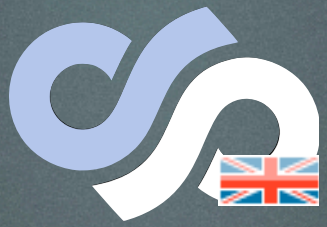
The Machines That Betrayed Their Masters

Glenn Wilkinson

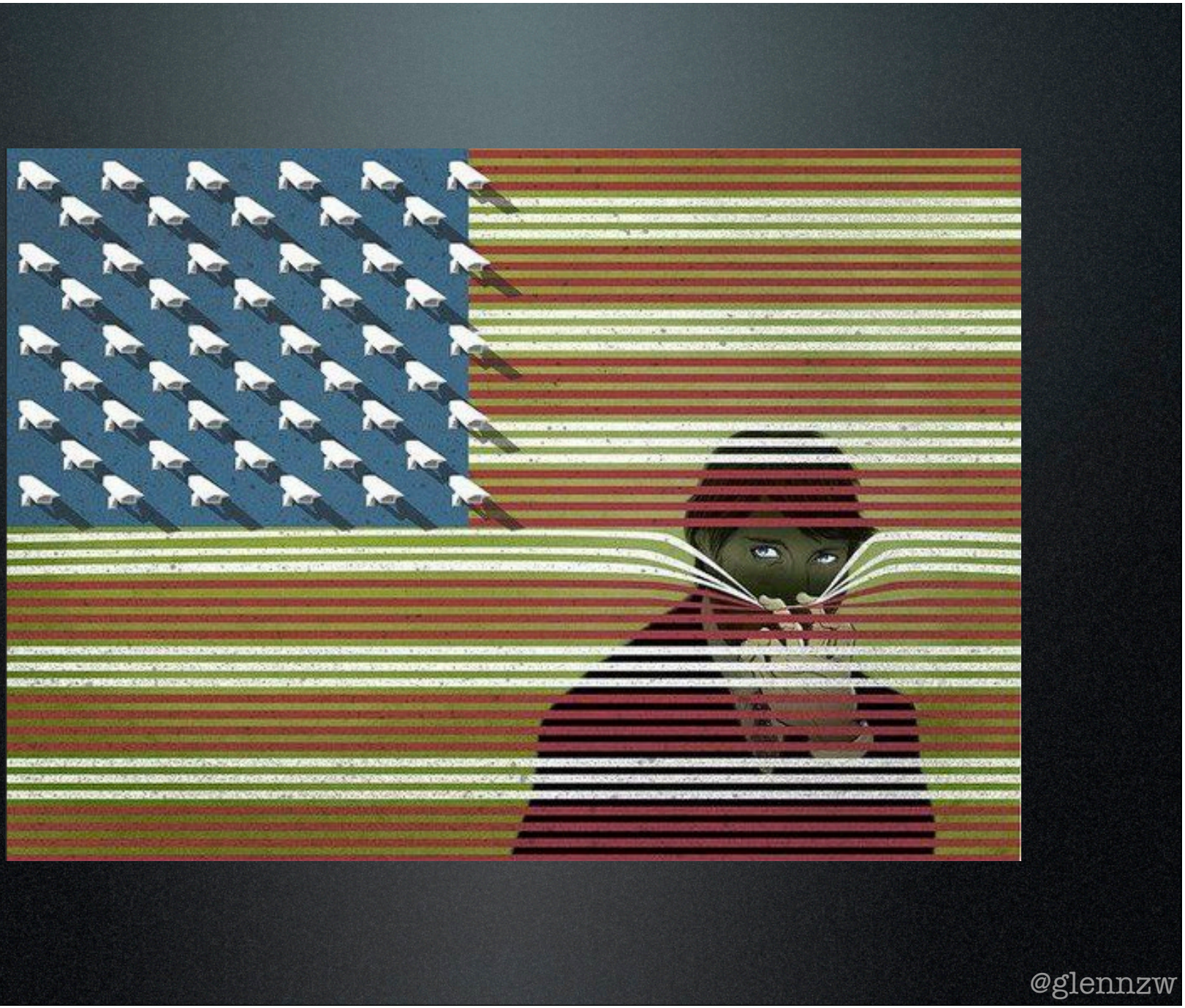
BlackHat Asia 2014



SensePost.com

Glenn Wilkinson
@glennzw

Machines? Betrayal?


@glennzw


UNITED STATES OF AMERICA
PASSPORT CARD
USA
Nationality
USA
Passport Card no.
C04627109
Surname
WEBER
Given Names
BRIAN PHILLIP
Sex
M
Date of Birth
22 NOV 1968
Place of Birth
UTAH, U.S.A.
Issued On
04 APR 2011
Expires On
03 APR 2021
E-2118615-07
UNITED STATES DEPARTMENT OF STATE


