

Tracking a Killer

Dan Kolb
Grow and Tell
January, 2018

Inspiration

<https://www.youtube.com/watch?v=hkDD03yeLnU>



Transcript

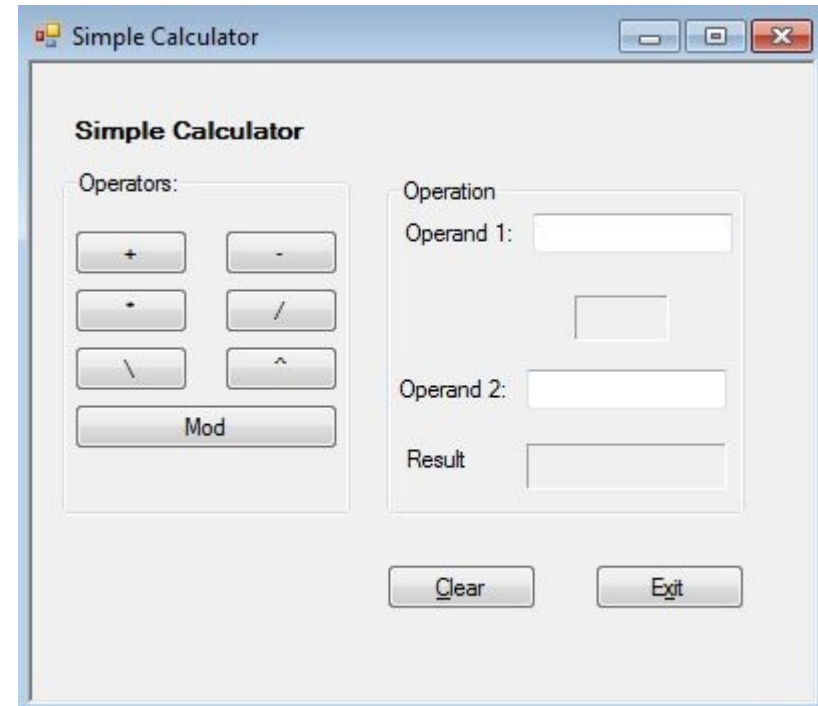
Mac Taylor: “For weeks I’ve been investigating the cabbie killer murders with a certain morbid fascination”

Stella Bonasera: “This is in real time”

Lindsay Monroe: “I’ll create a GUI Interface using Visual Basic, see if I can track an IP Address”

Visual Basic?

- **Event driven programming language from Microsoft**
- **Incredibly pervasive**
- **Visual Basic for Applications**
 - macros in Excel/Word



Interface - Electronjs

- **HTML, CSS, JavaScript**
- **Chromium and Nodejs in single runtime**
 - Nodejs derived from Chromium's JavaScript engine
- **You're probably using it**
 - Github Desktop, Atom, Visual Studio Code, Slack...

Location Information?

- **GeoIP**

- Open source information (LEGACY from MaxMind)
 - <https://dev.maxmind.com/geoip/legacy/downloadable/>

- **Whois Information**

- ICANN Registry Information

- ```
$ whois rackspace.com | grep Registrant
Registry Registrant ID:
Registrant Name: Domain Admin
Registrant Organization: Rackspace US, Inc.
Registrant Street: 1 Fanatical Place
Registrant City: San Antonio
Registrant State/Province: TX
Registrant Postal Code: 78218
Registrant Country: US
Registrant Phone: +1.2103124000
Registrant Phone Ext:
Registrant Fax: +1.2103124848
Registrant Fax Ext:
Registrant Email: domains@rackspace.com
```

