

# Watching IoTs That Watch Us

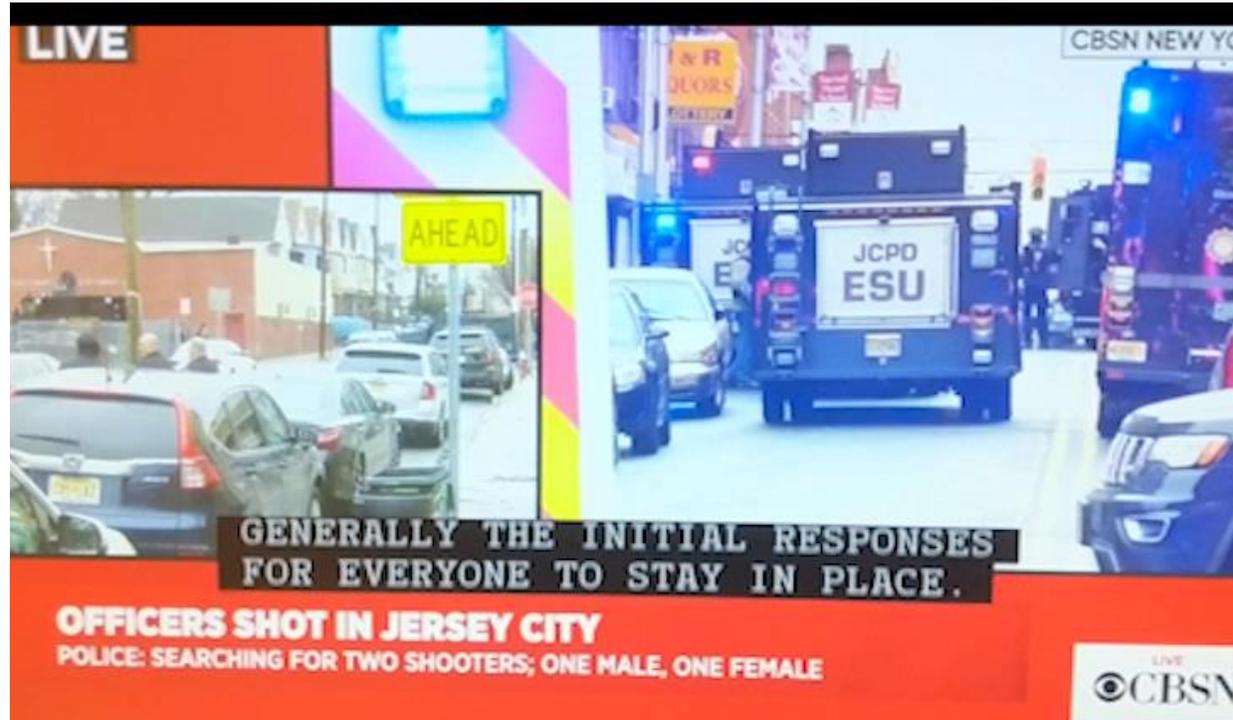
Danny Y. Huang

Assistant Professor



# Video: I'm watching my TV while it is watching me

**ROKU**<sup>®</sup>



# Video: I'm watching my TV while it is watching me

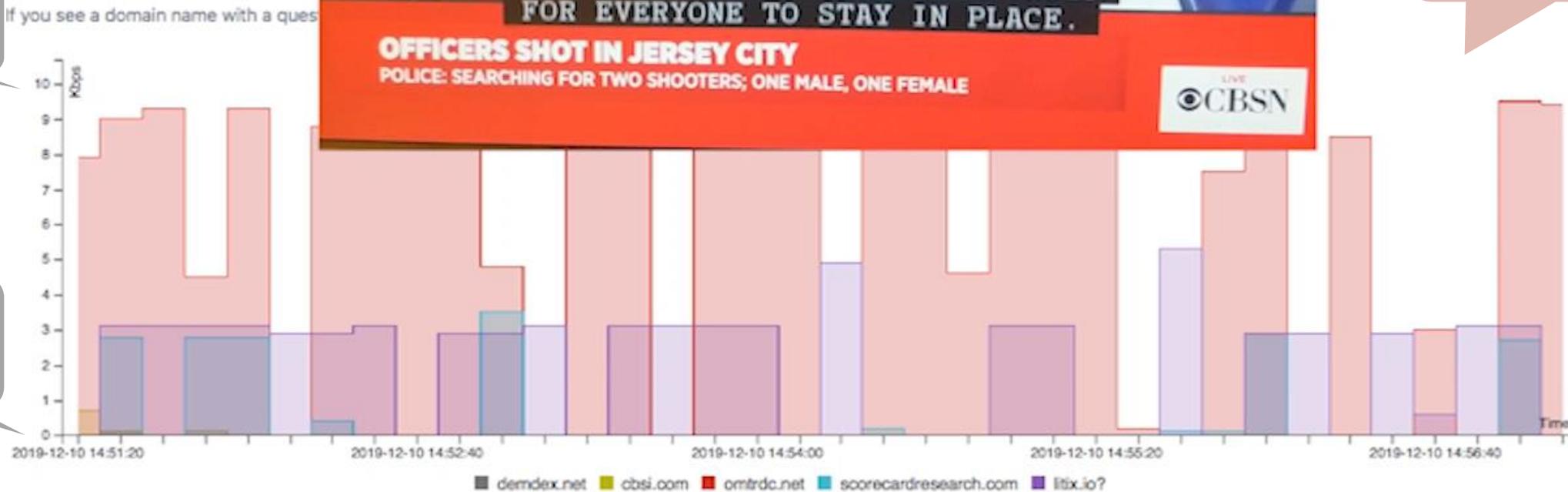
**ROKU**



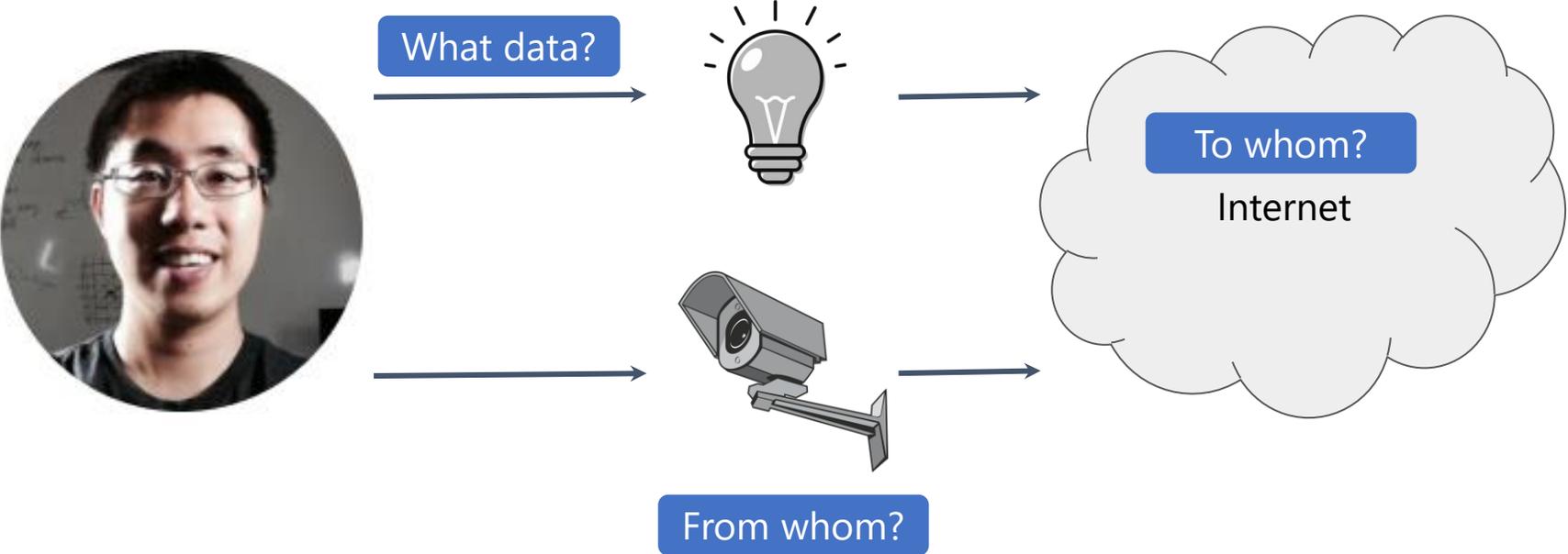