SONY
12:34
Twitter
Email
Music
Weather

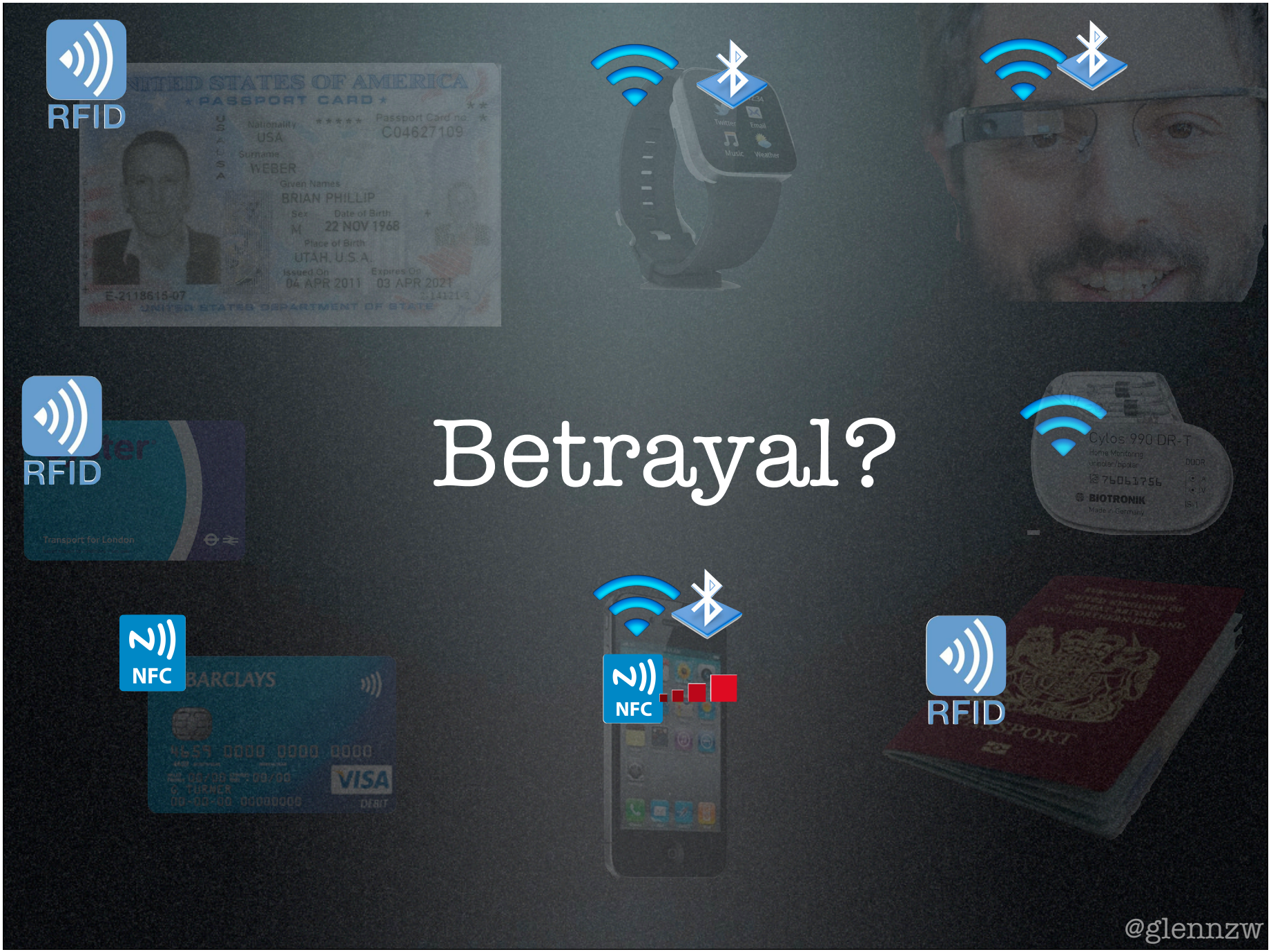
Machines?


oyster
Transport for London


Cylos 990 DR-T
Home Monitoring
unipolar/bipolar
DDDR
76061756
BIOTRONIK
Made in Germany
IS-1


BARCLAYS
4659 0000 0000 0000
VISA
DEBIT
G TURNER


EUROPEAN UNION
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
PASSPORT


RFID
UNITED STATES OF AMERICA
PASSPORT CARD
Nationality
USA
Passport Card no.
C04627109
Surname
WEBER
Given Names
BRIAN PHILLIP
Sex
M
Date of Birth
22 NOV 1968
Place of Birth
UTAH, U.S.A.
Issued On
04 APR 2011
Expires On
03 APR 2021
E-2118615-07
UNITED STATES DEPARTMENT OF STATE
RFID
Transport for London
Betrayal?
Cylos 990 DR-T
BIOTRONIK
Made in Germany
NFC
BARCLAYS
VISA
DEBIT
NFC
RFID
@glennzw

