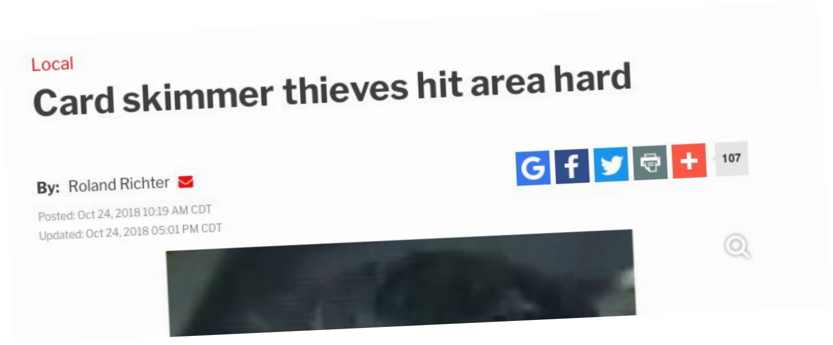
Detecting Bluetooth Card Skimmers Hidden in Gas Pumps

Nishant Bhaskar, Maxwell Bland,
Kirill Levchenko, Aaron Schulman

Card Skimming is a Big Problem

- Skimming : Implanting an electronic device to record card details
- Nilson Report estimates card fraud to reach $30 billion by 2020, and increase in skimming
- Official estimates in SD county in 2018 -> $43.01 million potential fraud



Local

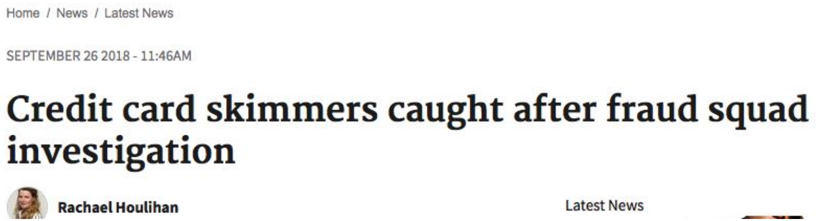
Card skimmer thieves hit area hard

107

By: Roland Richter

Posted: Oct 24, 2018 10:19 AM CDT

Updated: Oct 24, 2018 05:01 PM CDT



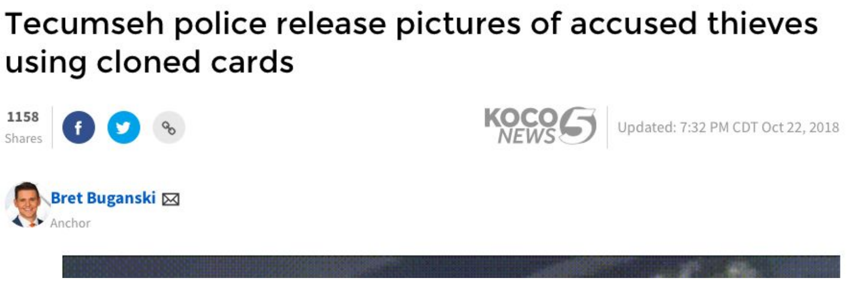
Home / News / Latest News

SEPTEMBER 26 2018 - 11:46AM

Credit card skimmers caught after fraud squad investigation

Rachael Houlihan

Latest News



Tecumseh police release pictures of accused thieves using cloned cards

1158 Shares

KOCO 5 NEWS

Updated: 7:32 PM CDT Oct 22, 2018

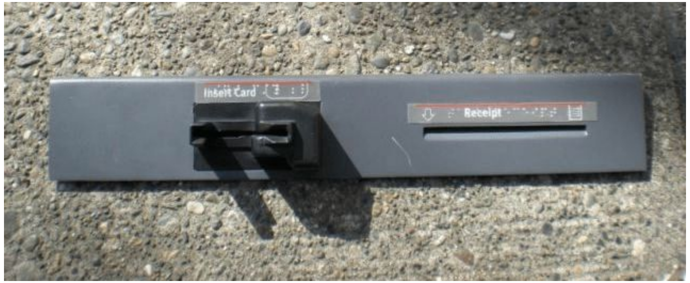
Bret Buganski

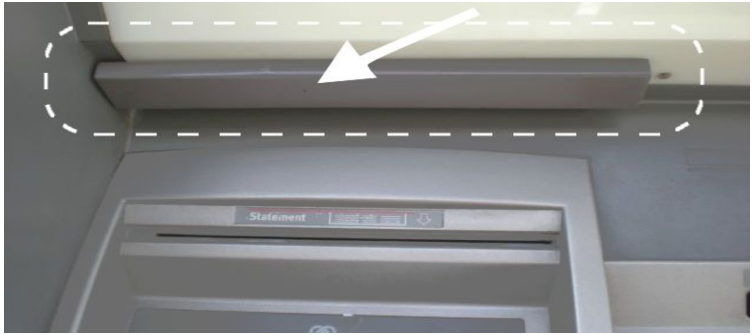
Anchor

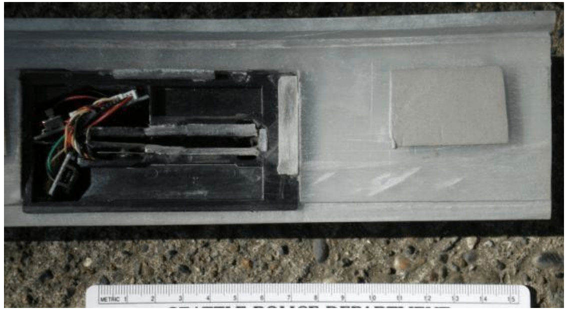
So how are the bad guys fooling us?

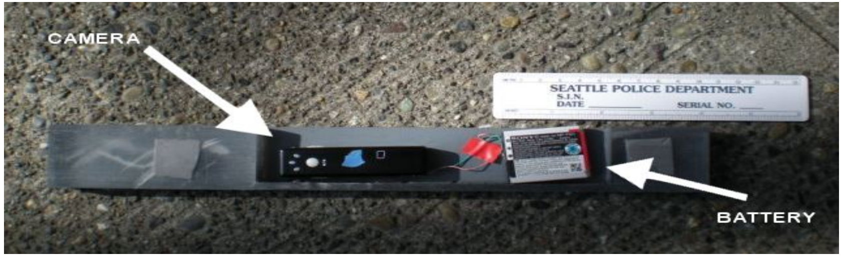
Card Skimmers are increasingly sophisticated

- Overlay: Enclosure cloning with pinhole camera for PIN capture



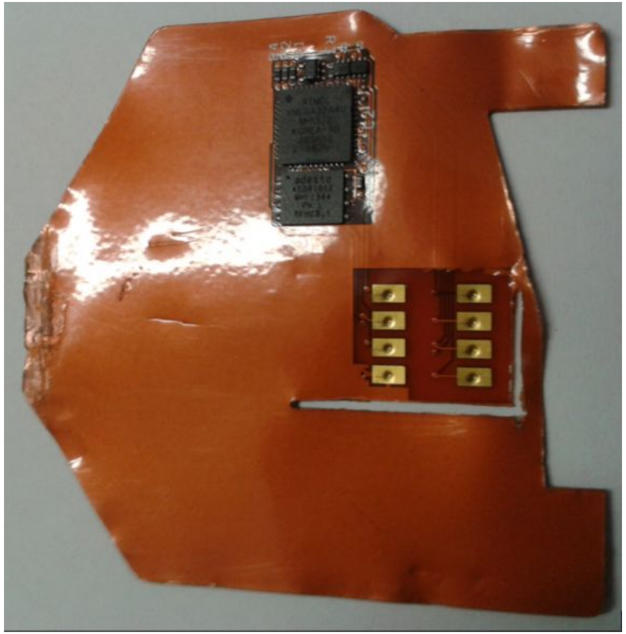


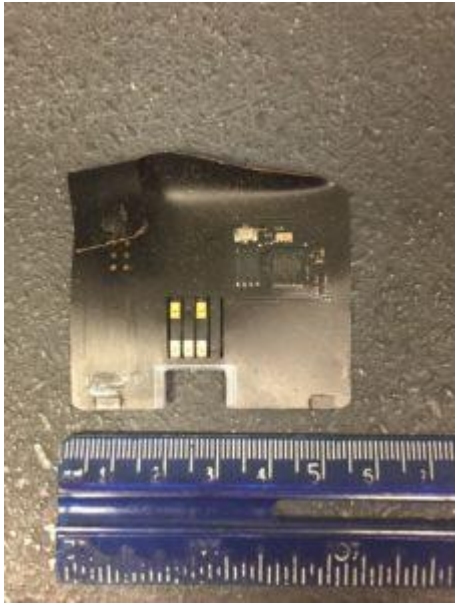




These are hard to discover visually

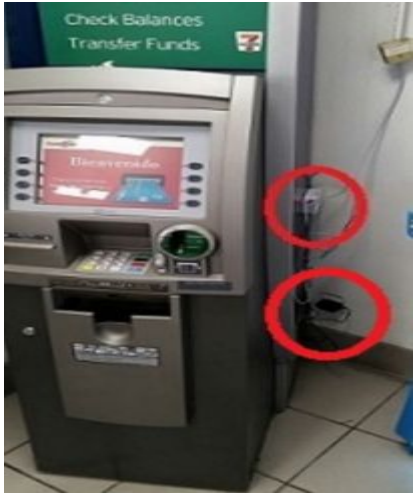
- Shimmer : Insert that hides in chip reader slot