**Adobe** Adobe Marketing Cloud

Kbps

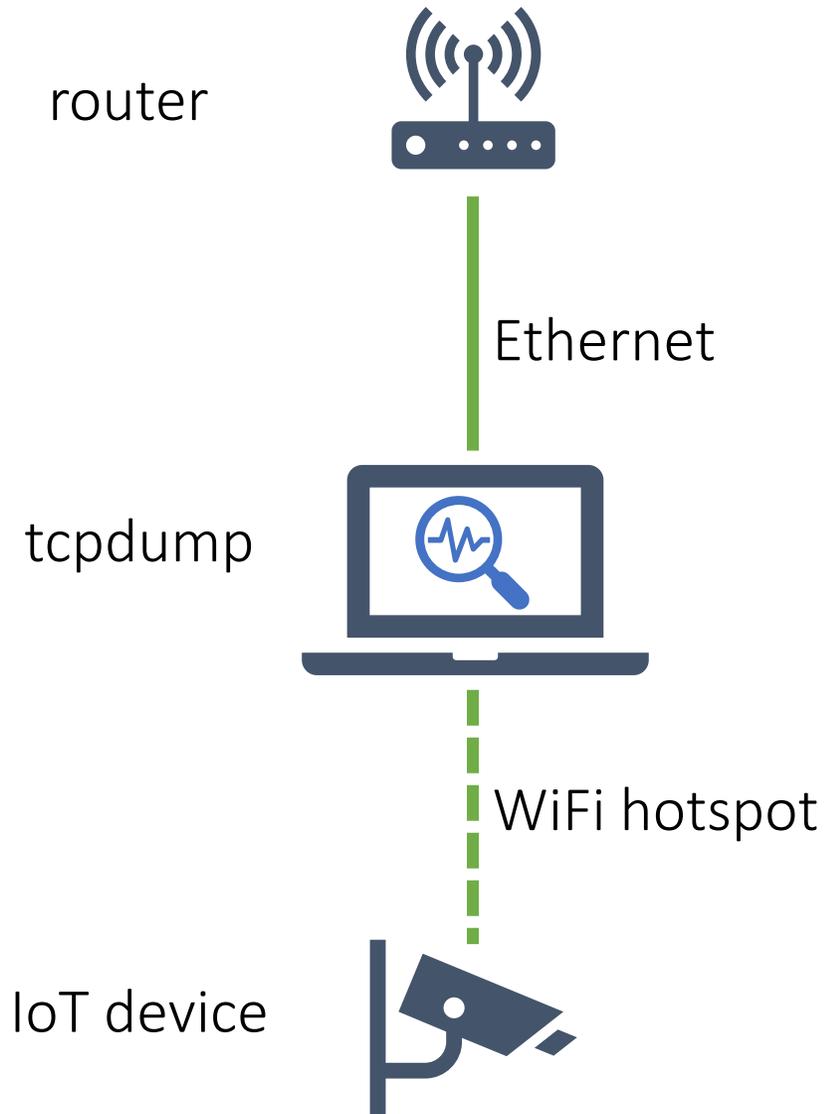
Time (10x)



# Many consumers are concerned about IoT security and privacy



# Analyzing devices' operational network traffic in lab



Are connections correctly encrypted?

Which Internet service is device talking to?

What data is being sent by device?