A Device

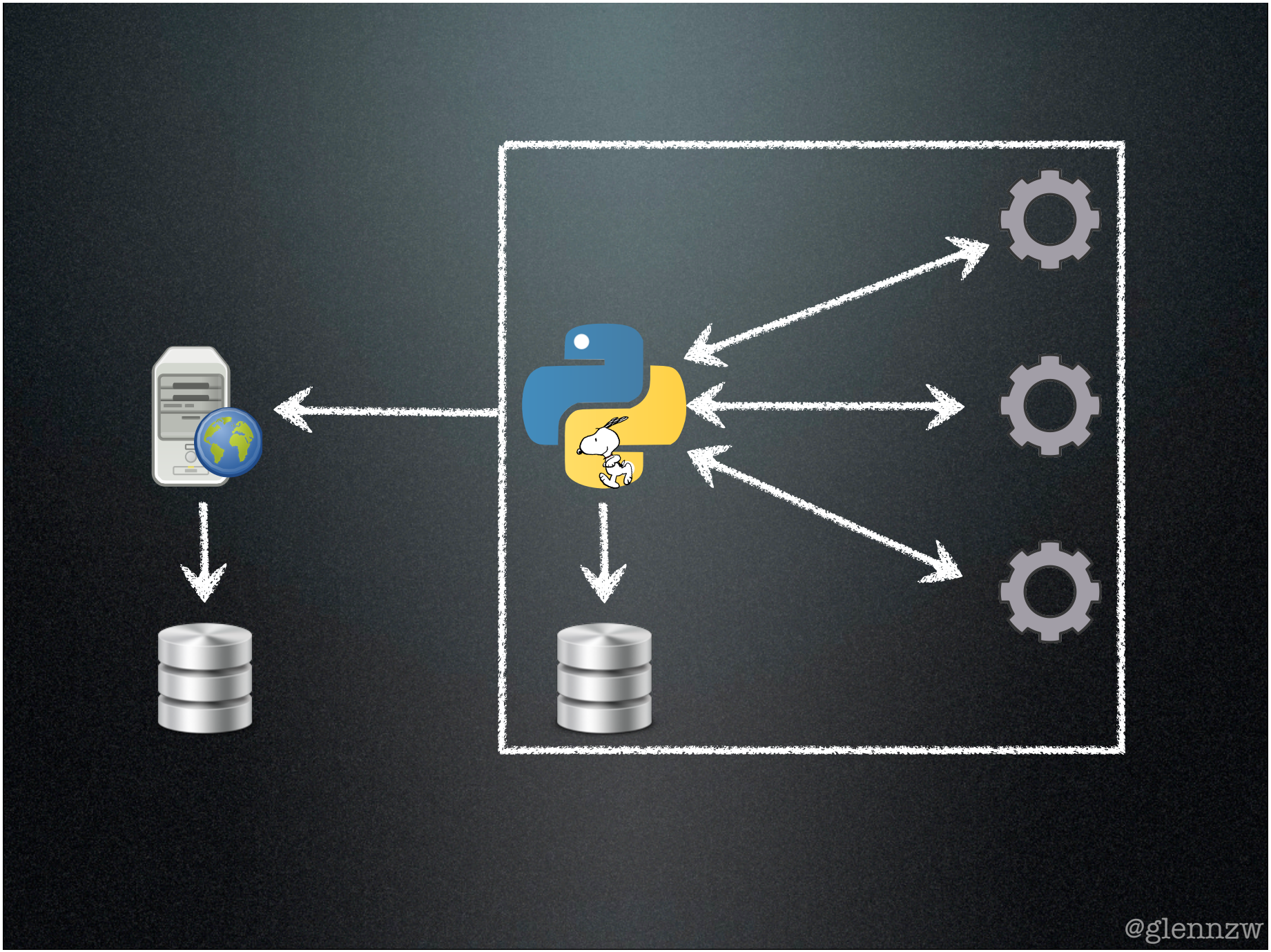
A Unique Signature

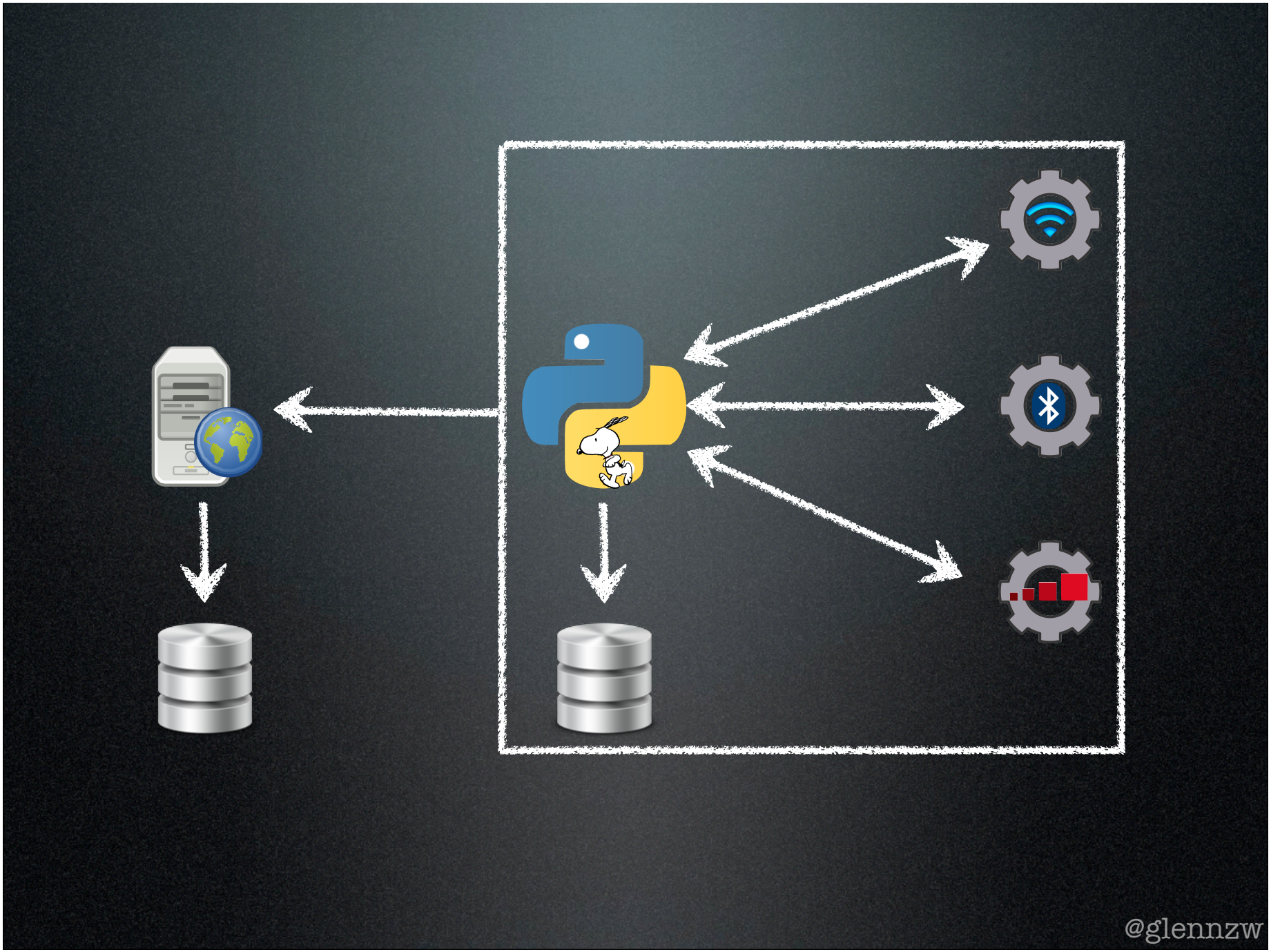