These are hard to feel and discover

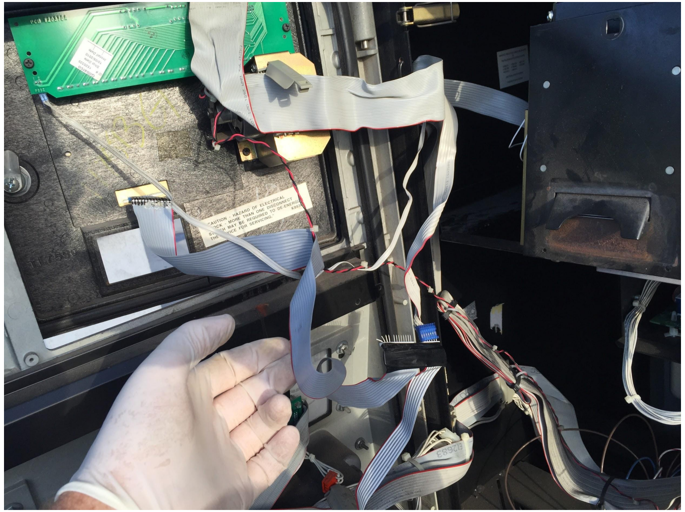
- Wiretap: Passive Phone/Network capture of transactions



These can not be detected by analyzing network traffic

Internal Skimmers: The Worst of All Worlds

- In this talk we will discuss about internal skimmers that are hidden inside the enclosure of a compromised terminal.



1. **Impossible to physically detect (Installation)**
    a. Where are these installed and what makes it so hard to detect

2. **Difficult to detect electronically (Exfiltration)**
    a. Our study on how difficult it is to detect presence of them in gas pumps
    b. Our tool design to enable detection
    c. Our validation to enable detection of these skimmers

B0: Requirements for an Internal Skimmer

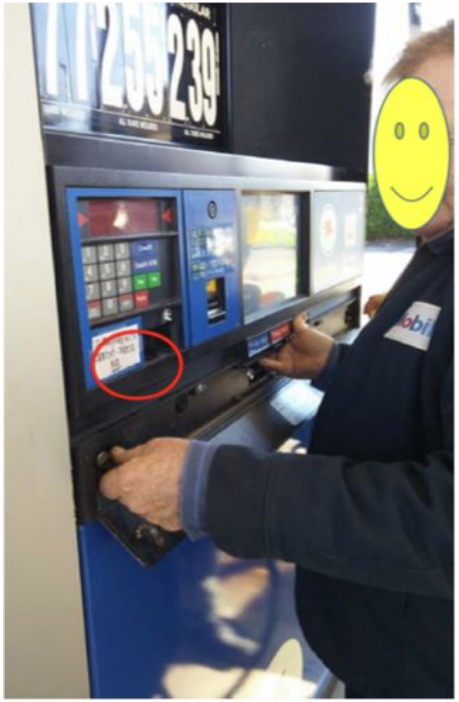
1) Needs a vector to be installed
2) Needs a way to exfiltrate the data

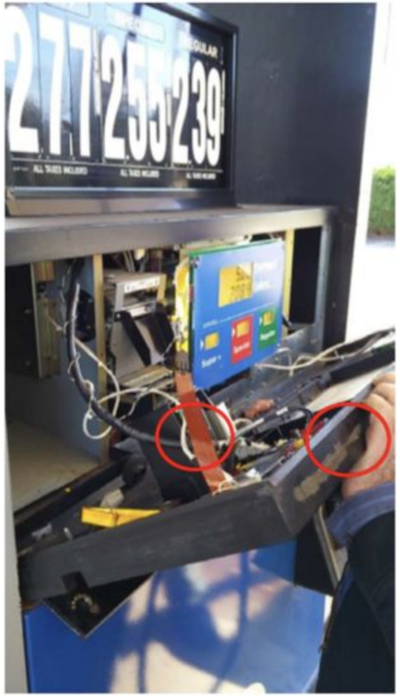
T: I will first discuss how they are installed, then I will discuss how we can discover them via the way they exfiltrate the data.

Gas pumps are an easy target

- **Minimal security features**
  - Universal keys

- **Lax video monitoring**
  - Not like an ATM where you have a camera on the customer



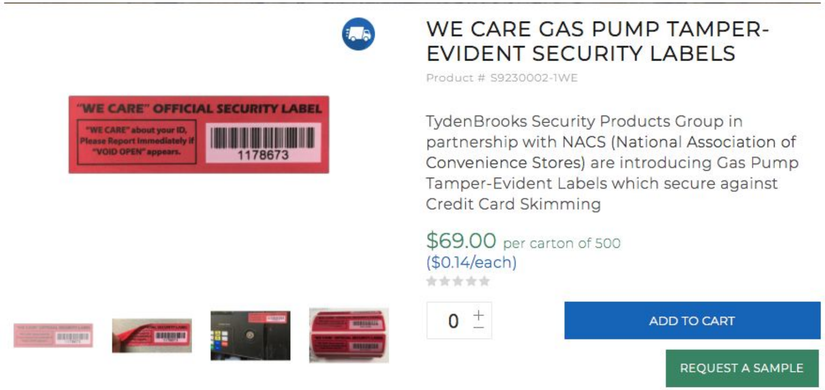


Security features ineffective

- **Universal keys** to open up most card reader access slots easily available online

- **Tamper proof seals** used to indicate if someone broke into card reader. Also available online

Having gotten in, where do we install the skimmer?



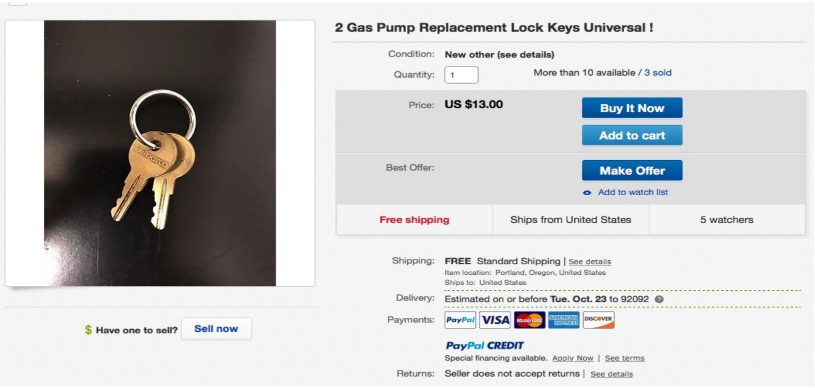
WE CARE GAS PUMP TAMPER-EVIDENT SECURITY LABELS

Product # S9230002-1WE

TydenBrooks Security Products Group in partnership with NACS (National Association of Convenience Stores) are introducing Gas Pump Tamper-Evident Labels which secure against Credit Card Skimming

$69.00 per carton of 500
($0.14/each)

"WE CARE" OFFICIAL SECURITY LABEL
"WE CARE" about your ID, Please Report Immediately if "VOID OPEN" appears.
1178673
0
ADD TO CART
REQUEST A SAMPLE



2 Gas Pump Replacement Lock Keys Universal !

Condition: New other (see details)

Quantity: 1 More than 10 available / 3 sold

Price: US $13.00

Best Offer:

Free shipping | Ships from United States | 5 watchers

Shipping: FREE Standard Shipping | See details
Item location: Portland, Oregon, United States
Ships to: United States

Delivery: Estimated on or before **Tue. Oct. 23** to 92092

Payments:

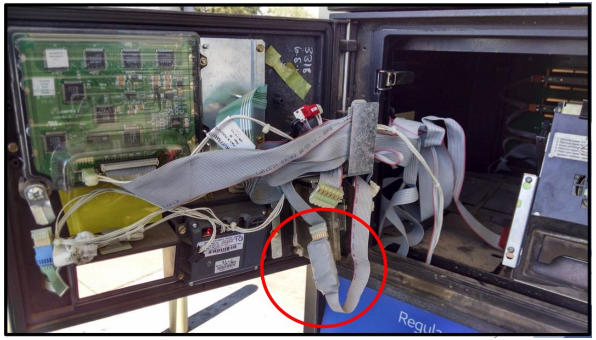
PayPal CREDIT
Special financing available. Apply Now | See terms