Google

小米  
xiaomi.com

amazon

dahua  
TECHNOLOGY

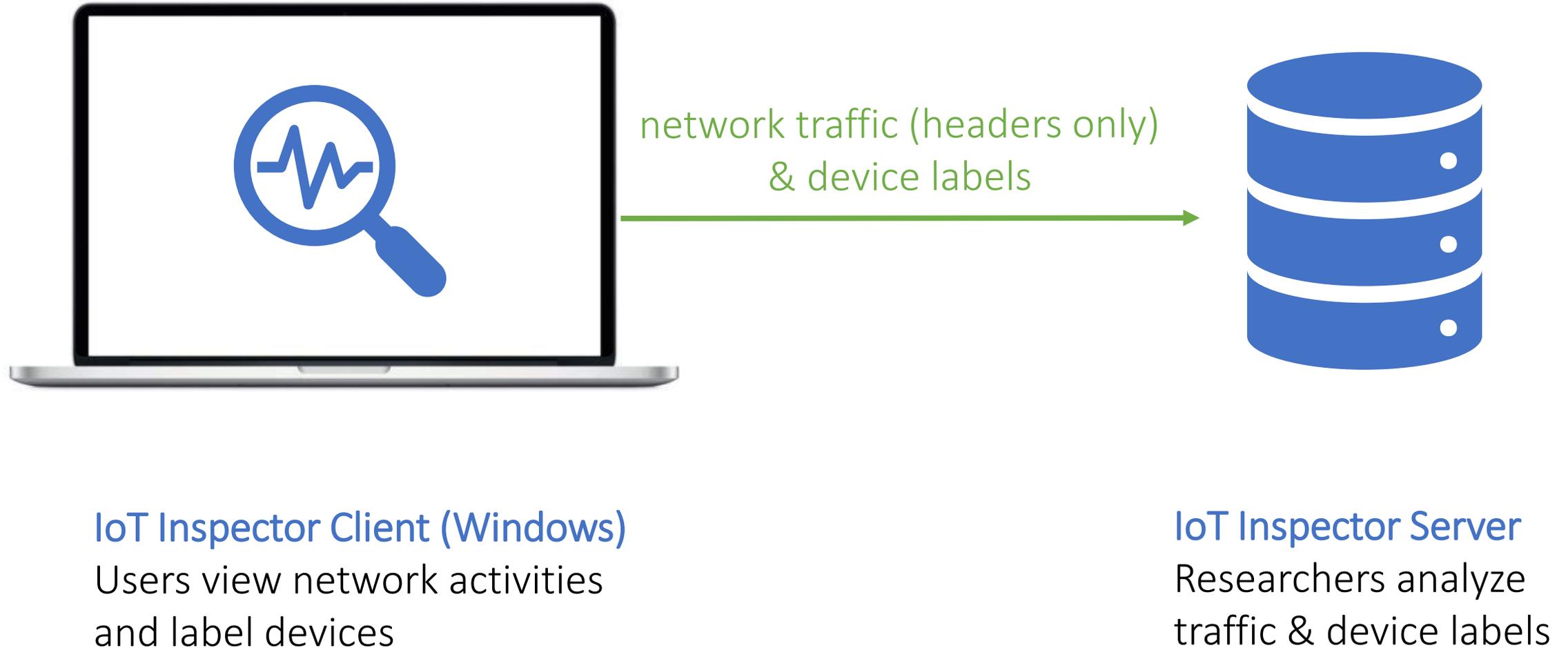
SAMSUNG

HIKVISION®

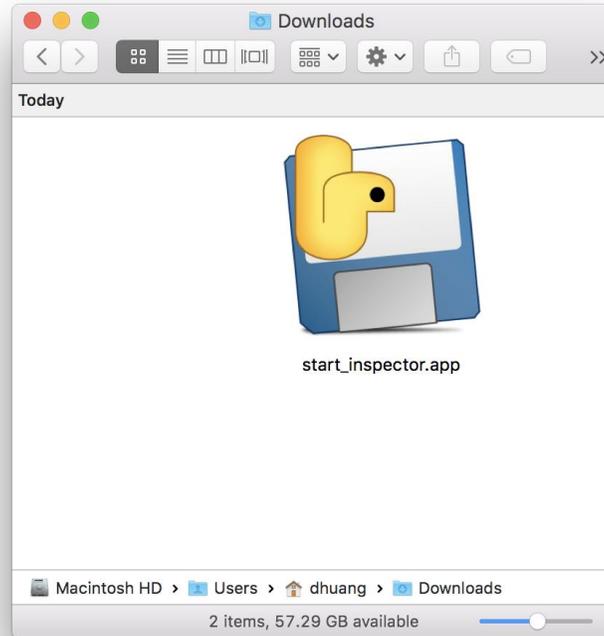
# Incentivizing volunteers to collect IoT network traffic at scale

Build **software** tool that provides volunteers with **usable insight** on IoT security & privacy with **one-click**

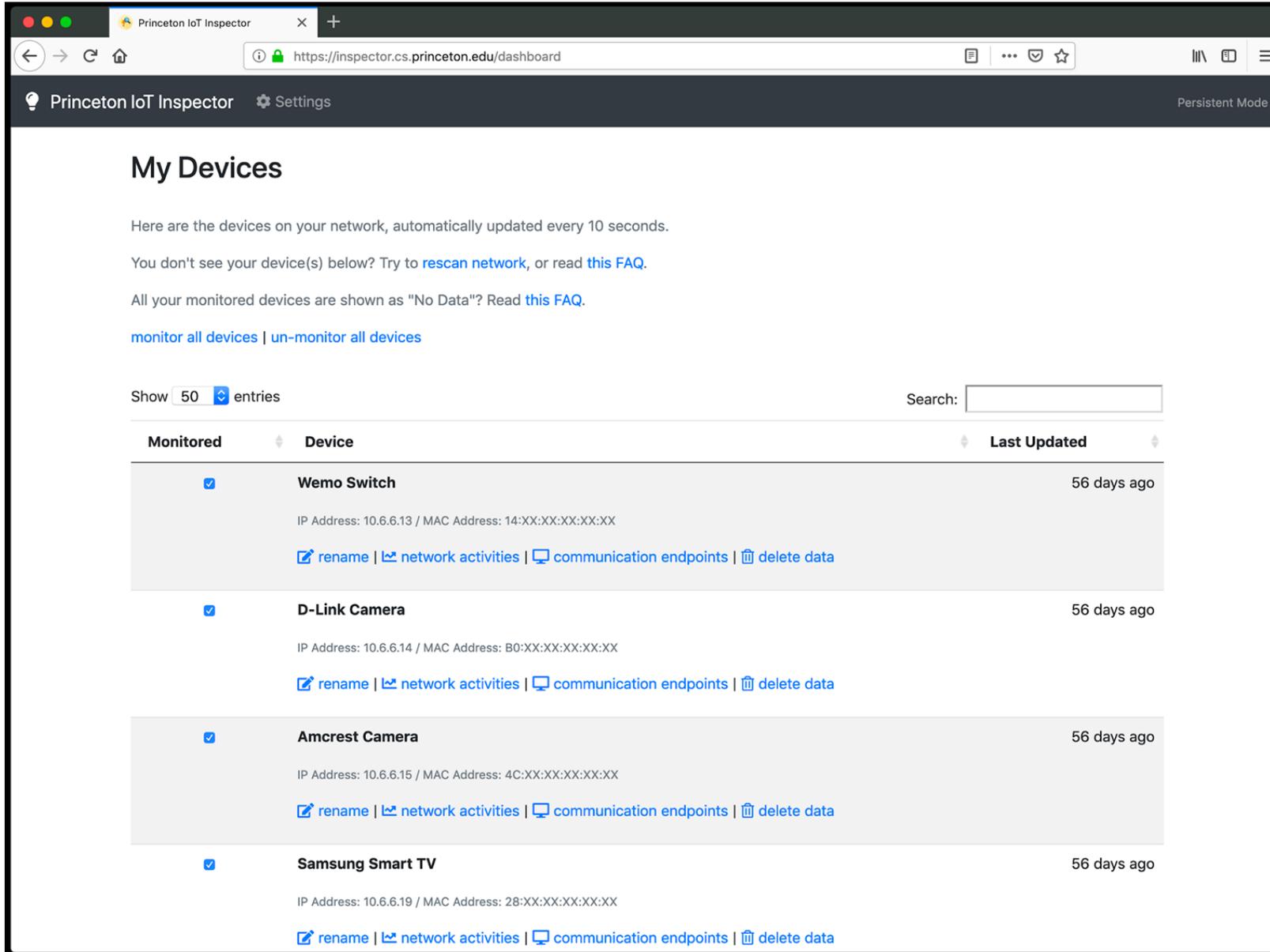
# IoT Inspector: usable system to crowdsource IoT network traffic at scale