aka

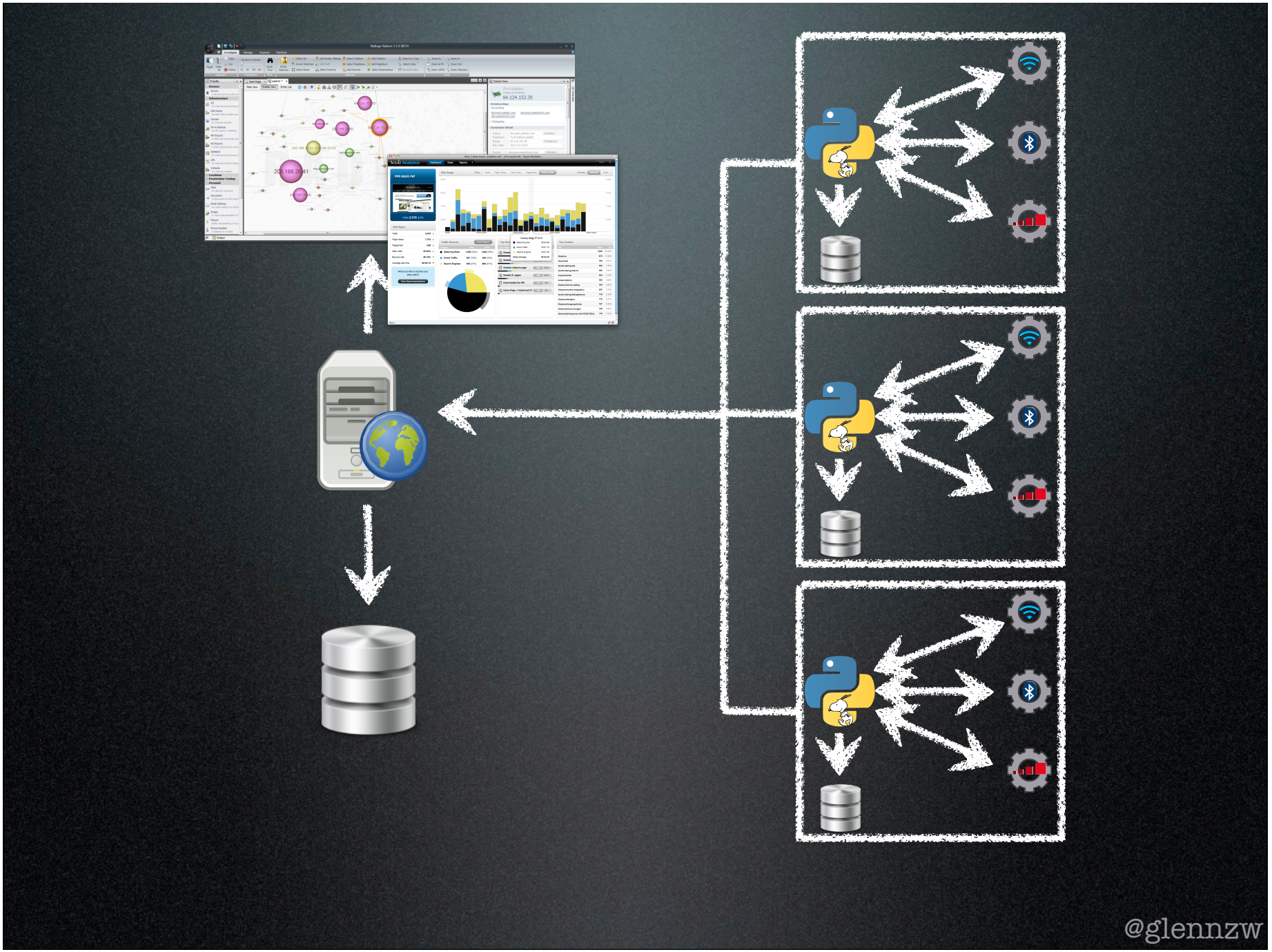
“Digital Terrestrial Footprint”

