Solving Crimes with Wireless GeoFencing and Multi-Zone Correlation Analytics

Gleb Esman, Senior Product Manager, Fraud Analytics and Research, Splunk.

gesman@splunk.com
https://www.linkedin.com/in/glebesman/
During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.
Listen to Your Data
Special thanks to:

ALFTELE SYSTEMS LTD
FORWARD THINKING SECURITY SERVICES AND TECHNOLOGIES

www.ALFTELE.com

• 2,4,8,12,16-Core Intel x86 CPU boards
• Support for World LTE access and data collection
• Up-to x16 dual-chain 802.11 a/b/g/n/ac USB/PCIe radios
• External battery power and backup
Special thanks to:

Scott Haskell
Principal Sales Engineer
Splunk, Inc.

https://splunkbase.splunk.com/app/3124/
Gleb Esman, Bio

gesman@splunk.com    linkedin.com/in/glebesman

Early career:
Anti-virus, anti-malware research and development:
Development of advanced methods and heuristic virtual machines to detect known and unknown computer viruses and malware.

Architecting and engineering management work in space of e-commerce, cryptocurrency, payment processing and digital information management solutions.
Data analytics and Fraud Detection solutions for financial services.

Since 2015: Sr. Product Manager, Fraud Analytics and Research at Splunk, San Francisco

Author of several Patent Applications for fraud detection with Deep Learning.
Agenda

• Definitions
• Use cases for Wireless GeoFencing
• Data:
  • Sources/Devices
  • Capture
  • Conversion
  • Ingestion
• Creating Splunk Application, step by step
• Data Visualizations and Maps+
• Solving Use Cases
• Completed App / Demo
Definitions

• **Wireless Forensics**  
  A process of collecting and analyzing data from wireless devices.

• **Geo-Fencing**  
  A process of defining geographical boundaries (zones)

• **Splunk**  
  is ...
Splunk: The Engine for Machine Data

Splunk makes software for searching, monitoring and analyzing machine generated big data

- Ingest in Real time
- Multiple formats
- Schema on the fly
- Scalable
- Fast
- Opened, customizable

- Data Science, Machine Learning
- SPL, API, SDK, Apps, Splunkbase
- Fast Time to Value
- Non-Intrusive
- “Google for Machine Data”
Use Cases

Pinpoint suspect or criminal using Wi-Fi signal footprint

- Crime 1: **arson** at location A at time_1, **arson** at location B at time_2
- Crime 2: **kidnapping** at location X at time_3, **kidnapping** at location Y at time_4
- Crime 3: **robbery** at location K at time_5, **robbery** at location L at time_6, **robbery** at location M at time_7

Questions:

- Who are possible suspects? (full list)
- Who are the most probable suspects? (sorted list – better)
Use Cases
Pinpoint suspect or criminal using Wi-Fi signal footprint

**Probe requests** are an 802.11 WIFI packet type that function to automatically connect network devices to the wireless access points (APs) that they have previously associated with. Whenever a phone, computer, or other networked device has Wi-Fi enabled, but is not connected to a network, it is constantly "probing"; openly broadcasting the network names (SSIDs) of previously connected Access Points. Because wireless access points have unique and often personal network names, it is easy to identify the device owner by recognizing the names of networks they frequently connect to.

By monitoring wi-fi spectrum for signals emitted by wireless devices we can match crime scenes and times to wireless devices owned by possible suspects.
Use Cases

Pinpoint suspect or criminal using Wi-Fi signal footprint

- Crime 1: *arson* at location A at time_1, *arson* at location B at time_2
- Crime 2: *kidnapping* at location X at time_3, *kidnapping* at location Y at time_4
- Crime 3: *robbery* at location K at time_5, *robbery* at location L at time_6, *robbery* at location M at time_7

Will build solution that:

1. Sort WiFi signal sources by probability of being suspect - taking GPS coordinates, time and signal strength into account to calculate probability.