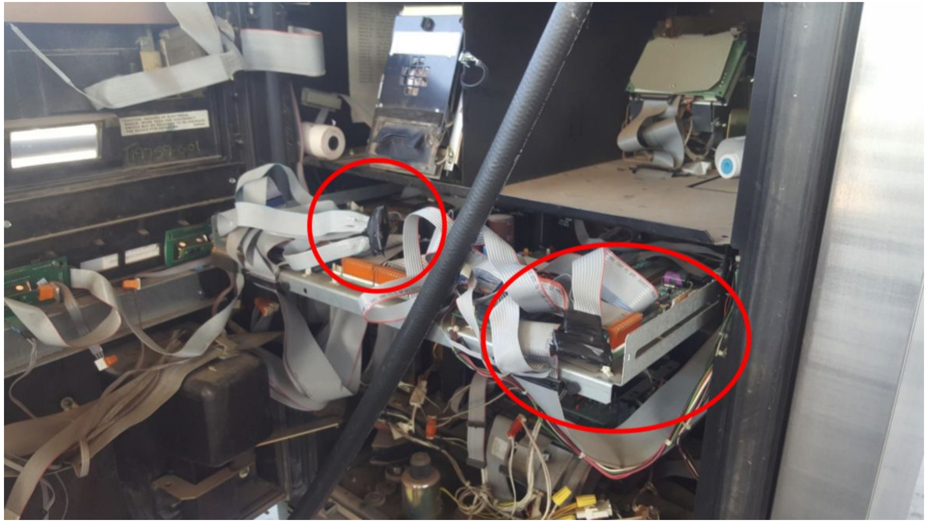
Returns: Seller does not accept returns | See details

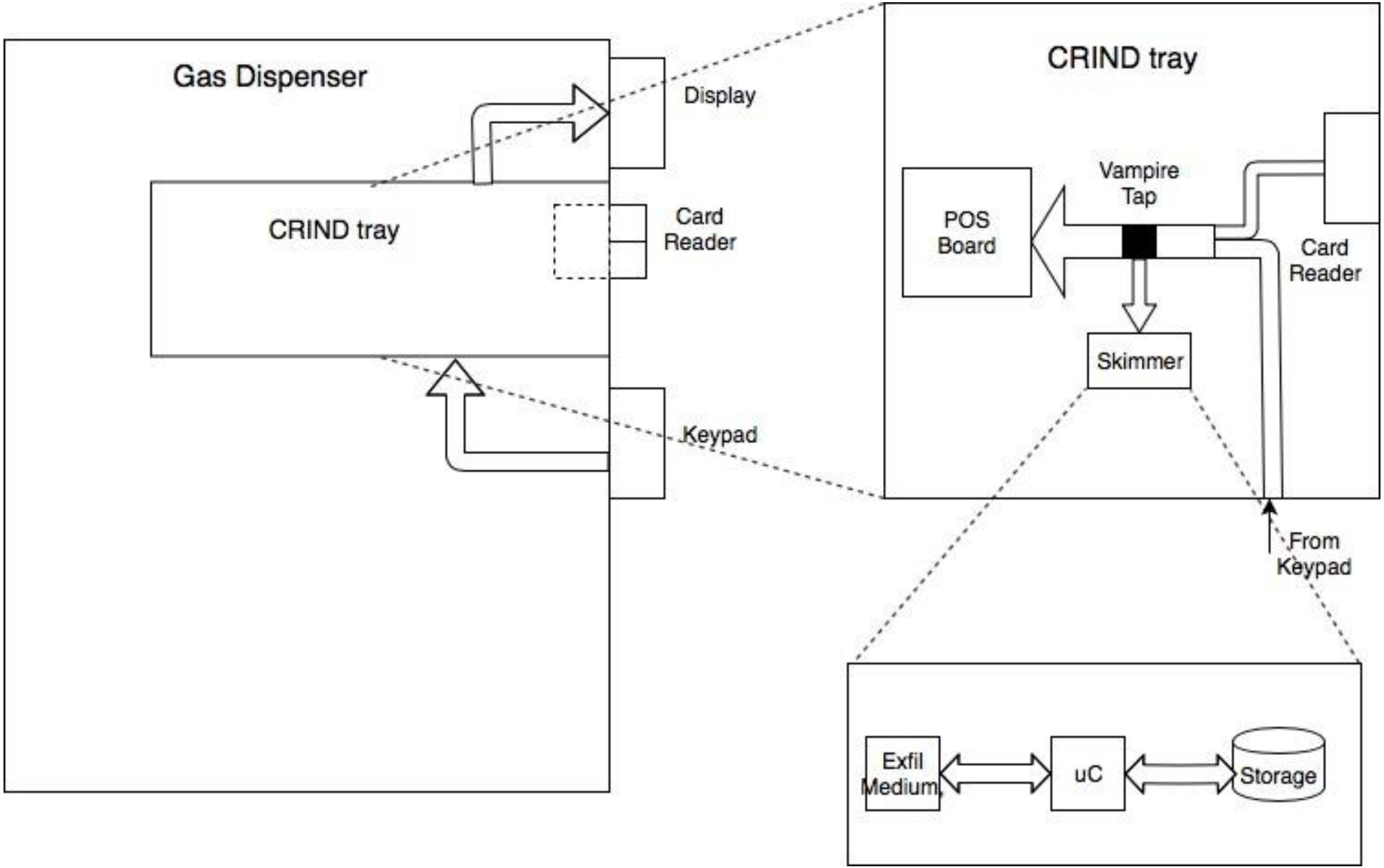
Getting the card info

- **Exposed ribbon cables** for card reader and keypad connection to POS terminal block

- **Vampire tap on ribbon cable** gives you passive captures of card numbers and PIN codes






Gas Dispenser
Display
CRIND tray
Card Reader
Keypad
CRIND tray
Vampire Tap
POS Board
Card Reader
Skimmer
From Keypad
Exfil Medium
uC
Storage

Once installed, they are really hard to find

- **Have on board storage**

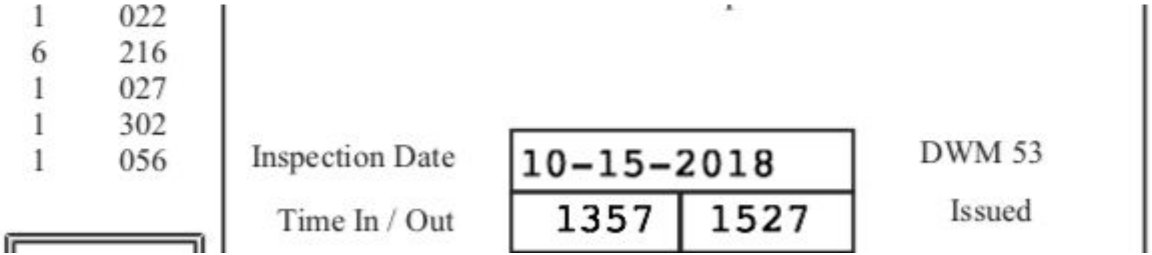
- Only way to detect presence is **manual inspection**

- State inspectors and law enforcement only inspect a gas station in two cases:
  - **Routine** : Gas dispenser inspections done for calibration. Skimmer check also done
  - **Complaint from credit card companies**: Multiple cards getting skimmed at location
  - **Complaint from individuals:** Very unreliable. Consumers don't do due diligence

- Why don't we just inspect all gas pumps more regularly?

How long do manual inspections take?

- Arizona state authorities post reports for every gas station inspection.
- We downloaded the inspection reports for the last 5 months and checked for time taken in unsuccessful inspections