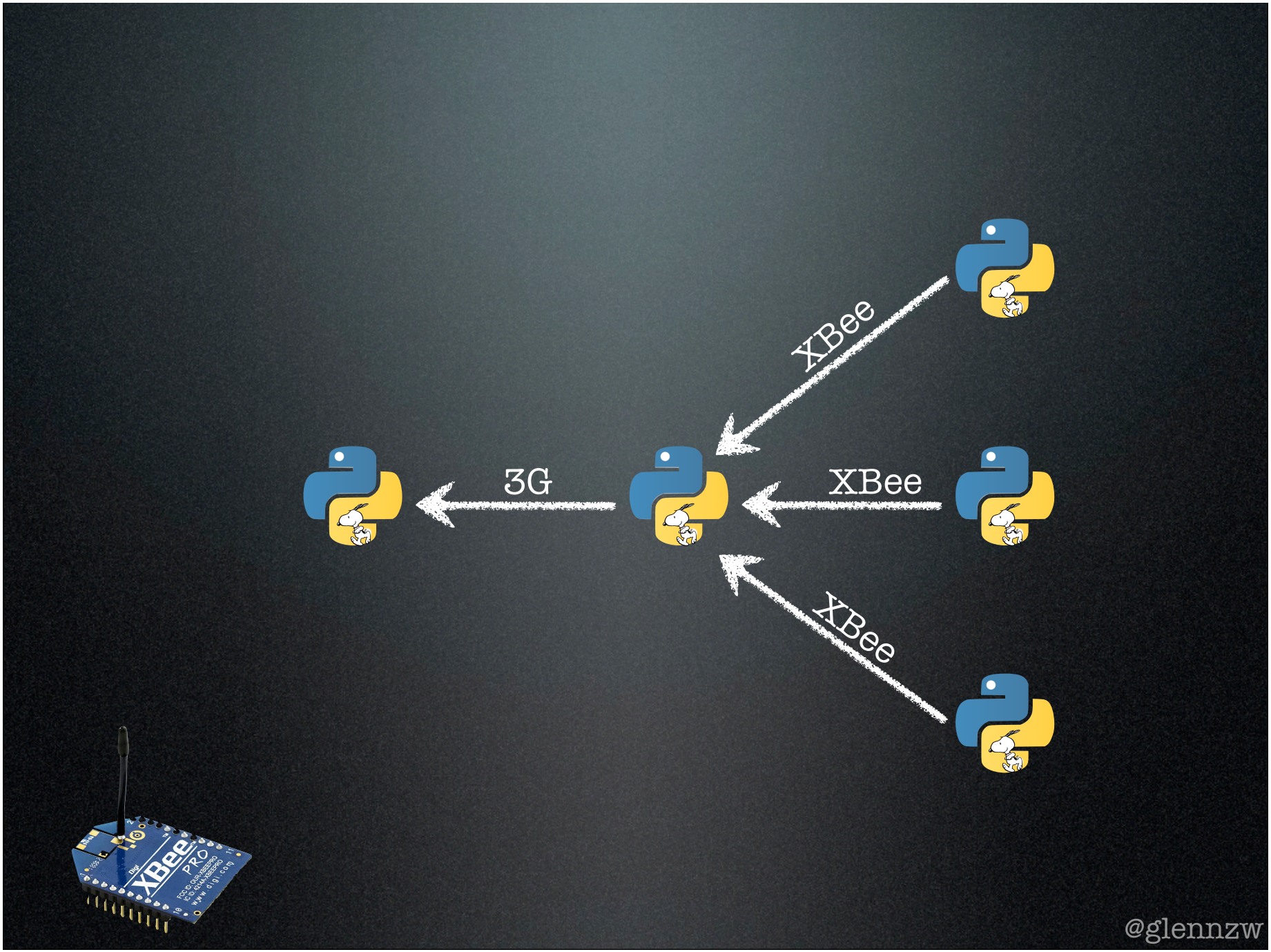
A Link from Signature to a Human

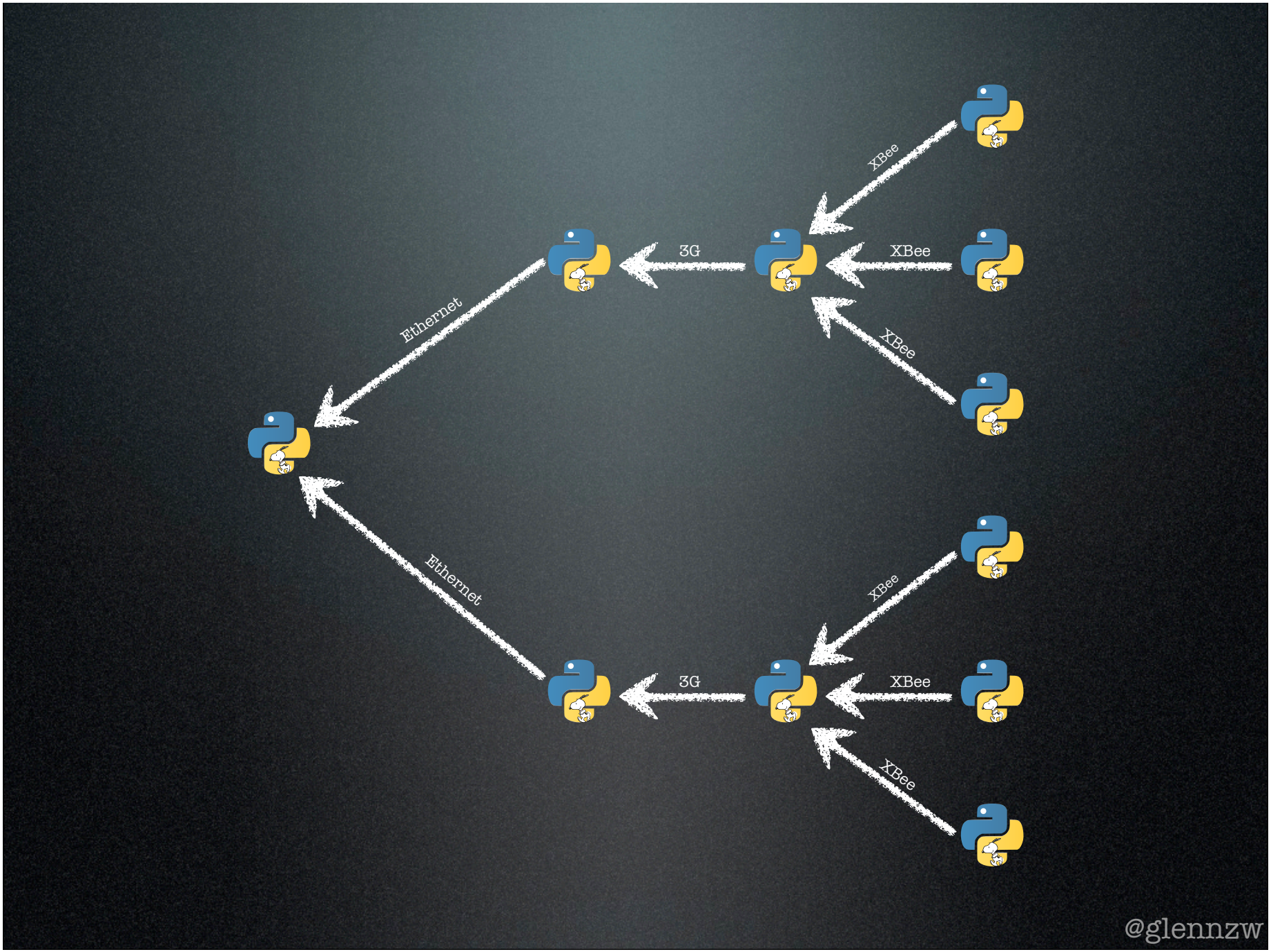
Snoopy Framework


@glennzw


@glennzw


@glennzw


XBee
3G
XBee
XBee
@glennzw


XBee
3G
XBee
Ethernet
XBee
Ethernet
XBee
3G
XBee
XBee
@glennzw


End
SAMSUNG
12:45
Thu, 3 May
@glennzw

A Unique Signature

98:03:ab:32:11:33

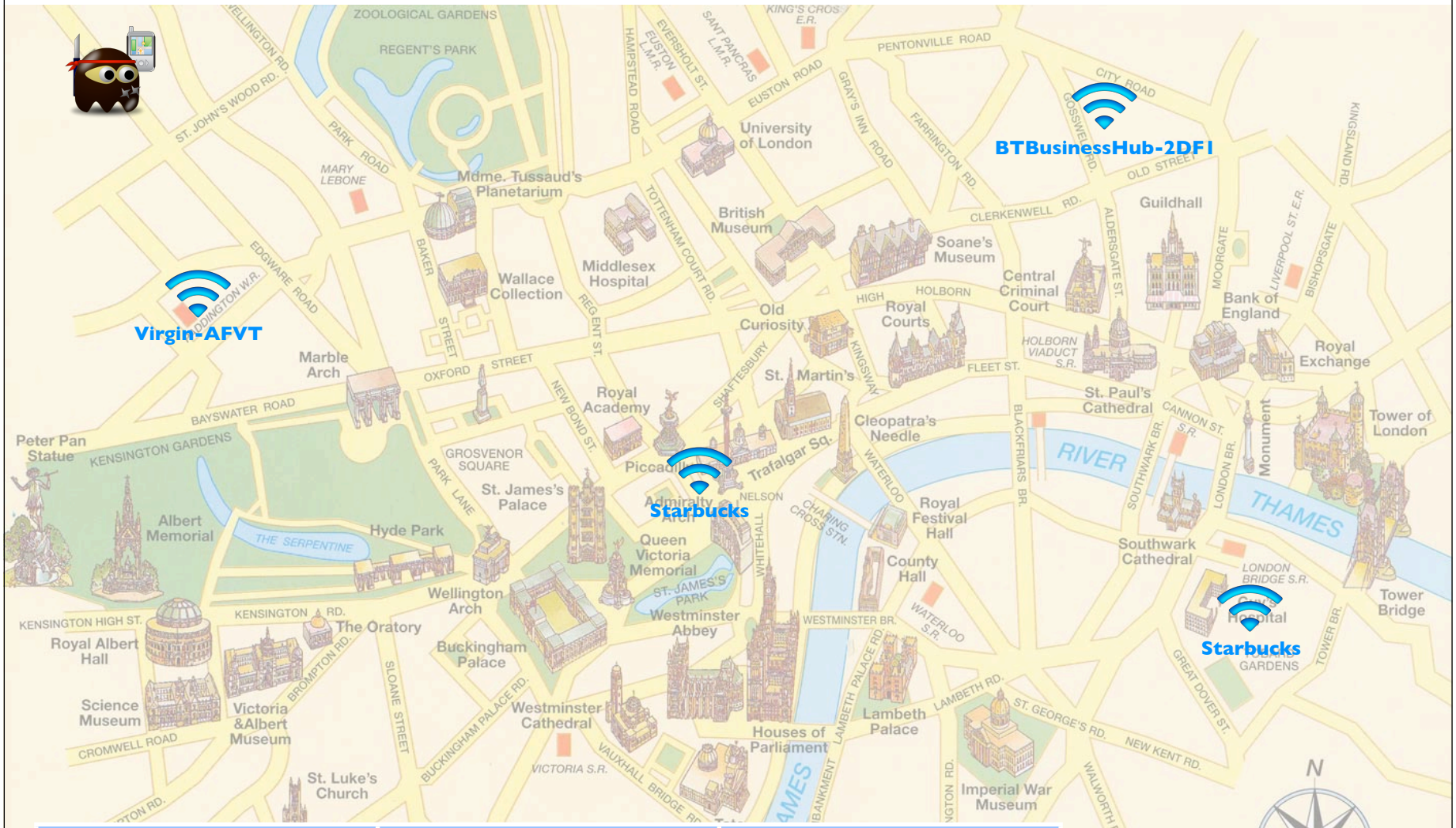
Linking the Signature

Linking the Signature

1. Passive Linking

BTHomeHub-AFV1, are you there?
Starbucks, are you there?
Virgin-AFVT, are you there?
Is anyone out there?

98:03:ab:32:11:33



SSID	GPS Lat	GPS Long
Virgin-AFVT	50.507	-0.128
Starbucks	50.408	-0.041
BTBusinessHub-2DF1	50.601	-0.045
Starbucks	50.391	-0.050

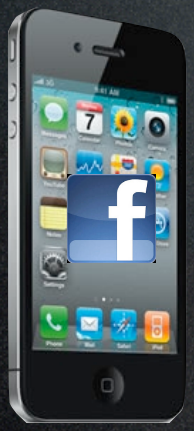
BTHomeHub-AFV1, are you there?
Starbucks, are you there?
Virgin-AFVT, are you there?
Is anyone out there?

98:03:ab:32:11:33

Linking the Signature?

