



Open Source Intelligence

Do you really know what data you're leaking?



Oh Hai!

David Busby
Senior Site Reliability Engineer, DevSecOps @ Quip
CISSP



@icelus



@oneiroi





Precepts

What this talk is, and what you should take away from the talk

Precepts

Rules:

1. Exercise some Wheaton's law (don't be a dick!)
2. Don't use what you learn here to stalk / harass / other abusive behaviour (see rule 1)
3. Unsure? see rule 1.
4. The birds work for the bourgeoisie
5. See rule 1.





Precepts

Rules of the ...

1. This is not a “how-to” for gathering information on an individual or organization.
2. This is not a “how-to” on how to become a creepy net stalker
 - a. **Seriously don't**
3. This is a small insight into what information you may not be aware of disclosing in your own life.
4. This talk covers how this information can be misused with real world examples.
5. This talk concludes with how this information can be used for good.
6. This talk highlights how analytical / critical thinking can be applied to discover connections between openly available information.



Terminology

Some of the terms I'm likely to discuss during this talk;

1. OSINT - Open Source Intelligence
2. OPSEC - Operational Security
3. PERSEC - Personal Security
4. COMSEC - Communication Security
5. INFOSEC - Information Security



But why?

Because, sometimes that little bit of data you were unaware of, could be a bad thing ...

Homicide Offender vs. Victim demographics

View by: **#** %

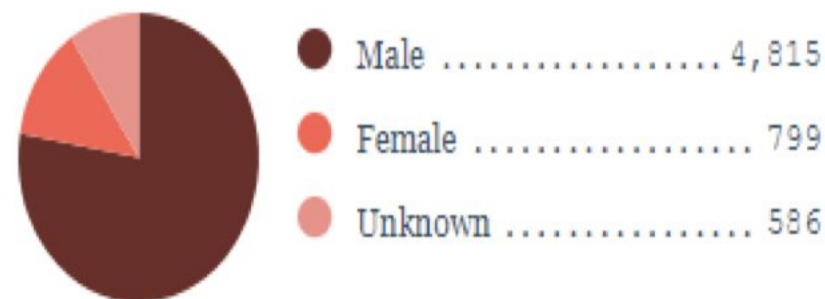
Sex

Race

Ethnicity

Age

Offender Sex

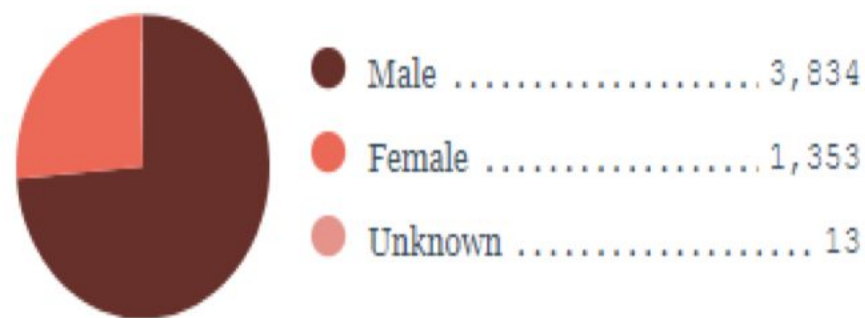


Offenders w/ reported sex

6,200

 Download

Victim Sex



Victims w/ reported sex

5,200

 Download



But why?

US Statistics of violent crimes are alarming, and perpetrators of these crimes are only learning how to use available OSInt information to carry out these crimes ...

Homicides:

77.7% Male offender
12.8% Female offence
73.7% Male victim
26% Female Victim

Sexual Assault

92.5% Male offender
4.2% Female offender
10.7% Male victim
89.71% Female victim



But why?

Because protection of human life and wellbeing should be everyone's first priority!

Inc, protecting quality of life.

Protection from abuse, fraud, malactors, malevolent behaviours, threats and threat actors.

bUt ThE sTaTs ArE blaSeD ...





Meanwhile, in the real world

There are examples of where data exposure has lead to very concerning issues ...

And we're going to cover some of these, and cover the transition between inference in the real world and data available.



Stalker used corneal reflection to
locate female singer ...



Data exposure, is not just digital

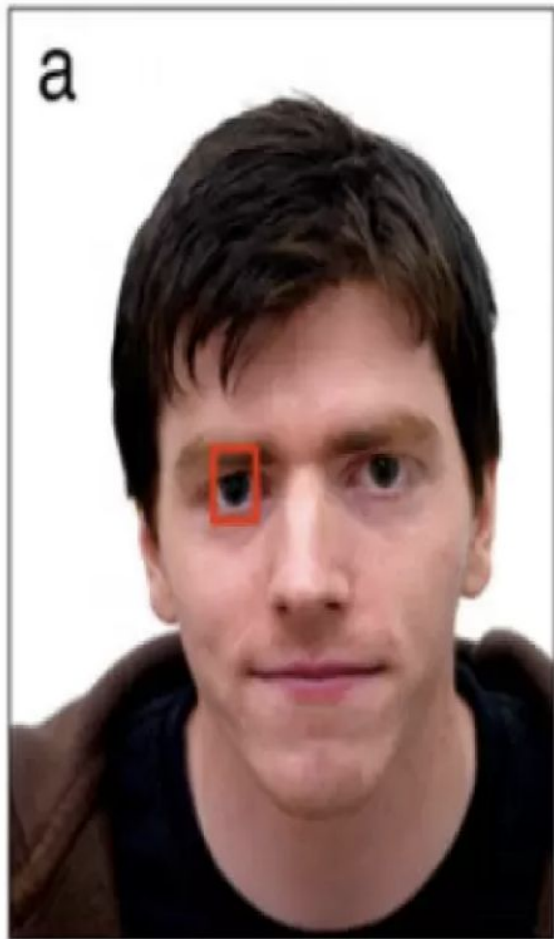
- [BBC article](#): Stalker 'found Japanese singer through reflection in her eyes' (October 2019)
- Corneal reflection allowed identification of a train station.
 - Stalker then used google street view to further confirm angle and approximate distance when the photo was taken.
- Such reflections were a noted concern in a [2013 peer reviewed academic research paper](#).