# Downloading and running IoT Inspector



# Downloading and running IoT Inspector



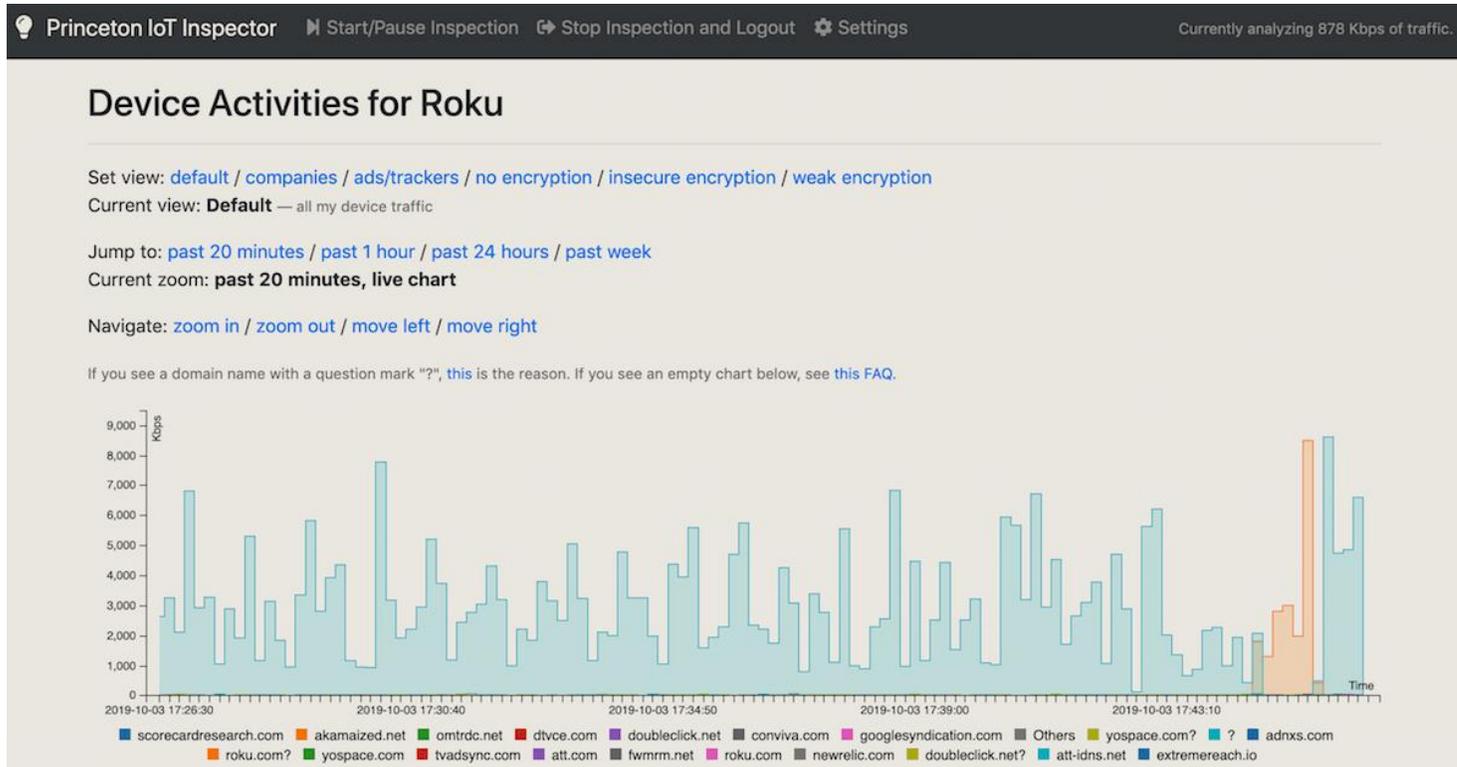
The screenshot shows the Princeton IoT Inspector web interface. The browser address bar displays `https://inspector.cs.princeton.edu/dashboard`. The page title is "Princeton IoT Inspector" and it includes a "Settings" icon and "Persistent Mode" text. The main heading is "My Devices".

Text on the page: "Here are the devices on your network, automatically updated every 10 seconds. You don't see your device(s) below? Try to [rescan network](#), or read [this FAQ](#). All your monitored devices are shown as "No Data"? Read [this FAQ](#). [monitor all devices](#) | [un-monitor all devices](#)"

Controls: "Show 50 entries" and a "Search:" input field.