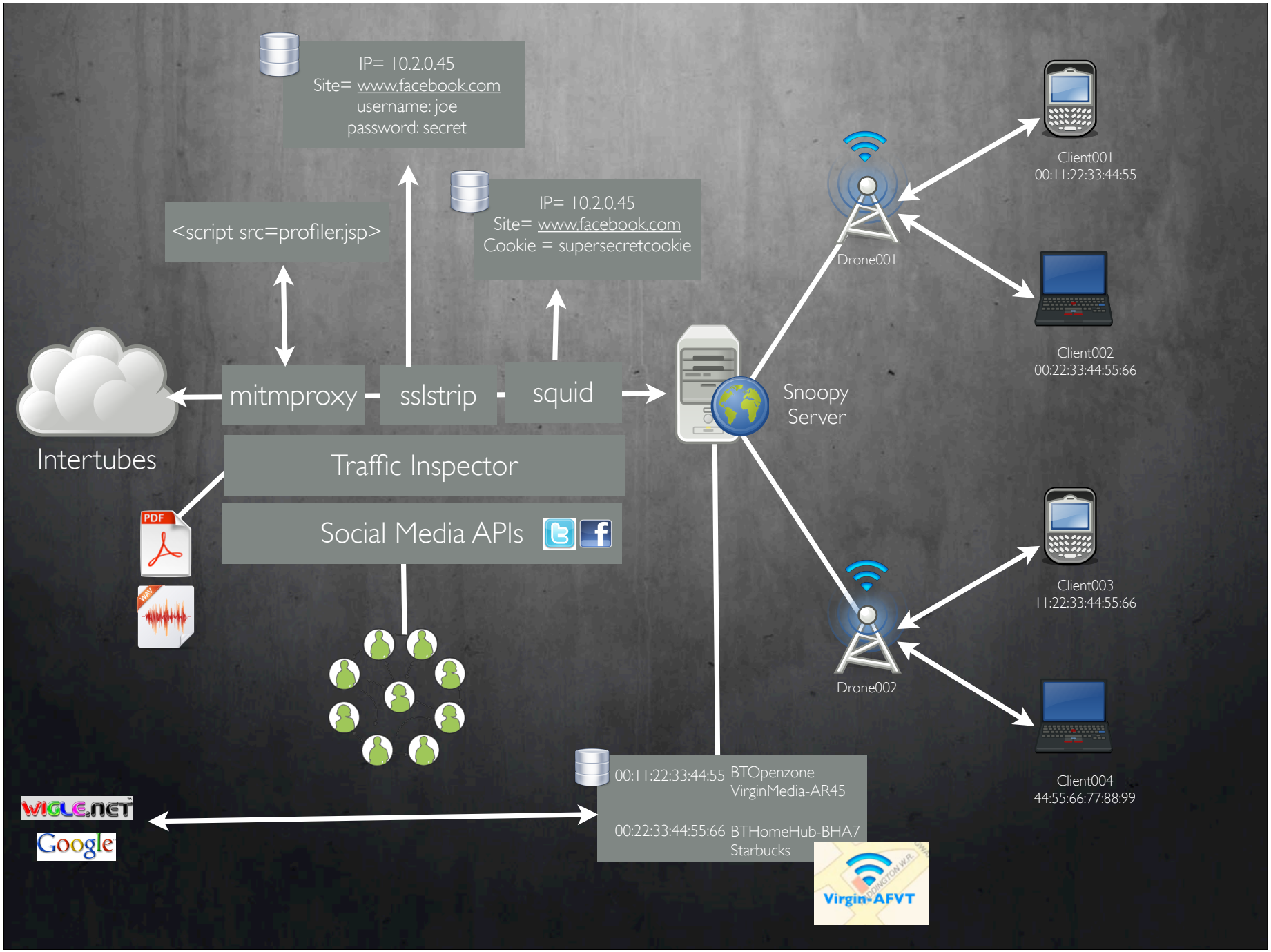
2. Active Linking

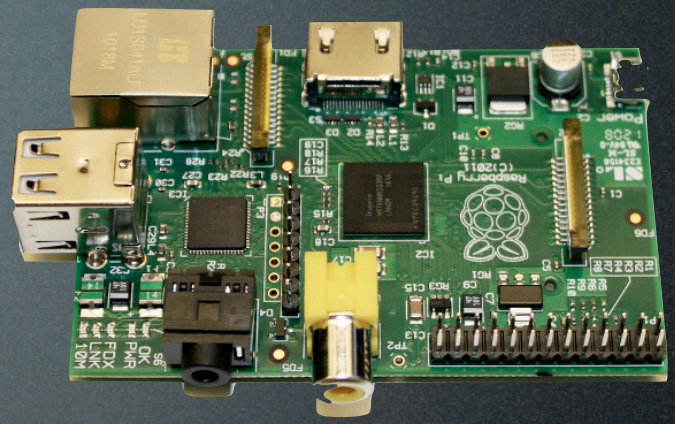
BTHomeHub-AFV1, are you there?
Starbucks, are you there?
Virgin-AFVT, are you there?
Is anyone out there?

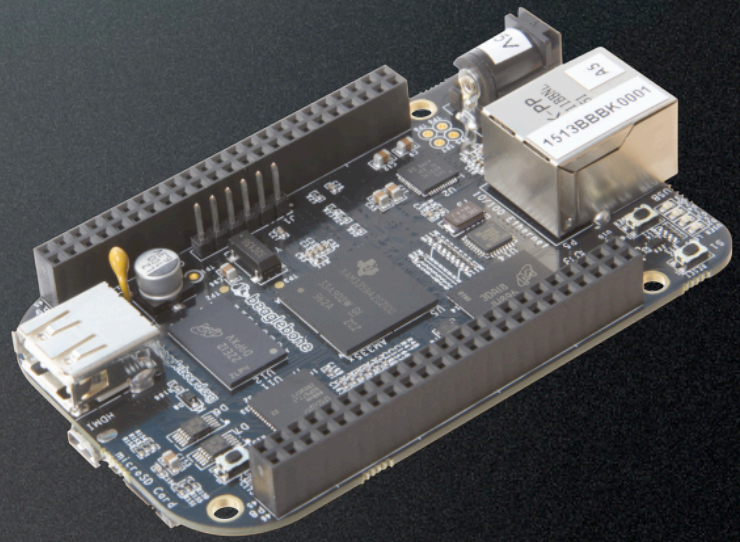


Hey iPhone! It's me, Starbucks!