2. Visually define multiple GeoFence zones directly on a map and have system to find potential suspects automatically.
## Probe Request / Response Data

Pinpoint suspect or criminal using Wi-Fi signal footprint

<table>
<thead>
<tr>
<th>frame_number</th>
<th>sender_moc</th>
<th>sender_moc_vendor_full</th>
<th>receiver_moc</th>
<th>receiver_moc_vendor_full</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>13925</td>
<td>34:12:35:AF:0D:CB</td>
<td>Huawei Technologies Co., Ltd</td>
<td>B4:31:30:AB:17:FA</td>
<td>XIAMDI Electronics,CO., LTD</td>
<td>Probe Response, WM=2378, FN=0, Flags=........, C=BI+100, SSDP=gigabyte-DonJuan</td>
</tr>
<tr>
<td>13918</td>
<td>02:0D:06:34:6C</td>
<td>Compal Broadband Networks, Inc.</td>
<td>B4:31:30:AB:17:FA</td>
<td>XIAMDI Electronics,CO., LTD</td>
<td>Probe Response, WM=3698, FN=0, Flags=........, C=BI+100, SSDP=USCO3DF467</td>
</tr>
<tr>
<td>13914</td>
<td>1C:66:30:00:00:02</td>
<td>Arcadyan Technology Corporation</td>
<td>B4:31:30:AB:17:FA</td>
<td>XIAMDI Electronics,CO., LTD</td>
<td>Probe Response, WM=3599, FN=0, Flags=........, C=BI+100, SSDP=WLAN-2D335</td>
</tr>
<tr>
<td>12600</td>
<td>06:02:01:FC:1F:1F</td>
<td>Zyxel Communications Corporation</td>
<td>DA:19:19:AB:12:3C</td>
<td>Google, Inc.</td>
<td>Probe Response, WM=3620, FN=0, Flags=........, C=BI+100, SSDP=WLNKINTER_NEX</td>
</tr>
<tr>
<td>12508</td>
<td>08:00:00:ED:DD:44</td>
<td>Sercom Corporation.</td>
<td>00:13:0C:CB:3E:34</td>
<td>Intel Corporate</td>
<td>Probe Response, WM=3429, FN=0, Flags=........, C=BI+100, SSDP=EasyBox-176282</td>
</tr>
<tr>
<td>12517</td>
<td>00:24:AF:04:12:10</td>
<td>Buffalo Inc</td>
<td>00:13:0C:CB:3E:34</td>
<td>Intel Corporate</td>
<td>Probe Response, WM=3353, FN=0, Flags=........, C=BI+100, SSDP=SSQL</td>
</tr>
<tr>
<td>12532</td>
<td>00:09:4F:95:0D:3D</td>
<td>elmgz GmbH &amp; Co. KG</td>
<td>00:13:0C:CB:3E:34</td>
<td>Intel Corporate</td>
<td>Probe Response, WM=3756, FN=0, Flags=........, C=BI+100, SSDP=RAE</td>
</tr>
<tr>
<td>12542</td>
<td>08:04:26:30:05:08</td>
<td>TP-Link Technologies Co., Ltd.</td>
<td>00:13:0C:CB:3E:34</td>
<td>Intel Corporate</td>
<td>Probe Response, WM=3409, FN=0, Flags=........, C=BI+100, SSDP=Dialite in wland</td>
</tr>
<tr>
<td>12341</td>
<td>08:EC:AC:34:56:59</td>
<td>Zyxel Communications Corporation</td>
<td>00:28:F8:45:2F:2C</td>
<td>Intel Corporate</td>
<td>Probe Response, WM=2251, FN=0, Flags=........, C=BI+100, SSDP=3Fi-CID-5G</td>
</tr>
<tr>
<td>11606</td>
<td>08:EC:6A:0A:CA:9E</td>
<td>Meru Networks Inc</td>
<td>C8:3C:85:53:09:5F</td>
<td>Apple, Inc.</td>
<td>Probe Response, WM=1835, FN=0, Flags=........, C=BI+100, SSDP=Merlion Gaeste</td>
</tr>
<tr>
<td>11618</td>
<td>0B:27:5D:07:2E:37</td>
<td>Raspberry Pi Foundation</td>
<td>C6:93:01:CD:AB:CB</td>
<td>Samsung Electronics Co., Ltd</td>
<td>Probe Response, WM=1764, FN=0, Flags=........, C=BI+100, SSDP=Okmire-01</td>
</tr>
<tr>
<td>11305</td>
<td>0C:5E:0D:08:26:82</td>
<td>Routerboard.com</td>
<td>E4:04:39:97:3B:AF</td>
<td>TomTom Software Ltd</td>
<td>Probe Response, WM=2357, FN=0, Flags=........, C=BI+100, SSDP=SDtins-IB-2G</td>
</tr>
</tbody>
</table>
Law Enforcement requested data from Google
Tracing unknown criminal by phone device signal data