Monitored	Device	Last Updated
<input checked="" type="checkbox"/>	<b>Wemo Switch</b> IP Address: 10.6.6.13 / MAC Address: 14:XX:XX:XX:XX:XX <a href="#">rename</a>   <a href="#">network activities</a>   <a href="#">communication endpoints</a>   <a href="#">delete data</a>	56 days ago
<input checked="" type="checkbox"/>	<b>D-Link Camera</b> IP Address: 10.6.6.14 / MAC Address: B0:XX:XX:XX:XX:XX <a href="#">rename</a>   <a href="#">network activities</a>   <a href="#">communication endpoints</a>   <a href="#">delete data</a>	56 days ago
<input checked="" type="checkbox"/>	<b>Amcrest Camera</b> IP Address: 10.6.6.15 / MAC Address: 4C:XX:XX:XX:XX:XX <a href="#">rename</a>   <a href="#">network activities</a>   <a href="#">communication endpoints</a>   <a href="#">delete data</a>	56 days ago
<input checked="" type="checkbox"/>	<b>Samsung Smart TV</b> IP Address: 10.6.6.19 / MAC Address: 28:XX:XX:XX:XX:XX <a href="#">rename</a>   <a href="#">network activities</a>   <a href="#">communication endpoints</a>   <a href="#">delete data</a>	56 days ago

# Insights from an independent user



Ira Flatow  
Host of Science Friday

“Here is what the **Princeton IoT Inspector** tracked in a 20 minute time span on Ira’s Roku.”

(October 4, 2019)

*Insight* – Ira’s Roku TV constantly communicated with advertising and tracking services

# Video: IoT Inspector showing network activities of Roku TV

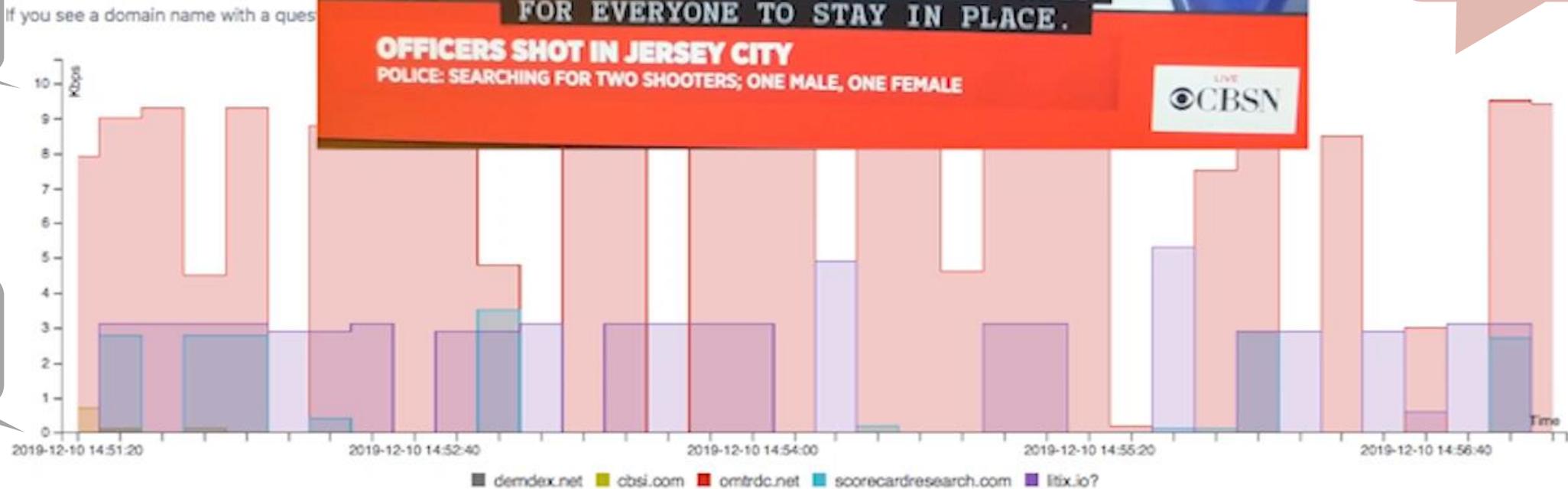
**ROKU**



**Adobe** Marketing Cloud

Kbps

Time (10x)



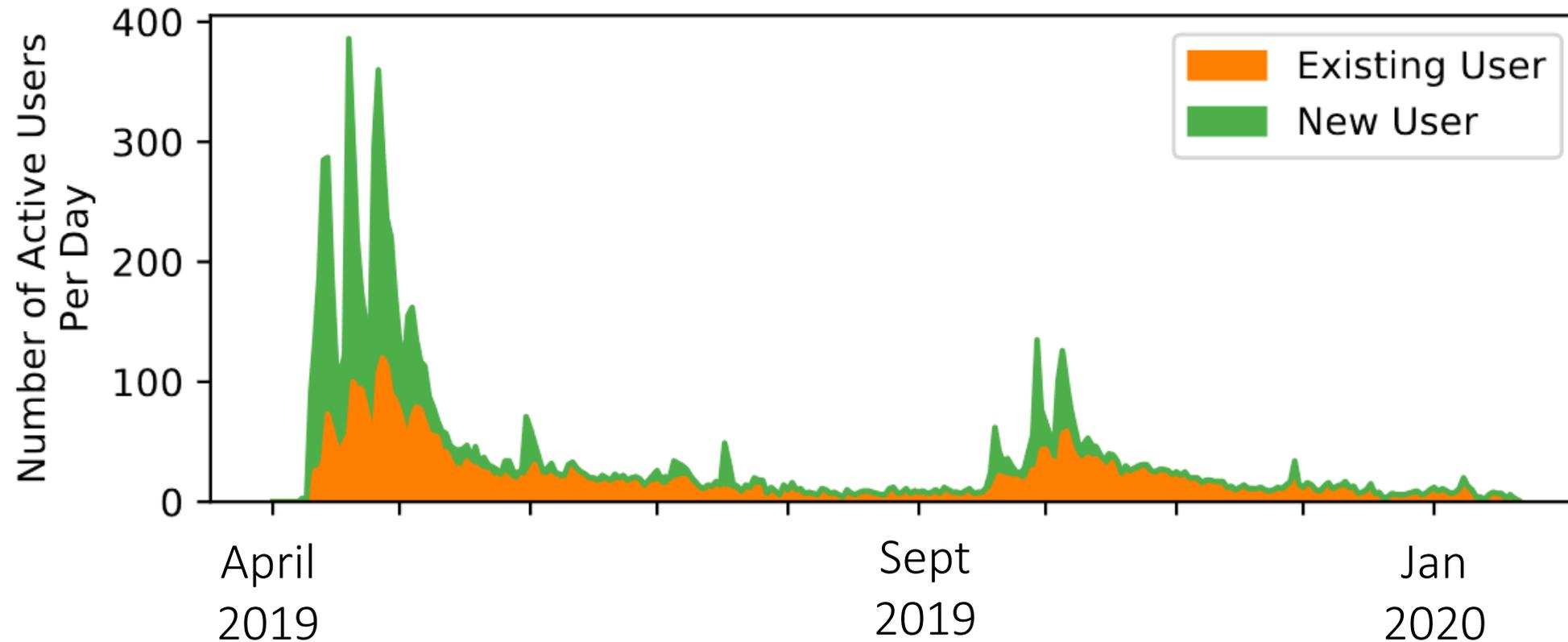
# Number of users and devices keep growing