A close-up photograph of a man with light brown hair, wearing a dark suit jacket over a blue shirt. He is holding a pair of thin-rimmed glasses up to his eyes with both hands, looking directly and intensely at the camera. The background is a plain, light gray.

ZOOM IN...

ENHANCE.

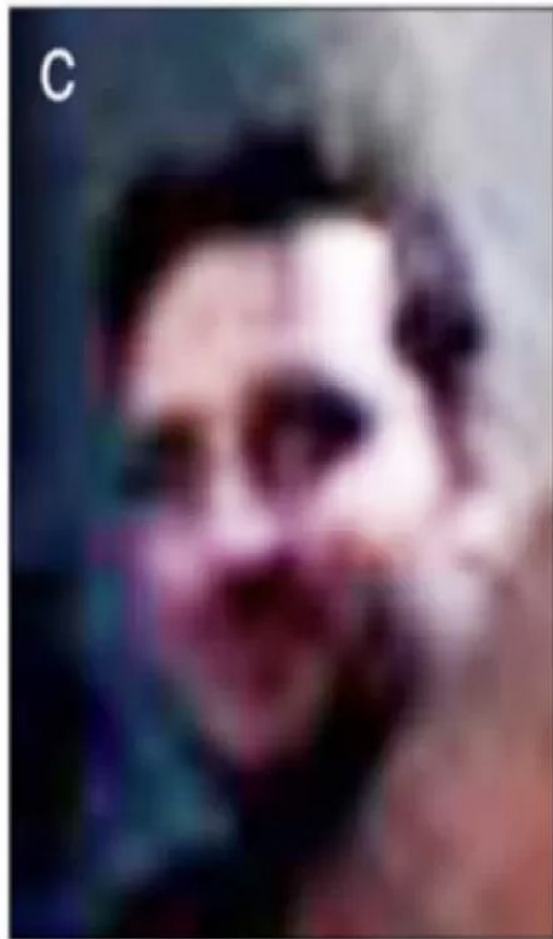
a



b



c





It is also digital ...

- Extensible Image Format (EXIF) data is embedded into every single photo you take on your “smart device”.
- Examples:
 - GPS (time, elevation, lat:long, direction facing, etc)
 - Date & time
 - Device type
 - And more

```
exiftool /Volumes/JetDrive/IMG_20160707_192748.jpg | egrep -i 'GPS|Software|Model'
```

GPS Date Stamp	: 2016:07:07
GPS Altitude Ref	: Unknown (2)
GPS Longitude Ref	: West
GPS Latitude Ref	: North
GPS Time Stamp	: 18:20:38
Camera Model Name	: ONEPLUS A3003
Software	: OnePlus3-user 6.0.1 MMB29M 4 dev-keys
GPS Altitude	: 0 m Above Sea Level
GPS Date/Time	: 2016:07:07 18:20:38Z
GPS Latitude	: 32 deg 58' 3.12" N
GPS Longitude	: 12 deg 40' 43.88" W
GPS Position	: 62 deg 18' 7.61" N, 2 deg 40' 43.88" W



It's not limited to images either ...

- Let's look at 802.x and what else you may be leaking without being aware!
- Bluetooth
 - Find a bluetooth device with centimeter accuracy written into the bluetooth spec...
 - [Bluetooth Received Signal Strength Indication \(RSSI\)](#)
 - Used in commercial products e.g. Tile, Trackr.
 - Used by marketing agencies to track population density of a given area.



It's not limited to images either ...

- WiFi
 - WiFi beacons broadcast (in the clear) every single WiFi AP your device has ever connected to
 - WiFi BSSID's
 - WiFi data is collected by Gov agencies such as T.F.L.



Wi-Fi data collection

We collect Wi-Fi connection data at this station to better understand journey patterns and improve our services

We will not identify individuals

You can opt out by turning off your device's Wi-Fi

For more information visit tfl.gov.uk/wifi-data-collection



**A little knowledge can be a
dangerous thing ...**



“I’m here to collect your council tax arrears on behalf of \$local_council ...”

*presents “id”

That ID is _actually_ an O.A.P Bus pass, with red electrical tape.

I swear I’ve seen this somewhere before



Leeloo Dallas. Multi-pass.



OSInt _can_ be used for good!

It's not all doom, gloom, and creepy stalking ... it can be #OSIntforgood

I highly recommend you look at [tracelabs](https://www.tracelabs.org/) (<https://www.tracelabs.org/>) if you want to learn more.

Trace Labs run “Searchparty” CTF events, maintain VM images for download to conduct OSInt research.

Those search parties, allow participants to submit “flags” to contribute to build an evidence file to help locate real missing person(s).

This can be looking at image artefacts, reflections, unique interesting items in the background, etc.

To simply searching for the \$name, \$location and the \$social_media profile of the missing person.



OSInt _can_ be used for good!

#OSIntforgood

You may be asking why?

You contribute towards a Capture the flag event, and the organizers gain crowd sourced perspectives of intelligence to build a case file to contribute towards real-world missing persons cases.



In closing

Like any piece of information, data, or software, **how** you use that which you know is key.

Analytical / critical thinking is all that's needed to make real world impacts to help families of missing persons (and you get the practise and grow your skillset).



Questions ?



Thank You!