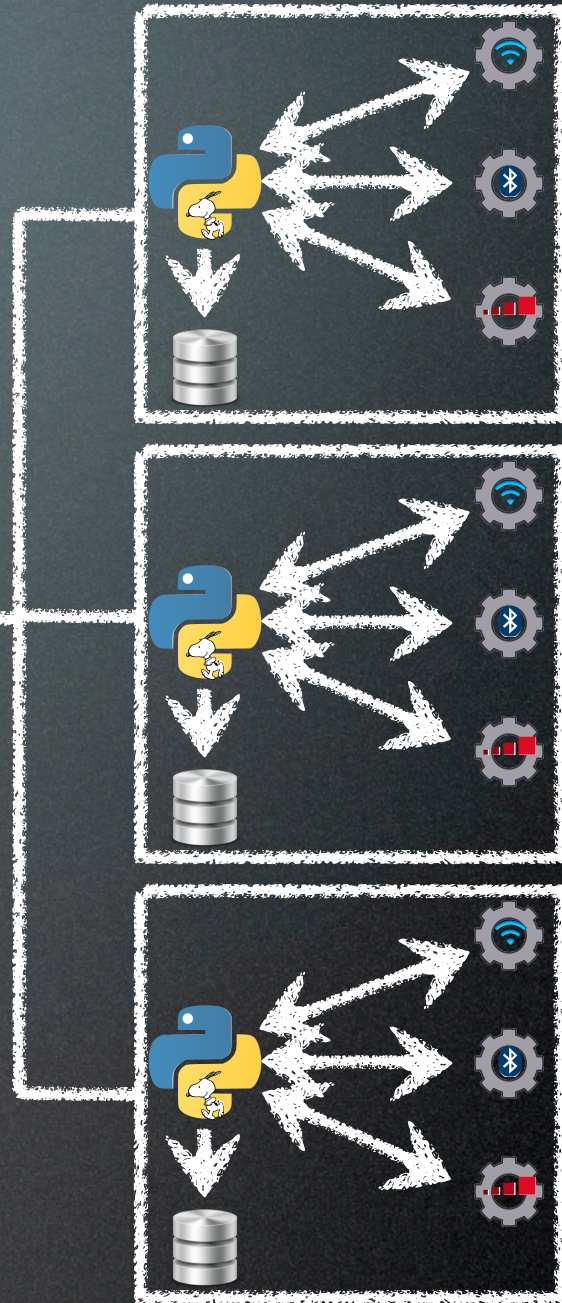
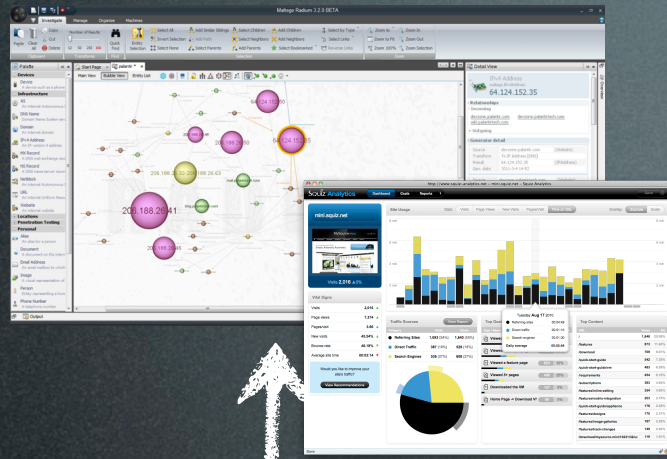
Welcome to Snoopy Version 2.0!





D.T.F






```
root@kali:~# snoopy -iii
```

```
 /_ ) ( \ ( ) ( _ ) ( _ ) ( _ \ ( \ / )  
 \_ \ ) ( ) ( ) ( ) ( ) ( ) _ / \ /  
 ( _ / ( ) \ ) ( _ ) ( _ ) ( ) ( ) ( )
```

Version: 2.0

Code: glenn@sensepost.com // @glennzw

Visit: www.sensepost.com // @sensepost

License: Non-commercial use

[+] Plugins available:

Name: **bluetooth**

Info: Discovers Bluetooth devices.