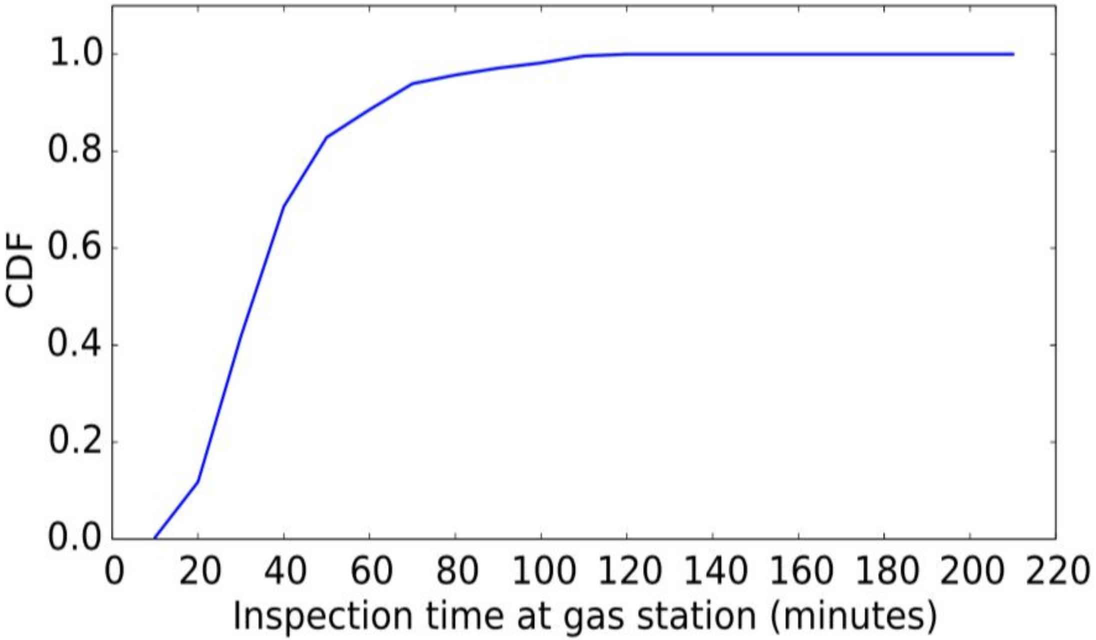


1	022
6	216
1	027
1	302
1	056

Inspection Date	10-15-2018		DWM 53
Time In / Out	1357	1527	Issued

Manual inspections are time consuming

Number of inspections	280
Total time	168 hours
Average time	36 minutes

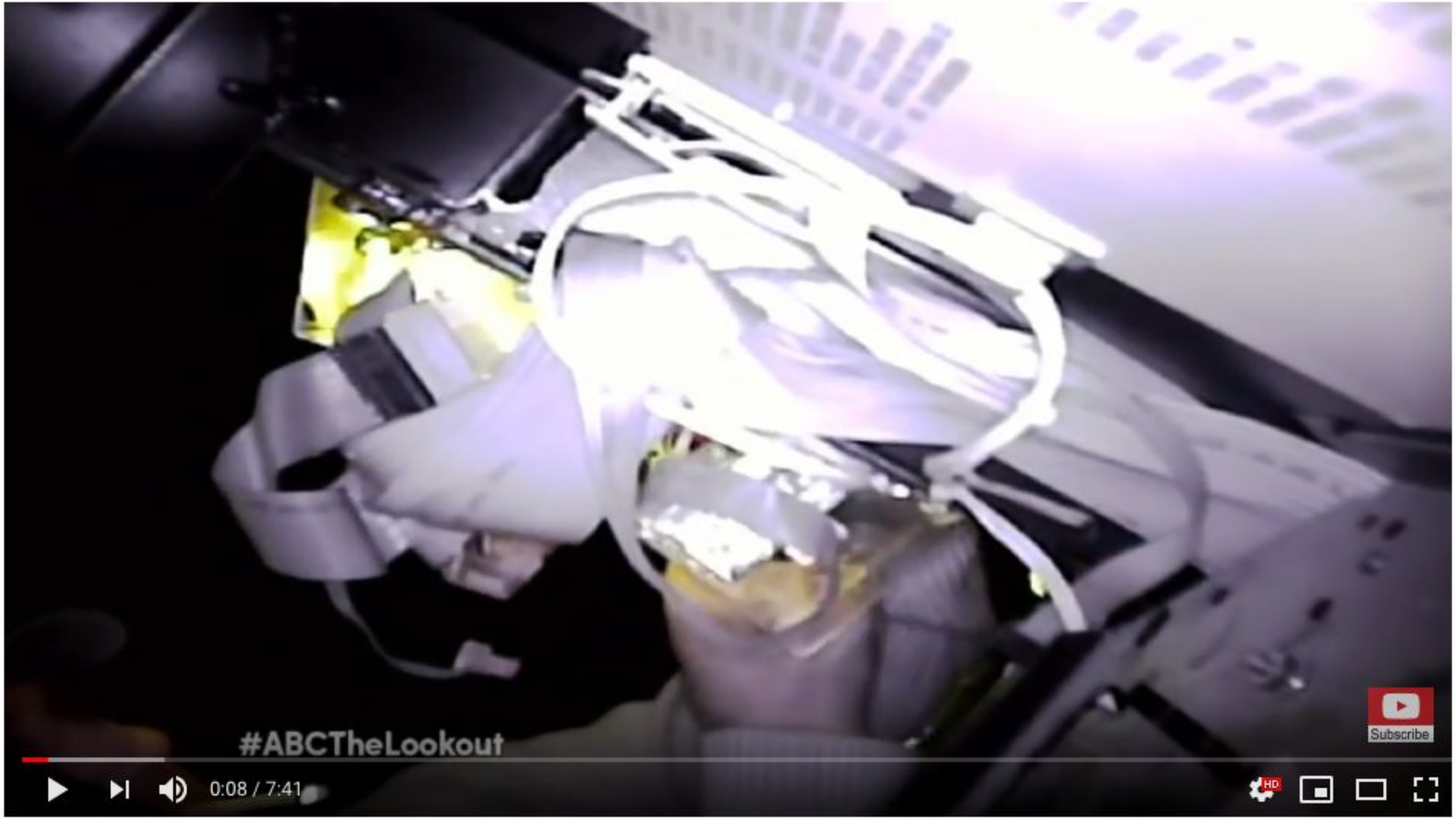


But the criminals do have to exfil their data…..

- **Internal skimmers have onboard memory**
  - **But how do you get the data out of the gas pump?**

- Early skimmers required criminal to open up pump to retrieve a memory card

- Law enforcement figured out a nice way to catch criminals during exfil


#ABCTheLookout
0:08 / 7:41
HD
Subscribe

So the bad guys adapted: Wireless Exfiltration

- Wireless modules can be added easily to existing skimmer designs.
  - Exfil process is all about parking at the gas station and pulling the data out while filling up.

- With a technology as simple as Bluetooth, **anyone can be employed to collect the data.**

However, with the presence of wireless signals, is there something that can be revealed about the skimmers?

So far no one has determined if these wireless exfils can be robustly detected

Challenges:

1. Tons of wireless devices at gas stations

2. Criminals are going to buy the same commodity wireless modules

3. Investigators don’t let us connect to all wireless modules to ask if they are skimmers. (history of MAC addresses paired lost)

What do we know about these skimmers?

- Criminals tend to use Bluetooth. Law enforcement reports that majority of skimmers recovered had Bluetooth

- A great choice - adaptive frequency hopping over 80 MHz, short range, modules readily available in the market

- Bluetooth allows you to scan (discover) nearby devices.

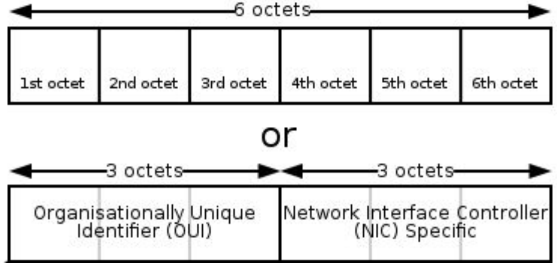
Information we can glean from Bluetooth Scans

- **Class of device:** What the intended device application is (e.g., Headphone, Printer etc) . A device is either categorized (assigned a class) or uncategorized (unassigned. CoD value 0x1F00)

- **RSSI:** Signal Strength of the scan response received

- **Device Name**

- **MAC Address:** 6 byte Bluetooth MAC address which can reveal the manufacturer by using IEEE OUI listing


6 octets
1st octet
2nd octet
3rd octet
4th octet
5th octet
6th octet
or
3 octets
3 octets
Organisationally Unique Identifier (OUI)
Network Interface Controller (NIC) Specific

So what do we do now?

- We know some information that Bluetooth devices reveal on scanning for them
- We went out there and did a large scale study of Bluetooth devices near gas stations
- Goal is to find any patterns or anomalies that translate to skimmers
- Contacts in law enforcement willing to check gas stations we report

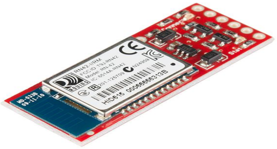
The Study: Overview of our Dataset

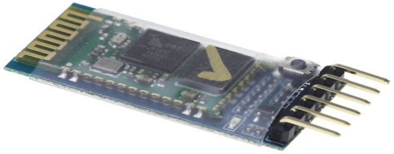
- Built an Android app to collect continuous scan data (Described later)
- Recorded Name, MAC address, CoD, RSSI as well as geolocation
- Recruited 20 people to run the app on their phones (provided phones to some) and collect data while driving in their normal routine
- Recruits include us, other researchers, Uber drivers, government inspectors
- Data collection across 10 states, primarily CA, MD, IL, NC

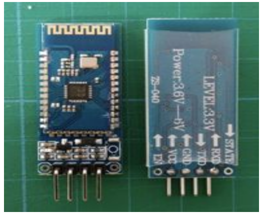
Number of gas stations seen with at least one BT device	1244
Number of classic Bluetooth devices near gas stations	2749
Number of LE Bluetooth devices near gas stations	8872

- Tons of devices. How do we find the skimmers in all of these? What knowledge do we have?

What modules do they use for skimmers?