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information that is maintained on computer servers controlled by Google, Inc. ("Google"), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A to the proposed warrant, which consists of Google location data associated with a particular specified location at a particular time, as specified in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google...
Correlating Different Zones and times together
Tracing unknown criminal by phone device signal data

They were looking for phones Google had recorded around the bombing locations.

Date/Time: From 7:00 p.m. on March 1, 2018 until 7:00 a.m. on March 2, 2018
Geographical box with the following 4 (four) latitude and longitude coordinates of 1112
Haverford Drive, Austin, Texas 78753:
1) 30.405511, -97.650988
2) 30.407107, -97.649445
3) 30.405590, -97.646322
4) 30.404329, -97.647983

Credits:
Building Geo Fencing Analytical Application

Step by Step Process

1. Download Splunk. [www.splunk.com](http://www.splunk.com)
   • Free, fully featured enterprise version. Mac / Linux / Windows. Local or on-cloud. 500MB/day free license. 50GB/day free developer license.
2. Create new app (application).
3. Create index (database for specific data) for Wi-Fi capture data
4. Capture data / .PCAP files
5. Convert data to .CSV format
6. Ingest data into Splunk
7. Build Analytical Layer logic - Dashboards / SPL Queries
#2-3: Creating new Splunk App, Creating Index

- Menu -> Apps -> Manage Apps -> [Create App] -> fill in info ... -> [Save]
- Settings -> Indexes -> New Index -> Index Name = “dc27_pcap” -> [Save]
#4: Capture Data – Hardware Devices

**Poor man solution:**

**Real man solution:** ALFTEL AirBud Wireless Monitoring Platform

Use: https://wireshark.org
#4-5: Capture and Converting Data to CSV format

- Captured Data is in binary format: typically `.PCAP*` files
- These need to be converted to pipe-delimited `.CSV` for analysis: `PCAP*` -> CSV
- Use `tshark` utility to convert files:

```
```
#5: Converted Data – Resulted Pipe-Delimited File

```bash
[root@localhost PCAP]# head -n 25 wifi_data.csv

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;Jul 25, 2019 04:30:07.662129000 PST&quot;</td>
<td>0.000000000</td>
<td>'1'</td>
<td>'ppi:ppi_gps:wlan'</td>
<td>'277'</td>
<td>'32:d3:2d:03:50:aa'</td>
<td>'32:d3:2d:03:50:aa'</td>
<td>'ff:ff:ff:ff:ff'</td>
<td>'ff:ff:ff:ff'</td>
<td>'32:d3:2d:03:50:aa'</td>
<td>0</td>
<td>8</td>
<td>0x00000000</td>
<td>0</td>
<td>8</td>
<td>0x00000000</td>
<td>48.4996146</td>
<td>9.2045593</td>
<td>377.636</td>
<td>0x0053494b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;Jul 25, 2019 04:30:07.611257000 PST&quot;</td>
<td>-0.050872000</td>
<td>'2'</td>
<td>'ppi:ppi_gps:wlan'</td>
<td>'308'</td>
<td>'30:d3:2d:03:50:aa'</td>
<td>'30:d3:2d:03:50:aa'</td>
<td>'ff:ff:ff:ff:ff'</td>
<td>'ff:ff:ff:ff'</td>
<td>'30:d3:2d:03:50:aa'</td>
<td>0</td>
<td>8</td>
<td>0x00000000</td>
<td>0</td>
<td>8</td>
<td>0x00000000</td>
<td>48.4996146</td>
<td>9.2045593</td>
<td>377.636</td>
<td>0x0053494b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;Jul 25, 2019 04:30:07.668295000 PST&quot;</td>
<td>0.057038000</td>
<td>'3'</td>
<td>'ppi:ppi_gps:wlan'</td>
<td>'321'</td>
<td>'bc:05:43:a5:f2:2a'</td>
<td>'bc:05:43:a5:f2:2a'</td>
<td>'ff:ff:ff:ff:ff'</td>
<td>'ff:ff:ff:ff'</td>
<td>'bc:05:43:a5:f2:2a'</td>
<td>0</td>
<td>8</td>
<td>0x00000000</td>
<td>0</td>
<td>8</td>
<td>0x00000000</td>
<td>48.4996146</td>
<td>9.2045593</td>
<td>377.636</td>
<td>0x0053494b</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

**Note:** The formatted data captures the timestamp, source, destination, and various wireless networking attributes. The data is timestamped with the format `"Jul 25, 2019 04:30:07.662129000 PST"`, indicating the time戳 in PST, and includes fields such as `wlan.sa_resolved`, `wlan.ta_resolved`, and `wlan.ra_resolved` among others.
Create **pcap** sourcetype telling Splunk how to parse fields from **wifi_data.csv**

- Create file (or append to existing one):
  
  `/opt/splunk/etc/apps/defcon27_geofencing/local/props.conf`

  The following contents:

  ```
  [pcap]
  BREAK_ONLY_BEFORE_DATE =
  DATETIME_CONFIG =
  FIELD_DELIMITER = |
  FIELD_QUOTE = '
  INDEXED_EXTRACTIONS = csv
  KV_MODE = none
  LINE_BREAKER = ([\r\n]+)
  NO_BINARY_CHECK = true
  SHOULD_LINEMERGE = false
  category = Structured
  description = PCAP file converted to CSV
  disabled = false
  pulldown_type = true
  FIELDALIAS-all-aliases = ws_col_Protocol AS Protocol
                      - ws_col_Length as Length
                      - ws_col_Source AS Source
                      - ws_col_Destination AS Destination
                      - ws_col_Info AS Info
                      - ppi_gps_lat AS lat
                      - ppi_gps_lon AS lon
                      - ppi_gps_alt AS alt
  TIMESTAMP_FIELDS = frame_time
  ```
#6: Ingest Data in Splunk

Update permissions and restart Splunk to make it recognize new sourcetype:

```
[root@localhost ~]# chown -Rf splunk:splunk /opt/splunk/etc/apps/defcon27_geofencing/
[root@localhost ~]# /opt/splunk/bin/splunk restart
```

- Adding data to index. After restart:
  - Settings -> [Add Data] -> [Upload] -> [Select File] -> navigate to wifi_data.csv
  - [Next] -> Set Sourcetype = “pcap” -> [Next] -> Index = dc27_pcap ->
  - [Review] -> [Submit]

Adding data file to Splunk index:
#6: Ingest Data in Splunk

Testing ingest - searching for data

SPL query:
```
index=dc27_pcap | table _time frame_number wlan_sa wlan_ta wlan_ssid wlan_supported_rates Info
```
#6: Ingest Data in Splunk

Building summary index

Summary index contains “clean”, deduplicated version of data with properly parsed, “fixed”, substituted or extracted fields, enriched from other sources (MAC-to-vendor names)

Ensure sender_name contains valid data:

```
| eval sender_name=replace(coalesce(wlan_sa_resolved, wlan_ta_resolved, Source), "(\.*\[_\._]*\)$", "\1")
```

Enrich MAC address with vendor/manufacturer information:

```
| lookup mac_vendor_lookup mac AS sender_mac, OUTPUT vendor AS sender_mac_vendor, vendor_full AS sender_mac_vendor_full
```

Ensure access point name does not contain invalid characters:

```
| eval ap_name2=substr(replace(ap_name, "[^\w\x20-\x7e\w-]++", "?"), 1, 50)
```
#6: Ingest Data in Splunk

### Building summary index

- **Create summary index:**
  
  Settings -> Indexes -> New index -> Index Name = “pcap_summ” -> [Save]

- **Execute SPL summary index generating search from Splunk ad-hoc search window:**