Name: **example**

Info: This is a test plugin. Testing 1,2,3. Can you hear me?

Parameter: x=<y>

↳ Test parameter one.

Parameter: v=[True|False]

↳ Test parameter two.

Name: **gpsd**

Info: Queries gpsd server for GPS co-ordinates. Ensure the gpsd daemon is running,

Parameter: freq=<seconds>

↳ Frequency to poll GPS. Set to 0 to get one fix, and end.

Parameter: lat=<LAT>

↳ Manually set GPS latitude

Parameter: long=<LONG>

↳ Manually set GPS longitude

Name: **heartbeat**

Info: Returns a heartbeat every 60 seconds.

Name: **local_sync**

Info: Pull database from remote server and sync it into the local one. Make sure to

Parameter: server_url=<url>

↳ URL of server to pull data from. Server plugin should be running on that x

Parameter: sync_freq=<secs>

↳ Frequency to pull a full replica of remote database in seconds


```
Name:      mitmproxy
Info:      This plugin runs a proxy server. It's useful in conjunction with iptables and rogueAP
Parameter: port=<port>
           ↳ Port for proxy to listen on.
Parameter: upprox=<ip:port>
           ↳ Upstream proxy to use.
Parameter: transparent=[True|False]
           ↳ Set transparent mode. Default is False

Name:      rogueAP
Info:      Create a rogue access point.
Parameter: ssid=<name>
           ↳ The SSID of the access point.
Parameter: promisc=[True|False]
           ↳ Set promiscuous mode (respond to all probe requests).
Parameter: run_dhcp=[True|False]
           ↳ Run a DHCP server.
Parameter: local_nat=[True|False]
           ↳ Run local NAT to route traffic out.
Parameter: hostapd=[True|False]
           ↳ Use hostapd instead of airbase-ng.
Parameter: hapdconf=<path>
           ↳ Specify the hostapd config file to use.
Parameter: hapdcmd=<path>
           ↳ Specify the hostapd binary to use.
Parameter: sslstrip=[True|False]
           ↳ Send traffic through Moxie's SSL strip.

Name:      server
Info:      Runs a server - allowing local data to be synchronized remotely.
Parameter: port=<int>
           ↳ The HTTP port to listen on.
Parameter: xbee=<int>
           ↳ The XBee PIN to listen on (see Pro version).

Name:      sysinfo
Info:      Retrieves system information, every 30 minutes.

Name:      wifi
Info:      This plugin intercepts and processes network traffic. A series of sub-plugins exists within
           *apple_guids - Apple devices emit a GUID when joining a network. This captures it.
           *wifi_aps - Extract BSSIDs (i.e. Access Points)
           *firelamb - Extract web cookies
           *wifi_clients - Observe WiFi client devices based on probe-requests emitted.
           *wpa - Capture WPA handshakes
Parameter: iface=<dev>
           ↳ interface to listen on. e.g. -m iface:iface=mon0
Parameter: mon=[True|False]
           ↳ First enable monitor mode on <iface>. e.g. -m wifi:iface=mon0,mon=True. If no <iface> sp
Parameter: pcap=<pcapFile>
           ↳ Read data from a pcap capture file instead of an interface.
```



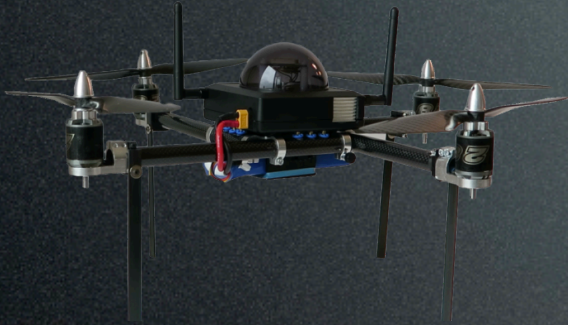
```
Name:         wigle
Info:         Looks up SSID locations via Wigle (from the ssid table).
Parameter:    username=<u>
              ↳ Wigle username
Parameter:    password=<p>
              ↳ Wigle password
Parameter:    email=<foo@bar.com>
              ↳ Supplied in query to OpenStreetView. It's polite to use your real email
```


It's open source!