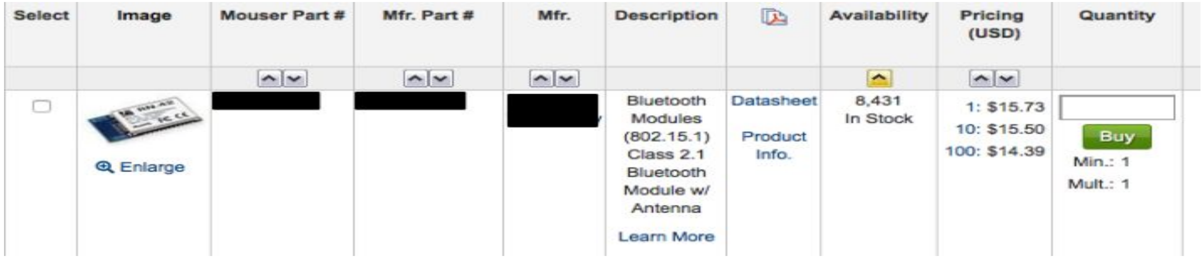






- Reports of recovered skimmers inform us serial to bluetooth modules are used
- They are used heavily in various embedded applications
- Can be retrofitted and used with existing non wireless internal skimmers
- We bought these modules and inspected them.
  We found that changing their MAC address or even class of device extremely difficult

Modules are widely available at part stores



Select	Image	Mouser Part #	Mfr. Part #	Mfr.	Description		Availability	Pricing (USD)	Quantity
□	Enlarge	[redacted]	[redacted]	[redacted]	Bluetooth Modules (802.15.1) Class 2.1 Bluetooth Module w/ Antenna Learn More	Datasheet Product Info.	8,431 In Stock	1: $15.73 10: $15.50 100: $14.39	Buy Min.: 1 Mult.: 1

So what do the Bluetooth characteristics of these modules look like?

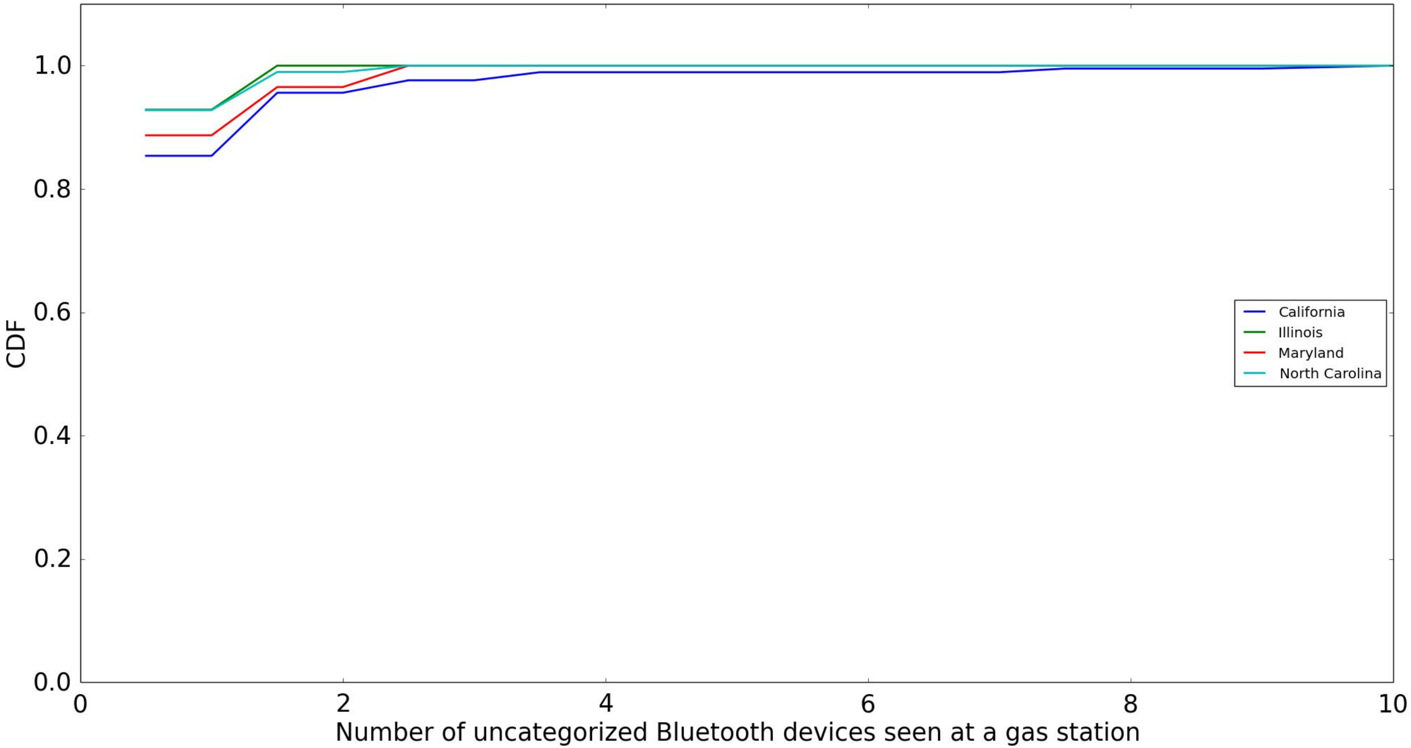
MAC address	Device Name	Class of device	Device Type
MAC Address A	Device Name A	0x1F00	Classic
MAC Address B	Device Name A	0x1F00	Classic

- Key insight being that these modules are classic Bluetooth and uncategorized (class 0x1F00)

- So can we use these insights to make sense of our huge data collection?

Analysis of data by state

Commodity Bluetooth modules used in recovered skimmers are classic, uncategorized. By applying this filtering we bring down the total number of devices to 243



MAC address based filtering of matching entries

- Further filtering of uncategorized devices can be done on basis of MAC.
- Recall we have OUI of the recovered skimmers
- We can filter our current list to look for devices that match the manufacturer
- By applying this filter we can reduce number of uncategorized devices to 44

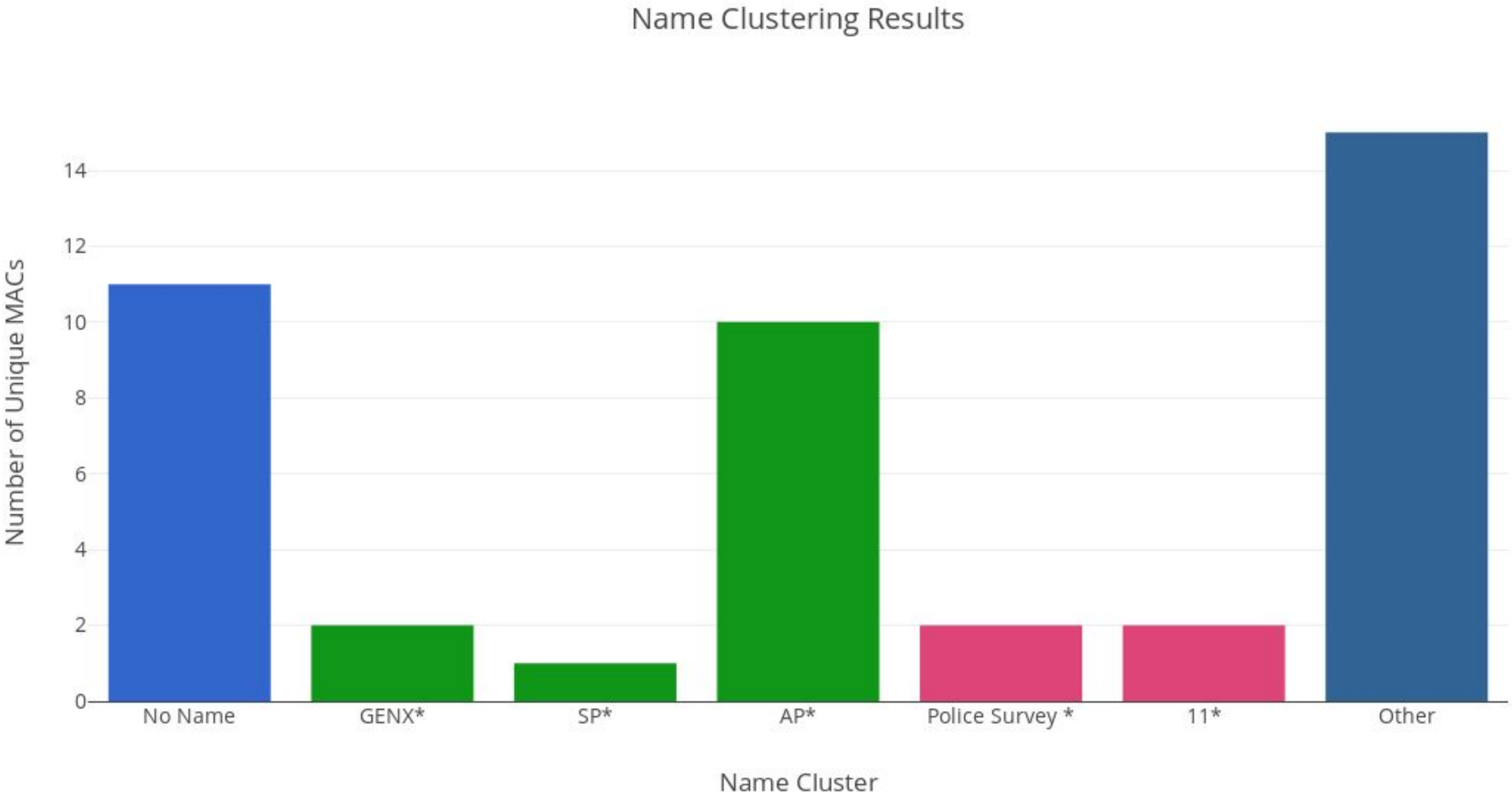
This is the final list of suspect modules that we should inspect. But is there any other information that can help us out?