Deployed since April 2019

125 daily active users in the first two months

5,404 users, 54,094 devices

63% users in US time zones, 28% in EU time zones



# Contributions of IoT Inspector



## Tool

5,400+ anonymous users since April '19  
Still gaining users and collecting data



## Dataset

54,000+ Internet-connected devices  
12,000+ device labels  
10+ organizations requesting data access



## Insight

Security: Non-encryption, security vulnerabilities →

Privacy: Tracking on smart TVs

## Users



The Washington Post  
The New York Times



## Collaborators



## Implications

Device certification? Min security standards?

Violation of COPPA?

# Insight: tracking on smart TVs

417 smart TVs in the dataset

22% of registered domains contacted by these smart TVs are advertising/tracking services, based on Disconnect List



Most TVs talk to what advertising/tracking companies?

A: Google

B: Amazon

C: Facebook

D: Others

# Insight: tracking on smart TVs

417 smart TVs in the dataset

22% of registered domains contacted by these smart TVs are advertising/tracking services, based on Disconnect List



doubleclick.net

34%

of smart TVs



scorecardresearch.com

14%

of smart TVs

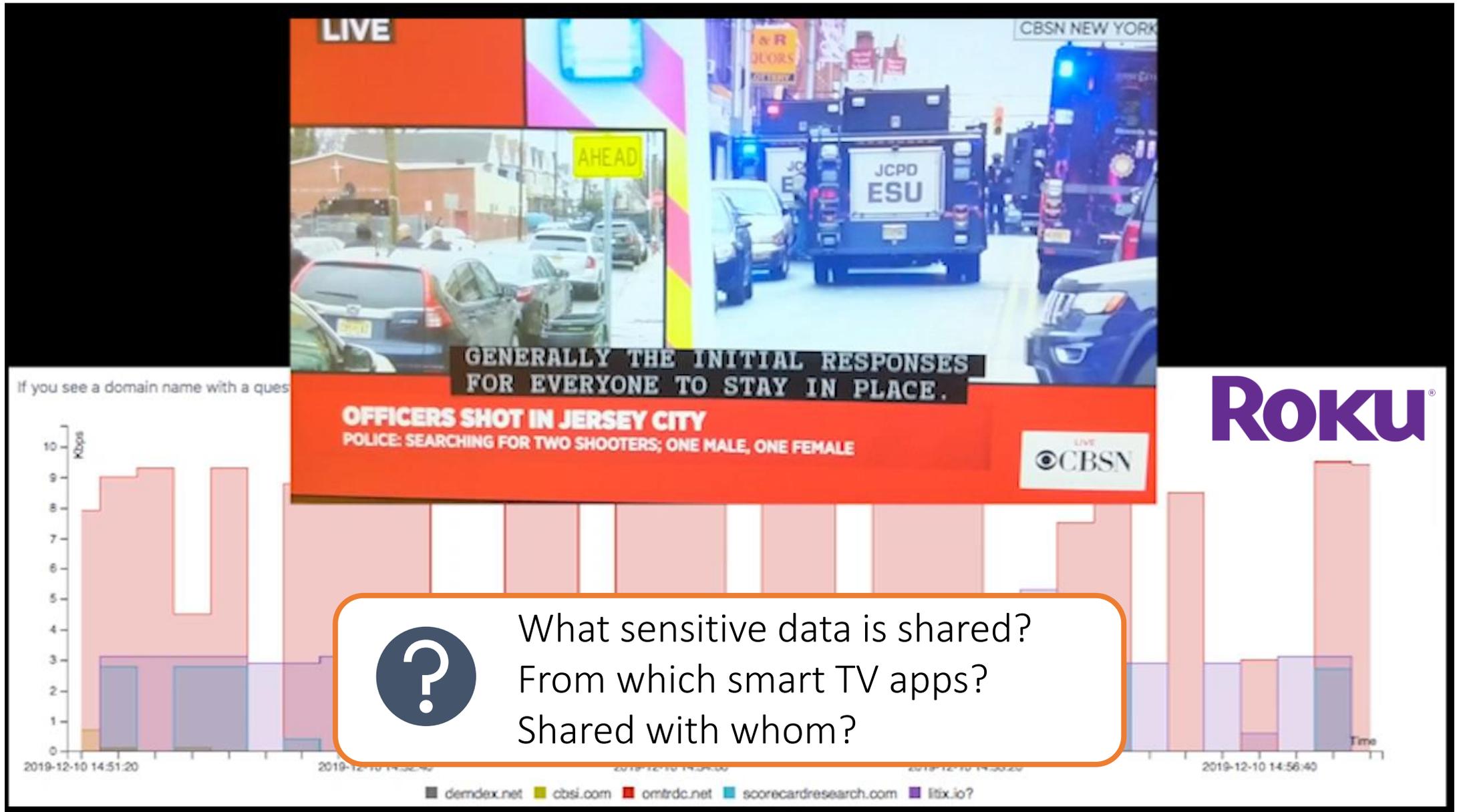


fwmrm.net

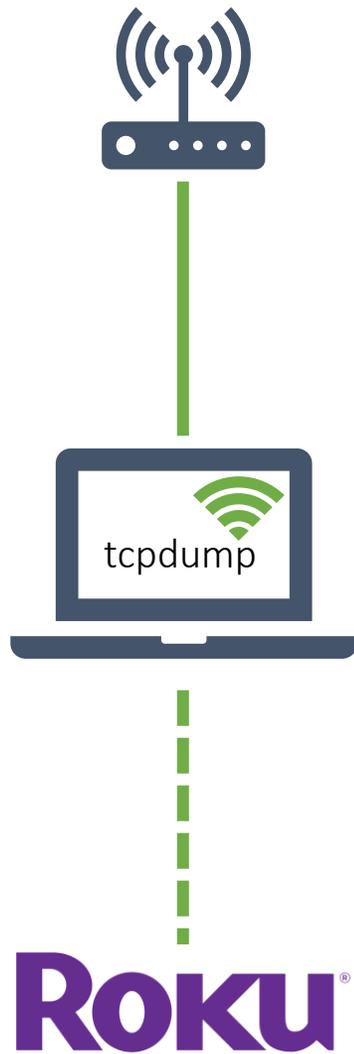
5%

of smart TVs

# Video: using IoT Inspector while watching live videos on CBS app



# Challenges of analyzing smart TV traffic in lab



**asiancrush** BROWSE MORE ✖

## Hwayi: A Monster Boy

2013 · South Korea · 125 min

Kidnapped as a child, Hwayi was raised by group of elite criminals to be the perfect assassin. Now - 14 years later - he is forced to make a hard choice when he learns the awful truth about his parents.