```splunk
index=dc27_pcap
| eval SRC=source, ST=sourcetype, IDX=index
| fields - `infields`
| eval sender_mac=upper(coalesce(wlan_sa, wlan_ta, wlan_bssid))
| eval sender_name=replace(coalesce(wlan_sa_resolved, wlan_ta_resolved, Source), ".*\[\^\]\$", "\1")
| eval sender_name2=substr(replace(sender_name, "^[\^\x20-\x7e]\[\^\]\$", "\1")
| eval sender_name_full=trim(coalesce(if(sender_name2==sender_mac, null(), sender_name2), "\1") as sender_mac, "\1") as sender_mac
| lookup vendor_mac_lookup mac AS sender_mac, OUTPUT vendor AS sender_mac_vendor, vendor_full AS sender_mac_vendor_full

| eval receiver_mac=upper(coalesce(wlan_da, wlan_ra))
| eval receiver_name=replace(coalesce(wlan_da_resolved, wlan_ra_resolved), ".*\[\^\]\$", "\1")
| eval receiver_name2=substr(replace(receiver_name, "^[\^\x20-\x7e]\[\^\]\$", "\1")
| eval receiver_name_full=trim(coalesce(if(receiver_name2==receiver_mac, null(), receiver_name2), "\1") as receiver_mac, "\1") as receiver_mac
| lookup vendor_mac_lookup mac AS receiver_mac, OUTPUT vendor AS receiver_mac_vendor, vendor_full AS receiver_mac_vendor_full

| eval ap_mac=if(wlan_bssid="ff:ff:ff:ff:ff:ff", null(), upper(wlan_bssid))
| eval ap_name=if(wlan_ssid==null(), upper(wlan_ssid))
| eval ap_name2=substr(replace(ap_name, "^[\^\x20-\x7e]\[\^\]\$", "\1")
| eval ap_name_full=trim(coalesce(if(ap_name2==ap_name, null(), ap_name2), "\1") as ap_name, "\1") as ap_name
| lookup vendor_ap_lookup mac AS ap_mac, OUTPUT vendor AS ap_mac_vendor, vendor_full AS ap_mac_vendor_full
```

| fields - _raw |
| collect index=pcap_summ |
#6: Ingest Data in Splunk

Building accelerated data model: pcap

- Create data model:
  Settings -> Data Models -> Tile = “Pcap”, ID=“pcap”, App=“DefCon27 GeoFencing”, [Create]
- Settings -> Data Models -> Pcap -> [Add Dataset] -> “Root Event”, Dataset Name = “pcap”, Constraints = “index=pcap_summ”, [Save]
- [Add Field], Auto-Extracted, [x] select all fields, [Save]
- NOTE: Download app contains all settings for data model already.
#7: Build Analytical Layer logic

Splunk Dashboards

1. When you build Splunk app – 90% of dashboards logic, code and queries are contained in pure XML. You may customize it with .CSS and .JS

2. 90% of everything could be built visually via Web Interface, no low level coding required

3. 90% of all dashboards could be build as following:
   1. Ad-Hoc query: `index=pcap_sum | table _time source_mac destination_mac`
   2. Visualization Tab – select appropriate visual data representation and options
   3. Save As “Dashboard Panel” – new or add to existing one
#7: Build Analytical Layer logic

Build “Top Protocols” Dashboards

1. When you build Splunk app – 90% of dashboards logic, code and queries are contained in pure XML. You may customize it with .CSS and .JS

2. 90% of everything could be built visually via Web Interface, no low level coding required

3. 90% of all dashboards could be build as following:
   1. Ad-Hoc query: `index=pcap_sum | table _time source_mac destination_mac`
   2. Visualization Tab – select appropriate visual data representation and options
   3. Save As “Dashboard Panel” – new or add to existing one
#7: Build Analytical Layer logic

Visualize “Wi-fi Protocols activity over time” on a dashboard

Run SPL data query to get results

Select desired Visualization
#7: Build Analytical Layer logic

Visualize “Wi-fi Protocols activity over time” on a dashboard

Save results as Dashboard

Customize Dashboard options and look
#7: Build Analytical Layer logic

DEMO
Splunk Maps+ App
Adding customizable interactive mapping capabilities

Selecting Maps+ as a Viz
Splunk Maps+ App
Example of Maps+

Mapping criminal activity in Chicago

Github repo: https://github.com/sghaskell/maps-plus
Adding WiFi Signal Sources on a Map

1. Input:
   - 2 different sources (s1.pcap, s2.pcap) of signal gathered by ALFTEL WiFi monitoring devices
   - ALFTEL devices were installed in moving cars.

2. Collected data converted to CSV format and ingested into Splunk

3. Adding to Map information about signal strength via Heatmap:

```plaintext
| eventstats min(wlan_radio_signal_dbm) as dbm_min, max(wlan_radio_signal_dbm) as dbm_max
   perc5(wlan_radio_signal_dbm) as dbm1, perc95(wlan_radio_signal_dbm) as dbm2
| eval hm_layer_1 = "Signal: ".dbm_min."...".dbm1." dbm"                                 
| eval hm_layer_2 = "Signal: ".(dbm1+1)."...".(dbm2-1)." dbm"                           
| eval hm_layer_3 = "Signal: ".dbm2."...".dbm_max." dbm"                              
| eval heatmapLayer=if(wlan_radio_signal_dbm<=dbm1, hm_layer_1, if(wlan_radio_signal_dbm>=dbm2, hm_layer_3, hm_layer_2)), heatmapBlur=if(wlan_radio_signal_dbm<=dbm1, 8, if(wlan_radio_signal_dbm>=dbm2, 40, 25)), heatmapRadius=if(wlan_radio_signal_dbm<=dbm1, 12, if(wlan_radio_signal_dbm>=dbm2, 50, 27))
| table latitude longitude heatmap*
```
Adding WiFi Signal Sources on a Map
Maps+ app includes ability to separate points into different layers

Heatmap allows to separate signal sources by strength in a different layers for visual filtering
Correlating data from multiple capture devices
Calculating “Suspect Score” for Wireless Sources

- Multiple WiFi Capture devices positioned in high risk areas
- Crime happened near device_1 at time_1
- Similar criminal activity registered near device_2 at time_2

SPL query to find signal sources that were present in both locations:
(SRC = “device_1.pcap”, “device_2.pcap”)
Calculating “Suspect Score” by Wireless Sources

SPL query to calculate “suspect score” and sort results by top suspects first.
Taking into account wireless signal strength of every source

index=pcap_summ
| eval dbm_score=(100+max_wlan_radio_signal_dbm)/20
| stats dc(SRC) as places,
  sum(dbm_score) as total_score
by sender_mac
| eval total_score=total_score*places*places
| sort - total_score
| table total_score sender_mac

Calculate score for each signal source (split signal strength in 5 bins)

Calculate number of locations for each source

Total_score = Sum(scores at all locations)

final_suspect_score = Sum(scores at all locations)*sources**2

NOTE:
Above formula gives higher “suspect score” to signal sources registered at multiple places.
Source with strong signal at a single location will have lower total score than weak signals detected in both locations.
Defining multiple GeoFence zones on a map

1. Splunk Maps+ allows to visually define zones
2. Each zone is represented by latitude, longitude of dots
3. After zone is defined – system calculated bounding rectangle for each zone
4. SPL automatically calculates presence (yes/no) of each wireless signal within each zone
Define GeoFence Zones around areas of interest
Define more complex GeoFence zone correlation

We can define multiple Wireless GeoFencing zones of interest and then request to show wifi data sources that are “Present in at least N” zones or “Present in All” zones.

This helps to discover potential suspects and solve crimes with higher degree of certainty.
Live demos ...
Thank You

Download all materials for this presentation here:
http://expe.us/geofencing/

Gleb Esman,
gesman@splunk.com
Sr. Project Manager, Fraud Analytics and Research, Splunk.

Splunk>