- In progress:
 - GSM, iBeacon, SDR, ZigBee, ANT, NFC, RFID
- Other ideas:
 - OpenCV, physical detection

<https://github.com/sensepost/snoopy-ng>

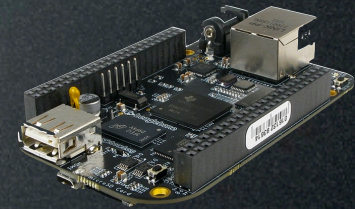
4. Methodology



Vehicle



Autonomy



Payload



Ground Control

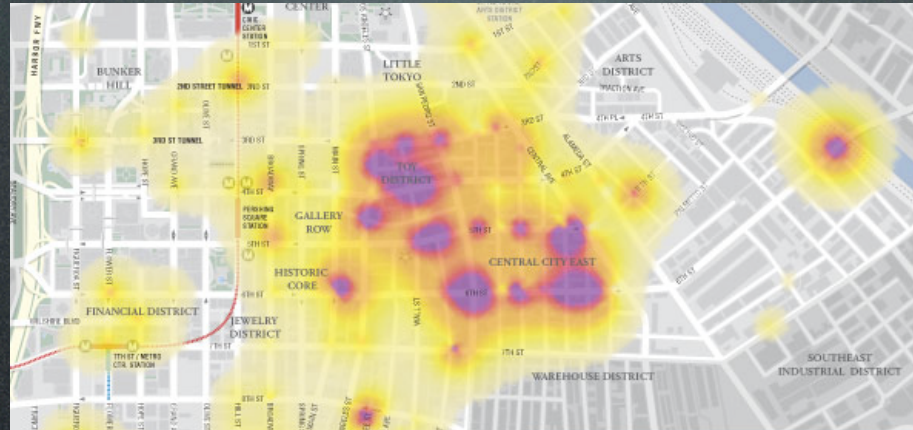
Use Cases



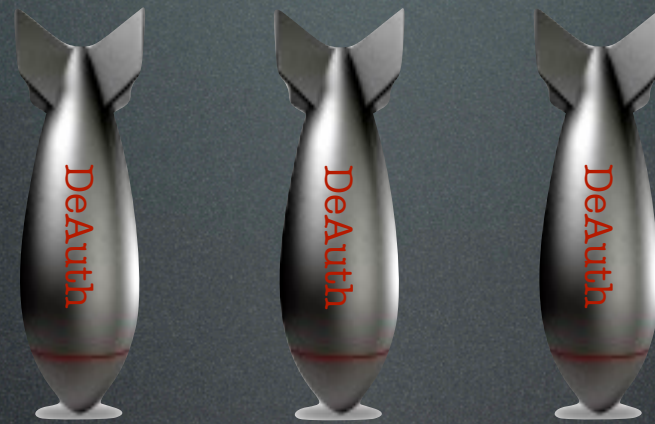
Use Cases

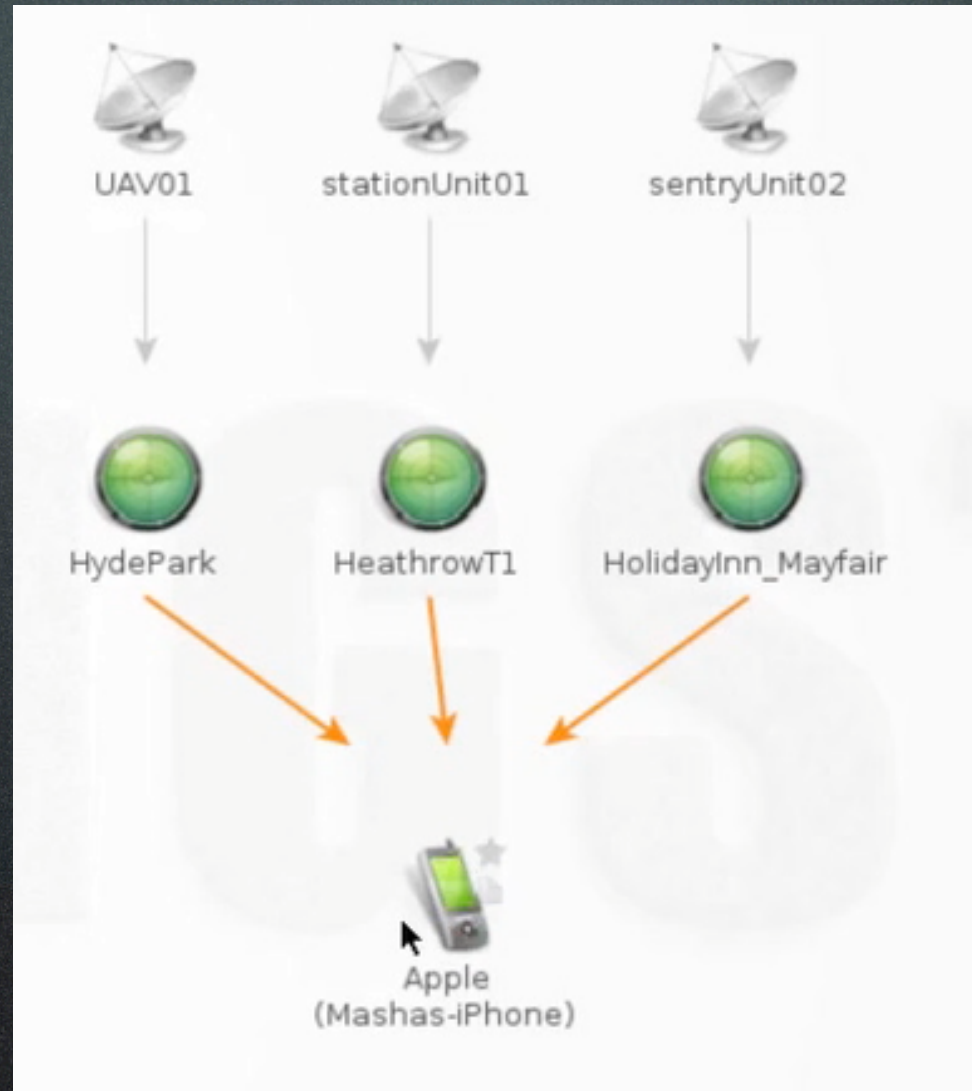


Use Cases



Use Cases





[Video Demo]

Snoopy's friends...

Retail





Military



VERINT