# Location Information??

- **Google**

- Collects WAP information with Street View cars
  - <https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data>
- Control Access Point Inclusion- determines location from WAPS
  - <https://support.google.com/maps/answer/1725632?hl=en>
- Android – Scanning WAPs **REQUIRES** ACCESS\_\*\_LOCATION permissions
  - [https://developer.android.com/reference/android/net/wifi/WifiManager.html#getScanResults\(\)](https://developer.android.com/reference/android/net/wifi/WifiManager.html#getScanResults())
  - Protection level: dangerous
    - Dangerous permissions cover areas where the app wants data or resources that involve the user's private information, or could potentially affect the user's stored data or the operation of other apps. For example, the ability to read the user's contacts is a dangerous permission. If an app declares that it needs a dangerous permission, the user has to explicitly grant the permission to the app. Until the user approves the permission, your app cannot provide functionality that depends on that permission.
  - <https://developer.android.com/guide/topics/permissions/overview#normal-dangerous>

# Electronjs files

- **Package.json**
  - Package information
- **Index.html**
  - “front page” of application
- **Main.js**
  - Application “Start up”
- **Render.js**
  - Nodejs functions
- **Styles.css**
  - Cascading StyleSheets information (display)



# Demo

# Results

Killer IP Tracker

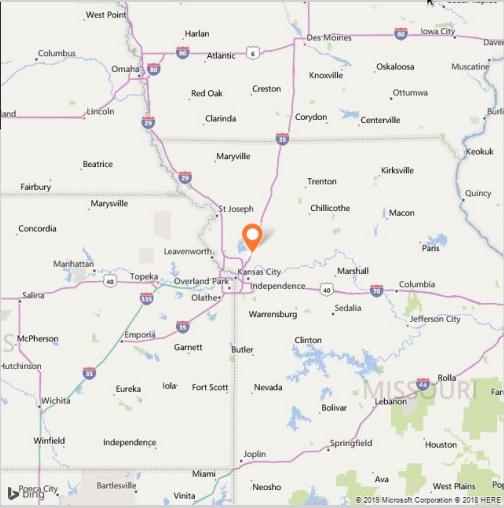
File Edit View Window Help

### GUI in Electron to Track Killer

.....  
Track IP

IP Location found

| GEO IP Information |                  |
|--------------------|------------------|
| Country            | US               |
| City               | Kearney          |
| Region             | MO               |
| Coordinates        | 39.3652,-94.3621 |
| ZipCode            | undefined        |



Killer IP Tracker

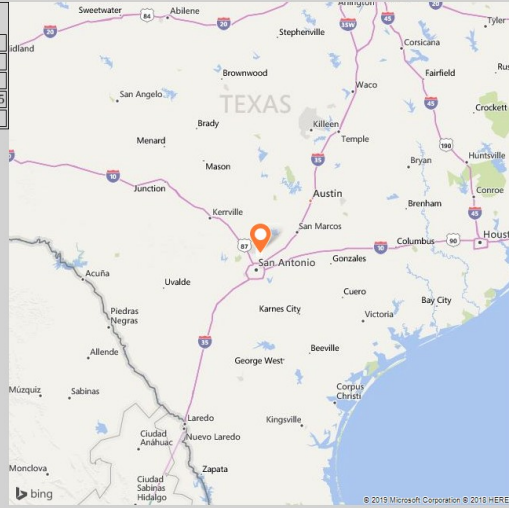
File Edit View Window Help

### GUI in Electron to Track Killer

.....  
Track IP

IP Location found

| GEO IP Information |                  |
|--------------------|------------------|
| Country            | US               |
| City               | San Antonio      |
| Region             | TX               |
| Coordinates        | 29.6283,-98.4445 |
| ZipCode            | undefined        |



# How did TV get it wrong?

- **Issues with IP address?**

- GeoIP not accurate to address
- VPN, TOR, SSH...
- NAT (Network Address Translation)

- **Get IP address**

- Contact IP address owner to track
  - Repeat until source found
    - (MAC address easily spoofed)

- **Correlate Cookie/Session/Account information**

- Traced phone number registered to account to another user that registered that phone number at that college
- <https://www.mcall.com/news/police/mc-nws-lafayette-bomb-threat-bail-hearing-20181218-story.html>

# What did we learn?

- **TV is wrong**
- **You don't want to watch TV shows that involve technology with Dan**