Optional Step: Device Name Clustering

- Isolates really odd devices
  - 44 matching hitlist -> 4 with really odd names

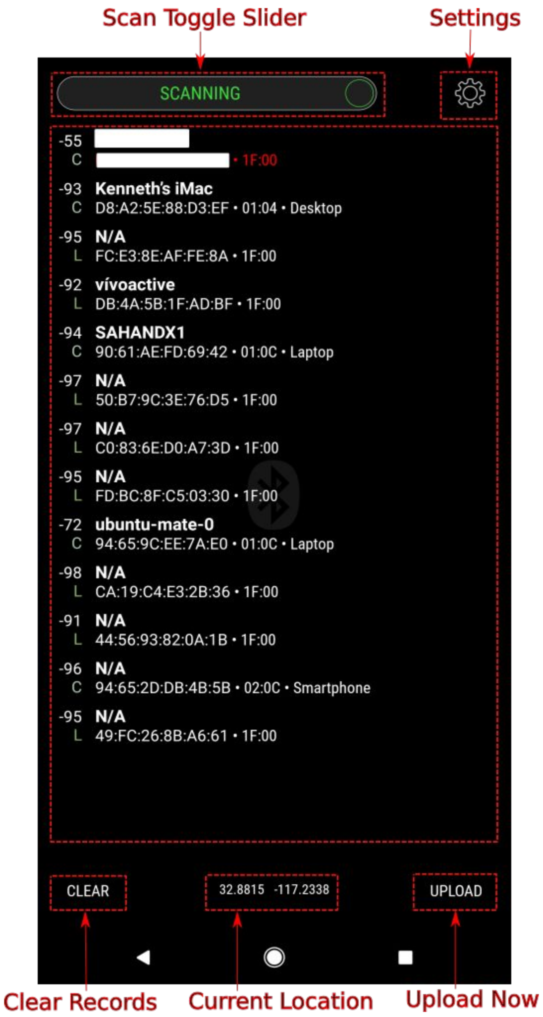
- Defines Product Groups
  - Example: Tiles, AP00-* Devices are OnBoard-Diagnostics (OBD-II) devices found at gas stations

- Actual verification comes from localization and manufacturer hitlist
  - Having an idea of common devices helps us isolate false positives


Name Clustering Results
Number of Unique MACs
0
2
4
6
8
10
12
14
No Name
GENX*
SP*
AP*
Police Survey *
11*
Other
Name Cluster

The Tool: Bluetana

- Application runs on any android smartphone
- Performs Bluetooth scan
- On-the-fly updates to hitlist, whitelist, and the app itself.
- Hitlist sourced from skimmer reports
- Hitlist devices show up in red, unless they match with common products, in which case they show up in orange



```
-55 [redacted]
 C  [redacted] • 1F:00
-93 Kenneth's iMac
 C  D8:A2:5E:88:D3:EF • 01:04 • Desktop
-95 N/A
 L  FC:E3:8E:AF:FE:8A • 1F:00
-92 vívoactive
 L  DB:4A:5B:1F:AD:BF • 1F:00
-94 SAHANDX1
 C  90:61:AE:FD:69:42 • 01:0C • Laptop
-97 N/A
 L  50:B7:9C:3E:76:D5 • 1F:00
-97 N/A
 L  C0:83:6E:D0:A7:3D • 1F:00
-95 N/A
 L  FD:BC:8F:C5:03:30 • 1F:00
-72 ubuntu-mate-0
 C  94:65:9C:EE:7A:E0 • 01:0C • Laptop
-98 N/A
 L  CA:19:C4:E3:2B:36 • 1F:00
-91 N/A
 L  44:56:93:82:0A:1B • 1F:00
-96 N/A
 C  94:65:2D:DB:4B:5B • 02:0C • Smartphone
-95 N/A
 L  49:FC:26:8B:A6:61 • 1F:00
```

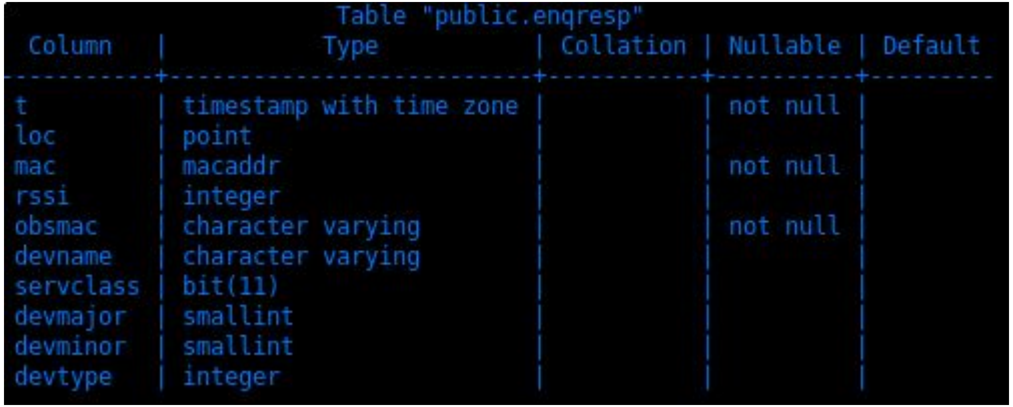
The Tool: Bluetana

- Collect all the necessary information mentioned previously

- Uses Android’s Bluetooth API to manage continuous scan

- Displays to user signal strength, device name, MAC Address, and [Classic/LE]
-

  More collected on the back end!

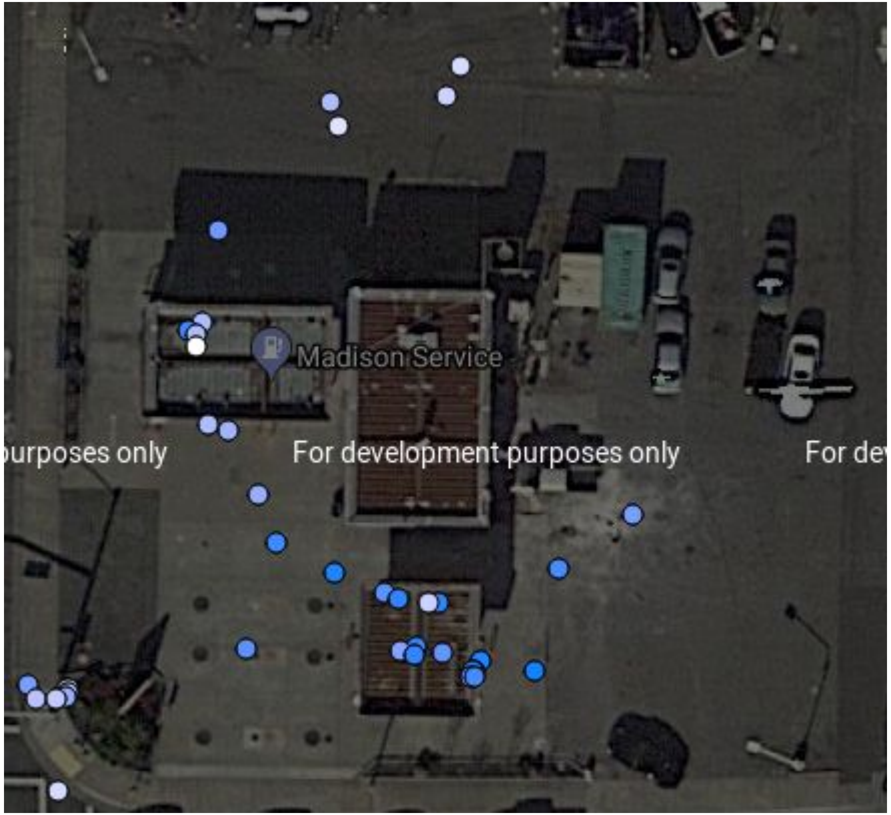


```
                    Table "public.enqresp"
  Column   |           Type           | Collation | Nullable | Default
-----------+--------------------------+-----------+----------+---------
 t         | timestamp with time zone |           | not null |
 loc       | point                    |           |          |
 mac       | macaddr                  |           | not null |
 rssi      | integer                  |           |          |
 obsmac    | character varying        |           | not null |
 devname   | character varying        |           |          |
 servclass | bit(11)                  |           |          |
 devmajor  | smallint                 |           |          |
 devminor  | smallint                 |           |          |
 devtype   | integer                  |           |          |
```