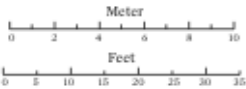
@glennzw

DRONE SURVIVAL GUIDE

د بي پيلوټه الوتكو د پايښت لارښود



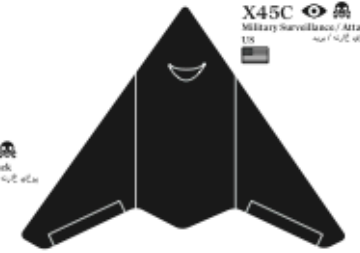
X47C
Military Surveillance / Attack
US



Sentinel
Military Surveillance
US



nEUOn
Military Surveillance / Attack
FUTURESURCHIES



X45C
Military Surveillance / Attack
US



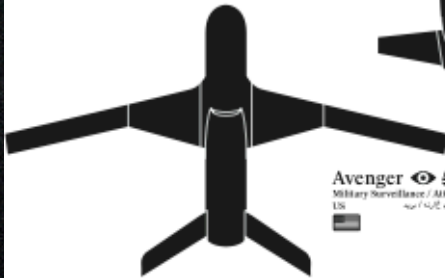
Global Hawk
Military Surveillance
US/UK



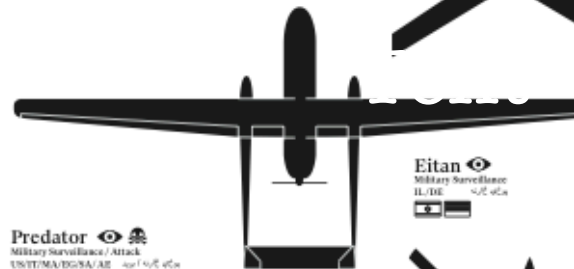
Soaring Dragon
Military Surveillance / Attack
CN