Thriller, Crime, Action  
Director: Jang Joon-hwan  
Starring: Cho Jin-woong, Jang Hyun-sung, Kim Sung-kyun

### Spotlight

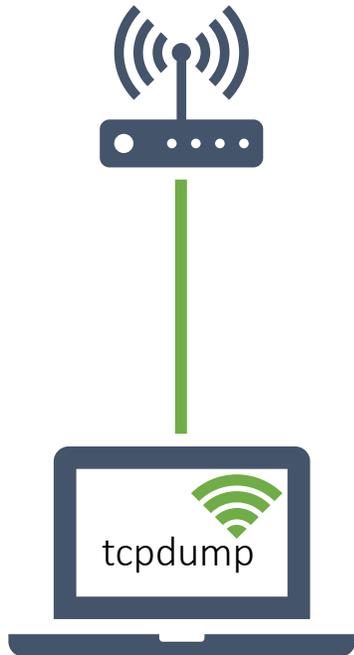
MONSTER BOY · INNOCENT THING · The Neighbor Zombie · A TALE OF TWO SISTERS · Sakura · Miracle Call No.7 · PERIOD PIECES · Vive L'Amour

### New Arrivals

Press Play to Add/Remove Favorite

FIST OF THE NORTH STAR

# Challenges of analyzing smart TV traffic in lab



**ROKU**

# SPOTX

So%20Young%20%3A%20Never%20Gone

HTTP outbound to 192.35.249.124:80 (DNS: search.spotxchange.com) (channel name: asiancrush)

```
GET /vast/3.0/146141?VPI[]=MP4&VPI[]=ROKU&app[name]=asiancrush&app[domain]=asiancrush.com&app[bundle]=com.dmr.asiancrush&player_width=1280&player_height=720&device[devicetype]=7&device[make]=Roku&device[model]=Roku&device[ifa]=39fc6352-aede-53f6-b3e3-58bf562bd074&ip_addr=128.112.139.195&cb=1557313464653&custom[movie_title]=So%20Young%20%3A%20Never%20Gone&custom[content_id]=3417&token[device_id]=39fc6352-aede-53f6-b3e3-58bf562bd074&token[connection]=wifi&token[category_ID]=241&token[category_Title]=Romance&device[dnt]=0&max_bitrate=7000 HTTP/1.1
```

Host: search.spotxchange.com

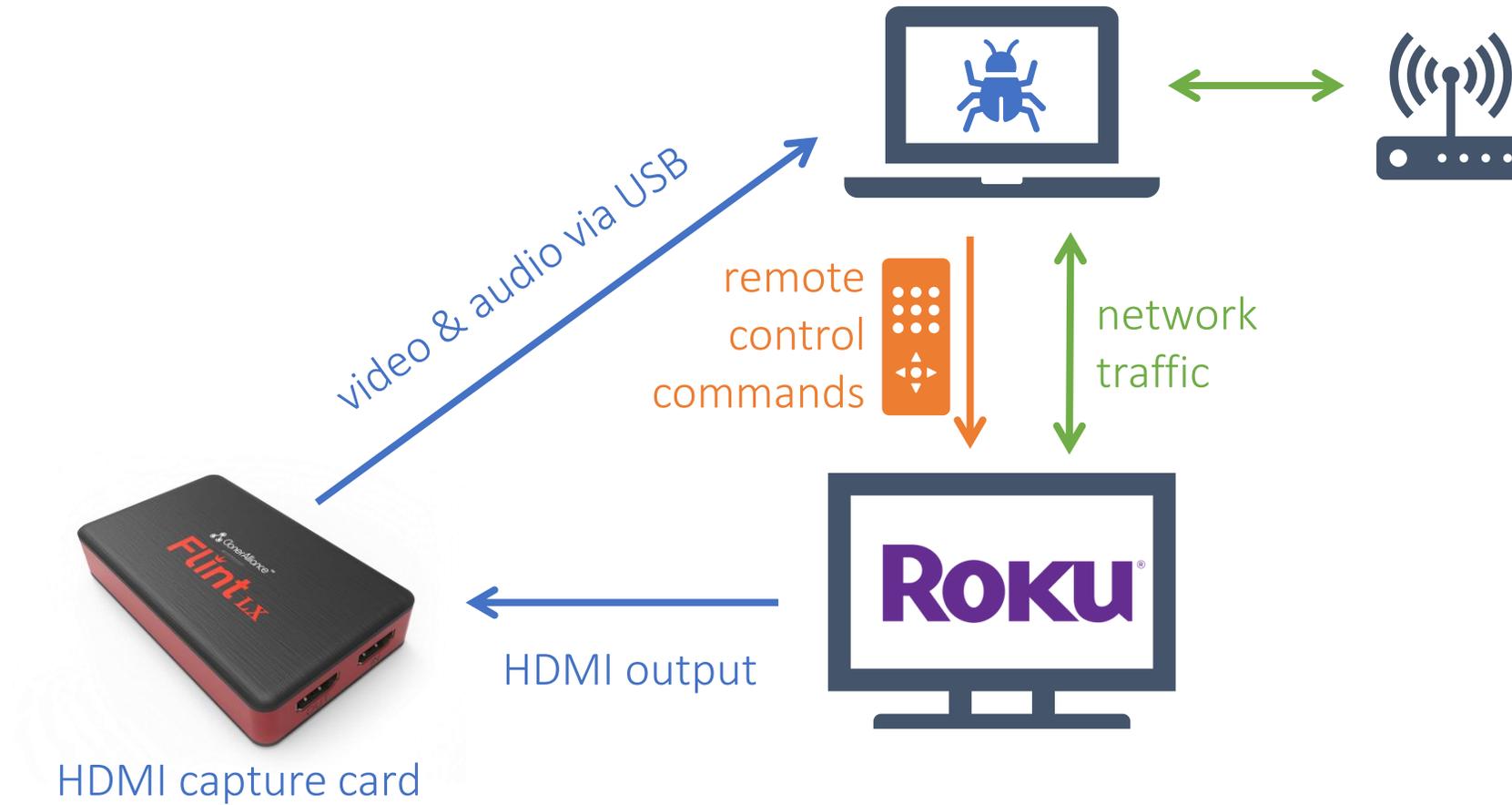
User-Agent: Roku/DVP-9.0 (519.00E04142A)

Accept: \*/\*



How to analyze the traffic of TV apps at scale?