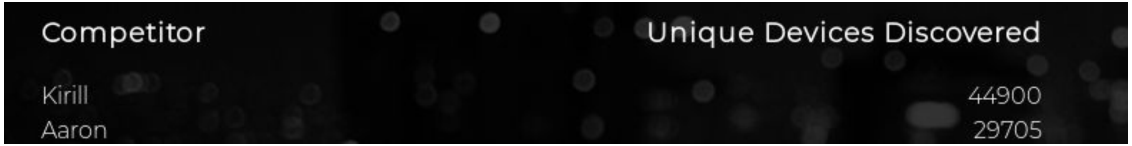
The Tool: Bluetana

- Signal strength measurements allow the user (and us!) to localize the device inside the gas pump

- We can combine the measurements from multiple users visiting the same station

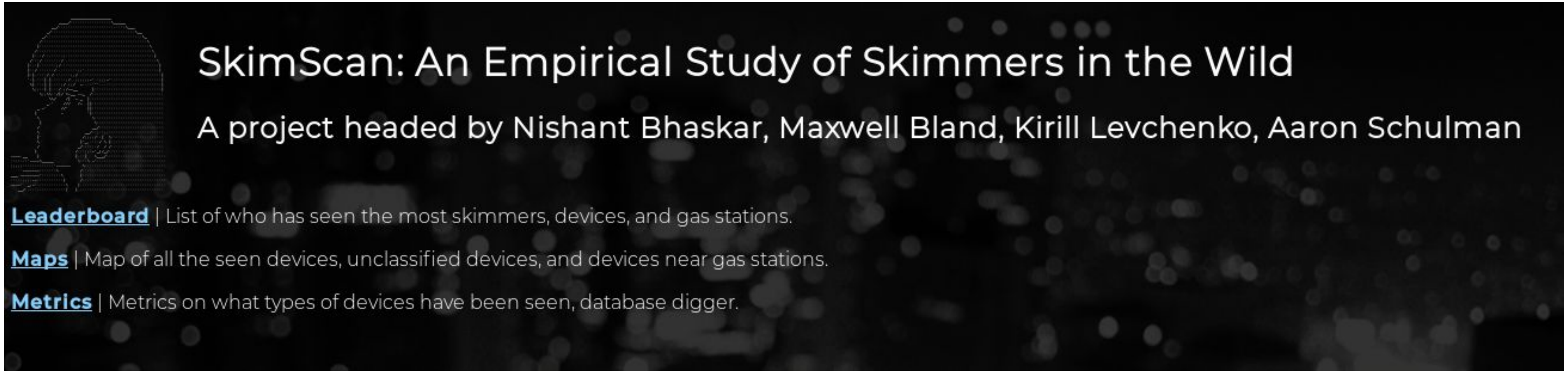


The Tool: Bluetana



Competitor	Unique Devices Discovered
Kirill	44900
Aaron	29705

- Data uploaded live via zipped CSV
- Hourly jobs are run to
  - provide a running leaderboard *(There are two notable outliers!)*
  - recluster device names
  - dynamically map observations
  - send slack notifications for interesting devices



SkimScan: An Empirical Study of Skimmers in the Wild

A project headed by Nishant Bhaskar, Maxwell Bland, Kirill Levchenko, Aaron Schulman

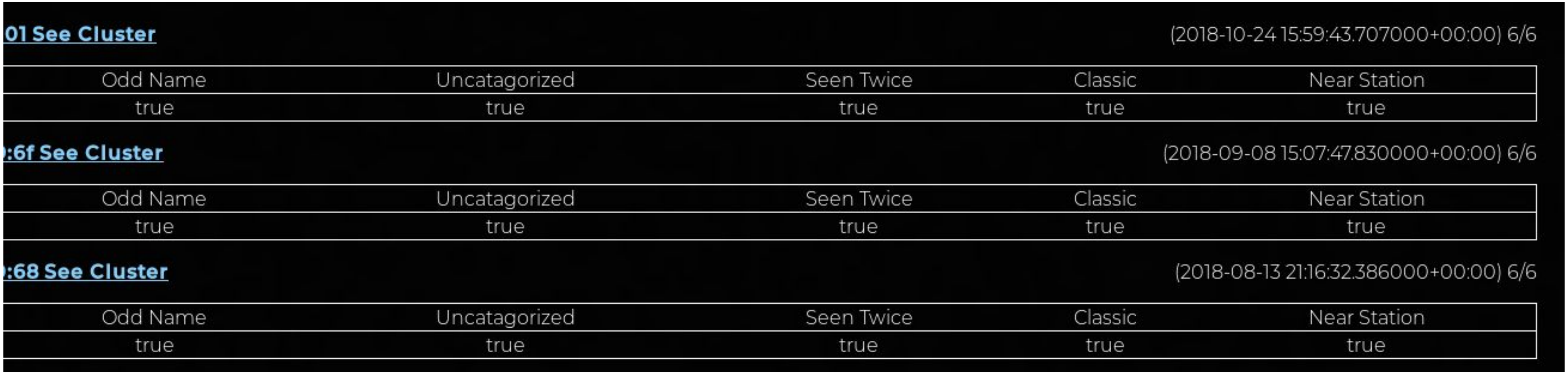
Leaderboard | List of who has seen the most skimmers, devices, and gas stations.

Maps | Map of all the seen devices, unclassified devices, and devices near gas stations.

Metrics | Metrics on what types of devices have been seen, database digger.

The Tool: Bluetana

- End result: a human readable list of potential skimmers.
- But how do we validate our approach?



01 See Cluster (2018-10-24 15:59:43.707000+00:00) 6/6

Odd Name	Uncatagorized	Seen Twice	Classic	Near Station
true	true	true	true	true

:6f See Cluster (2018-09-08 15:07:47.830000+00:00) 6/6

Odd Name	Uncatagorized	Seen Twice	Classic	Near Station
true	true	true	true	true

:68 See Cluster (2018-08-13 21:16:32.386000+00:00) 6/6

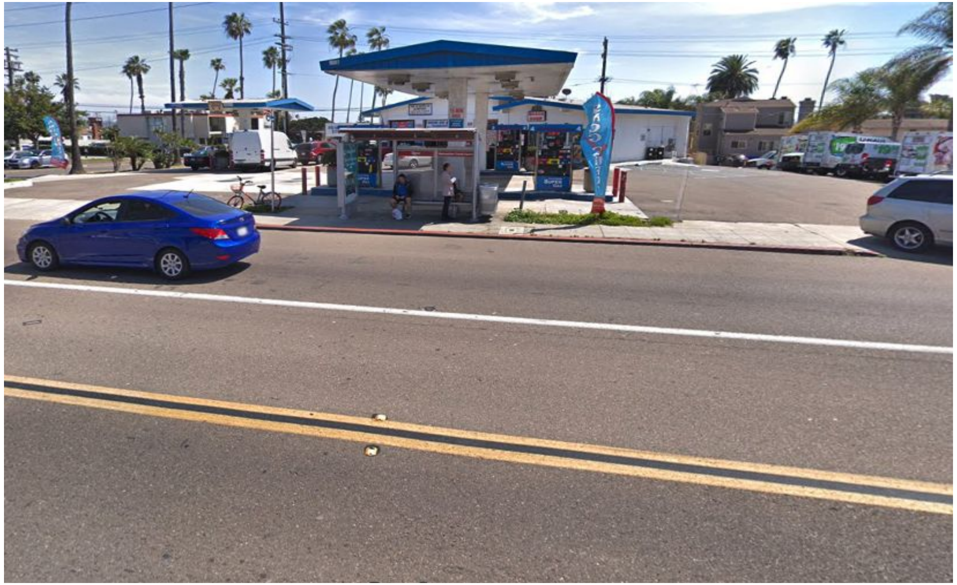
Odd Name	Uncatagorized	Seen Twice	Classic	Near Station
true	true	true	true	true

Validation of our method : Driving some more

- Short range of Bluetooth -> Validation can be done only by visiting gas stations
- We decided to test this out in SD county
- SD county has 875 gas station locations. Covering all in reasonable amount of time is difficult
- How can we choose a good sample set of gas stations to validate our tool?