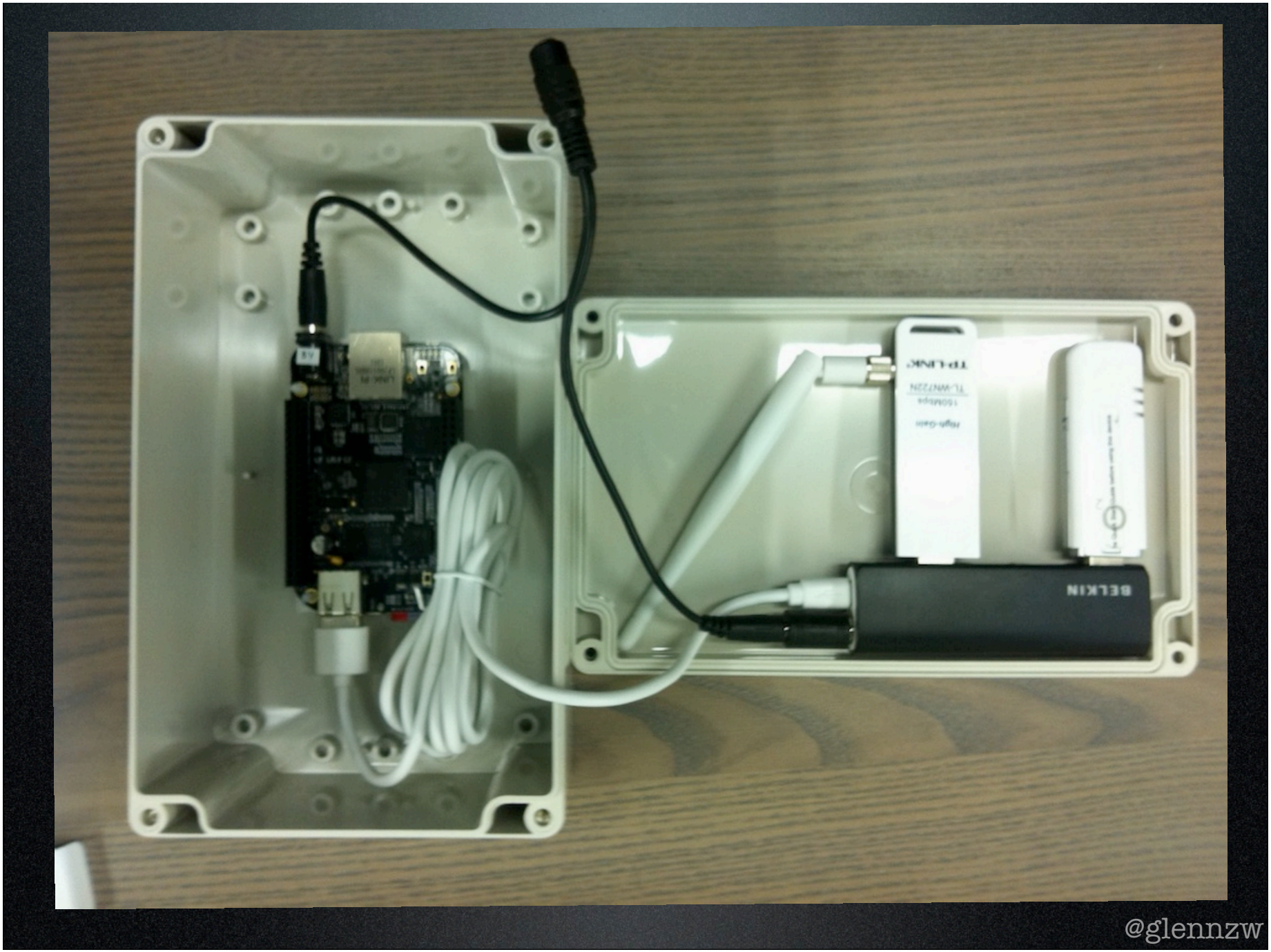
98:03:ab:32:11:33


IP= 10.2.0.45
Site= www.facebook.com
username: joe
password: secret
<script src=profiler.jsp>
IP= 10.2.0.45
Site= www.facebook.com
Cookie = supersecretcookie
Client001
00:11:22:33:44:55
Drone001
Client002
00:22:33:44:55:66
mitmproxy
sslstrip
squid
Snoopy
Server
Intertubes
Traffic Inspector
Social Media APIs
PDF
WAV
Client003
11:22:33:44:55:66
Drone002
Client004
44:55:66:77:88:99
00:11:22:33:44:55 BTOpenzone
VirginMedia-AR45
00:22:33:44:55:66 BTHomeHub-BHA7
Starbucks
WIGLE.NET
Google
Virgin-AFVT





@glennzw


TP-LINK
TL-WN722N
150Mbps
High-Gain
BELKIN
@glennzw

@glennzw


MALTEGO
RADIUM
PATERVA

Scenarios

Conference	Unique Devices	Number of Attendees	Device Per Person
BlackHatVegas ‘12	4778	6500	0.74
ITWeb ‘12	1106	400	2.77
44CON ‘12	969	350	2.77
BlackHatEU ‘13	681	607	1.12
Securitay ‘13	375	100	3.75
BSides ‘13	208	474	0.44
Hackito ‘13	309	400	0.77
CERT Poland ‘13	598	500	1.2
ZeroNights ‘13	507	600	1.18
BlackHat Brazil ’13	719	?	
BlackHat Asia ’14	719	?	


sensepost
glenn@sensepost.com
jobs@sensepost.com
http://research.sensepost.com/
@glennzw