Mantis
Military Surveillance / Attack
GB



Avenger
Military Surveillance / Attack
US



Eitan
Military Surveillance
IL/IE



Reaper
Military Surveillance / Attack
USA/GB/FR/ITA/UNL



Herti
Surveillance
GB



Predator
Military Surveillance / Attack
US/UK/MA/ISRA/AF



Hummingbird
Military Surveillance / Attack
US



Fire Scout
Military Surveillance / Attack
US



Heron
Military Surveillance
IL/UN/DE/FR/CA/AM



Barracuda
Military Surveillance / Attack
EU/ES



Shadow
Military Surveillance
US/UK/FR/RO/ISR/IT



Rustom I
Military Surveillance
IN

WASP III
Military Reconnaissance
US/FR/AU/SE



Scan Eagle
Military Surveillance
US/GR/CA/MY/CO/UN/JP/PL/SG/IN



Harpy
Military Attack
IL/IR



Killer Bee
Surveillance
US/IR/ISRA/PAK/AF



Raven
Military Reconnaissance
US/CO/UK/PAK/AF



Air robot
Domestic Surveillance
UK

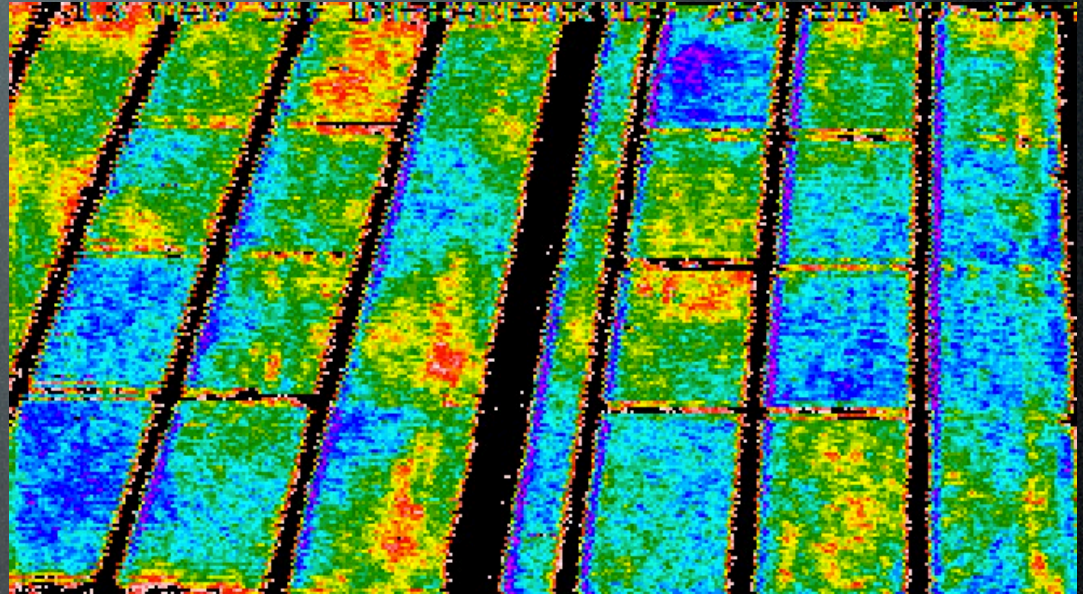


Aeryon Scout
Domestic Surveillance
CAN/US/UK




AR Parrot
Consumer photography
US

The good!



Site launch!

SHADOWDARKLY SENSOR ABOUT THE SENSOR FEATURES BUY DEPLOYMENT OPTIONS FAQ



ShadowDarkly Sensor is a distributed, tracking, profiling, data interception, and visualisation framework. It allows the tracking of a wide array of signal emitting devices that people carry with them - from mobile phones, to smart watches, to RFID/NFC tags.

The modular nature of ShadowDarkly Sensor allows the easy addition of new capabilities as new technologies emerge.