# Automating interactions with smart TVs



# Findings: sensitive data shared with ad/tracking services

<b>Roku</b>	% apps	<b>amazon</b>	% apps
Ad ID			
App name			
Serial number			
Zip code			
City or state			

# Findings: sensitive data shared with ad/tracking services

<b>Roku</b>	% apps	<b>amazon</b>	% apps
Ad ID	32%		
App name	20%		
Serial number	11%		
Zip code	1%		
City or state	1%		

# Findings: sensitive data shared with ad/tracking services

	% apps		% apps
Ad ID	32%	Android ID	39%
App name	20%	Ad ID	22%
Serial number	11%	Serial number	10%
Zip code	1%	MAC address	5%
City or state	1%	WiFi SSID	2%



# Limited ad tracking (Roku) / No interest-based ads (Amazon)



Roku | Privacy gP 7:53 pm | Options \*

< Advertising  
Microphone

Limit ad tracking  
Reset advertising identifier

"Limit Ad Tracking" stops Roku from personalizing ads on this Roku device and sharing viewing data from streaming channels on this Roku device for measurement purposes. Press \* for more information.

Advertising ID

Interest-based Ads **ON**

Your Advertising ID

If you opt-out of interest-based ads on this device, apps will be instructed not to use the advertising ID to build profiles for advertising purposes or target you with interest-based ads, on this device. The advertising ID is a resettable, anonymous identifier that can be used to build profiles or show you interest-based ads.

# Poll: What happens when you disable ad tracking?

	<b>Roku</b>	% apps	<b>amazon</b>	% apps
<b>A</b>	Ad ID	32%	Android ID	39%
<b>B</b>	App name	20%	Ad ID	22%
<b>C</b>	Serial number	11%	Serial number	10%
<b>D</b>	Zip code	1%	MAC address	5%
<b>E</b>	City or state	1%	WiFi SSID	2%

# Finding: 0 apps sent Ad ID under “limited tracking”

<b>Roku</b>	% apps	<b>amazon</b>	% apps
Ad ID	32%	Android ID	39%
App name	20%	Ad ID	22%
Serial number	11%	Serial number	10%
Zip code	1%	MAC address	5%
City or state	1%	WiFi SSID	2%

0%





**FEDERAL TRADE  
COMMISSION**

September 4, 2019

## Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children’s Privacy Law

**FTC, New York Attorney General allege YouTube channels collected kids’ personal information without parental consent**

The “FTC and New York Attorney General allege that YouTube violated the COPPA Rule by collecting personal information—in the form of persistent identifiers that are used to track users across the Internet—from viewers of child-directed apps, without first notifying parents and getting their consent.”

# Privacy for children?



**FEDERAL TRADE  
COMMISSION**

September 4, 2019

## Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children's Privacy Law

**FTC, New York Attorney General allege YouTube channels collected kids' personal  
information without parental consent**

The “FTC and New York Attorney General allege that YouTube violated the COPPA Rule by collecting personal information—in the form of **persistent identifiers** that are used to track users across the Internet—from viewers of **child-directed apps**, **without** first notifying parents and getting their **consent**.”

# Findings from smart TV study: privacy leaks in child-directed apps

**Roku**

**amazon**

Number of apps

1,882

1,183

Number of child-directed apps

470

220

# Findings from smart TV study: privacy leaks in child-directed apps

**Roku**

**amazon**

Number of apps	1,882	1,183
Number of child-directed apps	470	220
Number of child-directed apps that leaked persistent IDs	34	23

# Examples of persistent IDs in child-directed apps



PBS KIDS Video

Oct 16, 2012 | by PBS KIDS

★★★★☆ ~ 4,547

App

FREE

Available instantly on compatible devices.

Leaked  
Android ID



Fun with Roblox by HappyKids.tv

Jan 4, 2019

★★★★☆ ~ 88

App

FREE

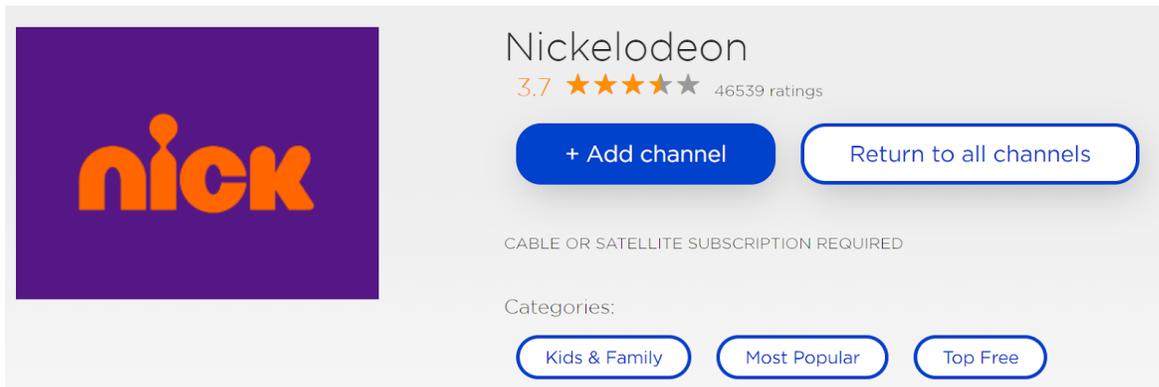
Available instantly on compatible devices.

Leaked  
Android ID  
Serial Number

# Examples of persistent IDs in child-directed apps



Leaked  
Ad ID  
Serial Number



Leaked  
Ad ID  
Serial Number



How to identify child-directed contents?  
What features? Manual labeling?

# My ongoing work with collaborators



IoT firewall



IoT privacy perception



Healthcare



Voice assistant privacy



Privacy law?

Cybersecurity insurance?