Choosing the gas stations

- Recall certain gas pump types can be opened using a replacement key.
- Confirmation from law enforcement that these are commonly affected
- How do you figure out the gas dispenser type at a particular location
- Google Street View to the rescue



We inspected Street View images for all 875 gas stations and narrowed it down to 208

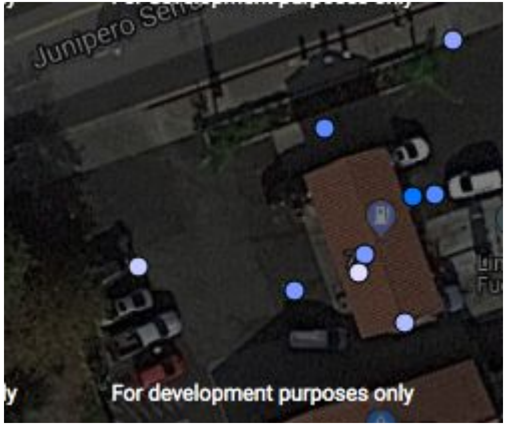
Results of the validation

Number of gas station stations	208
Number of Bluetooth devices	4761
Classic devices near gas stations	332
Uncategorized devices	25
Matching hitlist	14
After whitelist filtering	13

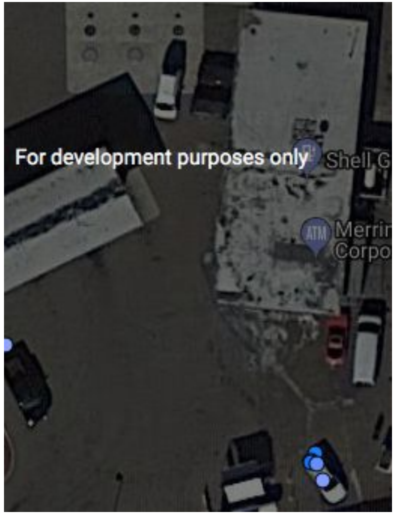
All filtering done and displayed on the front end, so real time tracking is possible.

Bluetana also records something else...

- RSSI an indication of signal strength of device. Very useful in the field



Skimmer



Neighbor

RSSI for confirmation

- RSSI can be used in the field for confirmation of skimmer location in the pump

- Our process is:
  1. drive to the gas station
  2. stop by for a few minutes
  3. check app to see if any devices flagged
  4. do a walkabout to see RSSI variations

- The app continually updates the RSSI and therefore you can see variations in real time. Can be used to localize a suspect device to a gas pump

Validation : Reporting to law enforcement

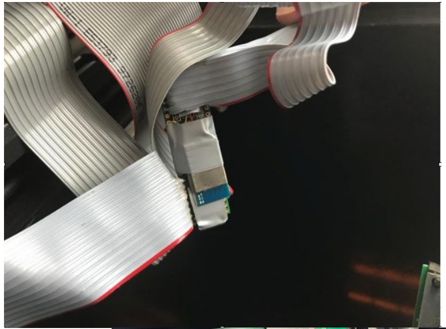
- From our validation we discovered a total of 8 skimmers and reported them to law enforcement contacts

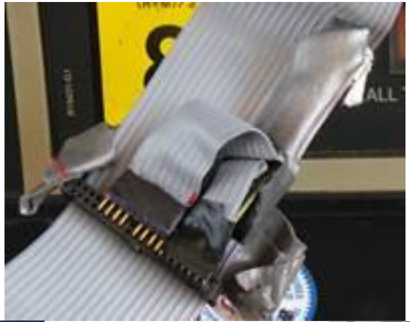
- They went in and did a manual inspection of all gas stations reported

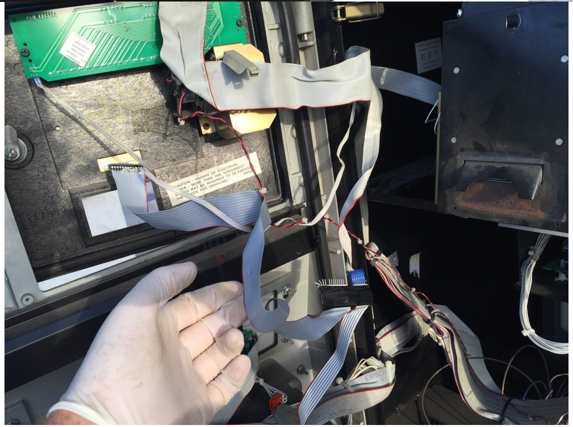
- **Found skimmers in all reported locations and gas pumps.**

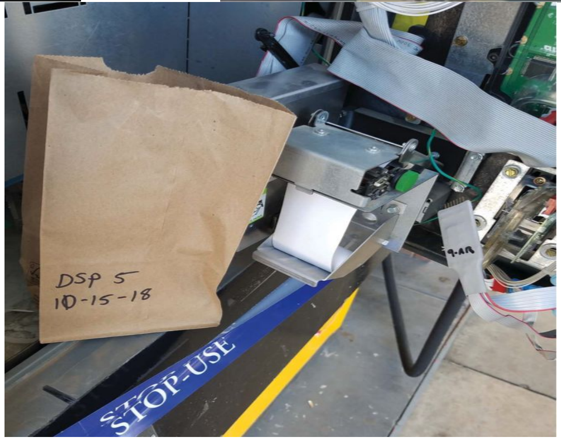
  Success rate 100%

Enter 5-0









Success story

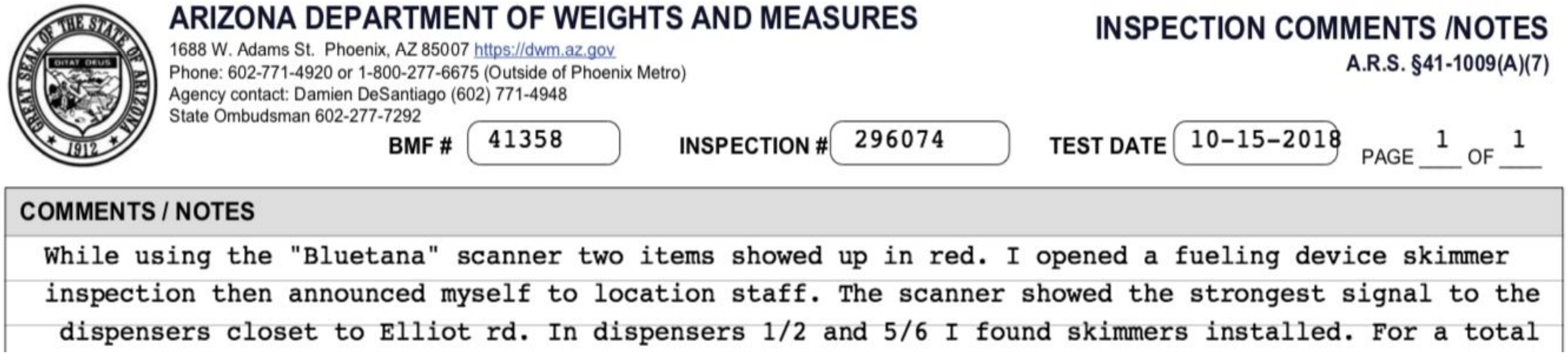
- Total time spent in scanning 208 gas stations - 40 hours
  (Including drive time between gas stations)

- Average time at gas station for detecting presence of skimmer - 5 minutes

- Our law enforcement contact informs us that they we have discovered
  25% of all gas station skimmers recovered in the county this year

Who else is using Bluetana?

- Simple tool design and usage has enabled scaling abilities of our contacts in state and local inspectors and law enforcement agencies as well
- Our tool has been successfully utilized in Arizona. Within a week of usage they were able to find skimmers !!



ARIZONA DEPARTMENT OF WEIGHTS AND MEASURES

1688 W. Adams St. Phoenix, AZ 85007 https://dwm.az.gov
Phone: 602-771-4920 or 1-800-277-6675 (Outside of Phoenix Metro)
Agency contact: Damien DeSantiago (602) 771-4948
State Ombudsman 602-277-7292

INSPECTION COMMENTS /NOTES

A.R.S. §41-1009(A)(7)

BMF # 41358 **INSPECTION #** 296074 **TEST DATE** 10-15-2018 PAGE 1 OF 1

COMMENTS / NOTES

While using the "Bluetana" scanner two items showed up in red. I opened a fueling device skimmer inspection then announced myself to location staff. The scanner showed the strongest signal to the dispensers closet to Elliot rd. In dispensers 1/2 and 5/6 I found skimmers installed. For a total

Bluetana skimmers found over the year

City	No . of skimmers recovered
Sacramento, CA	2
San Juan Capistrano, CA	2
Escondido, CA	1
San Diego, CA	7
Tempe, AZ	4

So how can we expect criminals to adapt?

- **Criminals can move to other technologies** like Bluetooth LE:

  Our methodology can still be effective

- **What about turning off discoverability?** With discoverability turned off, criminals have to resort to using a pre paired device with the Bluetooth skimmer.