SHADOWDARKLY SENSOR Logged in as glenn Logout

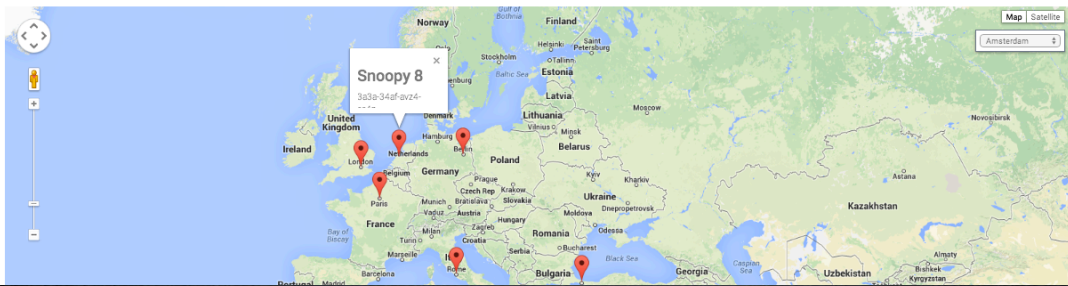
Your Sensors

10 records per page Filter:

Name	ID	Location	Uptime	Load	Status	Action
Snoopy 1	aafe-34af-nrtz-hngs	London	--	--	Offline	View Edit Delete

Showing 1 to 2 of 2 entries Previous 1 Next

Sensor Locations



<http://www.sensepost.com/blog>

@glennzw

#SnoopySensor

Digital Terrestrial Tracking: The Future of Surveillance



Glenn Wilkinson
SensePost
@glennzw



glenn@sensepost.com

ABSTRACT

In this paper, the terms *Digital Terrestrial Tracking* (DTT) and *Digital Terrestrial Footprint* (DTF) are introduced. The DTF defines the uniquely identifiable signature of wireless signals emitted by a device or collection of devices that an individual carries on their person in the physical world. These signals can reveal a device's history at a location and point in time, and potentially disclose details about the owner. Interrogation or interaction with the device may reveal further details.

The DTF positions itself between an individual's physical world footprint (their unique personal attributes), and their online footprint (defined by their unique online persona). Physical world tracking would involve following a person based on what they look or sound like; online tracking would involve tracking a person online activity based on their unique online signature (cookies, IP addresses, social media accounts); and digital terrestrial tracking involves tracking a person in the real world based on a unique signature emitted by devices on their person.

The goal of the research conducted and discussed in this paper was to build a mass data collection and correlation framework based on information leaked from the wireless devices that people carry. The framework should be able to identify, track, and profile people by passively collected wireless information from devices, and collect information that is more verbose by optionally interrogating devices.

(and therefore the owner) can be identified as being in a certain location at a certain time. The signals may also reveal personal information about the owner, or upon interrogation or interaction divulge such information.

An example of such signals is the 802.11 wireless *probe-request* that is broadcast from mobile phones and other portable Wi-Fi enabled devices. These signals include a unique MAC address of the device, and the name (SSID) of the wireless network being searched for. The SSID may be able to be geo-located, or simple link-analysis could be conducted by identifying different devices searching for the same SSIDs, thus revealing secondary and even tertiary relationships (e.g. a spouse, or business partner).

Active interaction with devices may also be possible. For example, due to a lack of verification with WEP or OPEN Wi-Fi networks it is possible to respond to arbitrary probe requests from client devices with a *beacon*, thereby impersonating the desired access point, and intercepting network traffic from client devices. Similar techniques work with GSM, by detecting the unique IMSI (international mobile subscriber identity) of a mobile phone, with the option of operating a personal cellular tower (small cell) to intercept data. Other examples include detecting the MAC address and device name via Bluetooth; detecting the device ID with RFID; reading data from an NFC device; or detecting the device number of an ANT fitness device. Furthermore, if carrying multiple devices the cloud of device signals may provide a unique identity even if individual devices do not.

<http://www.sensepost.com/blog>

@glennzw

Mana From Heaven:

Improving the state of wireless
rogue AP attacks

Saturday, 4pm, Penn & Teller



sensepost

glenn@sensepost.com

jobs@sensepost.com

<http://research.sensepost.com/>

@glennzw