IotShark - Monitoring and Analyzing IoT Traffic

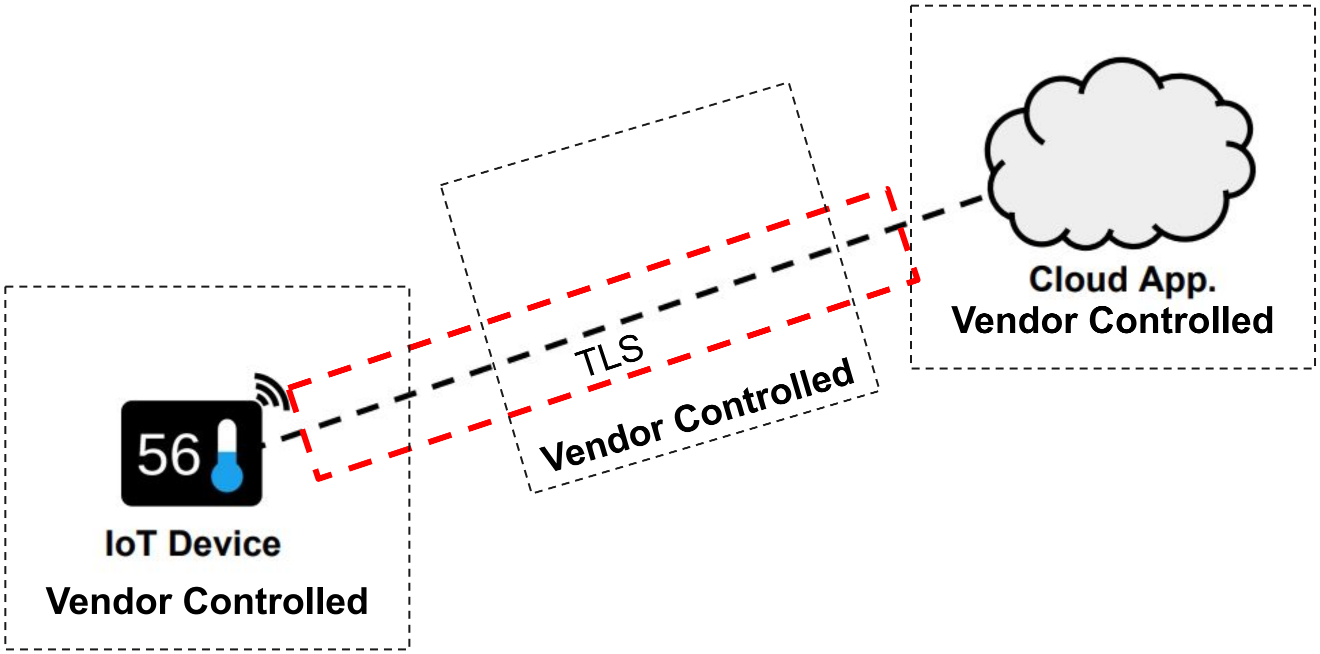
By Sahil, Max, and Daniel

Background & Motivation

IoT Proliferation

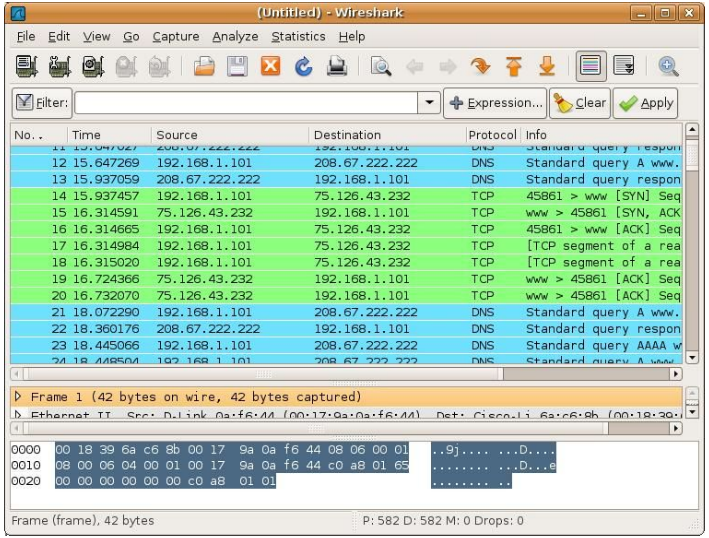
Internet of Things
30

IoT Communication



WireShark & EtterCap

- Powerful but complex
- Need networking knowledge
- No visualization of data

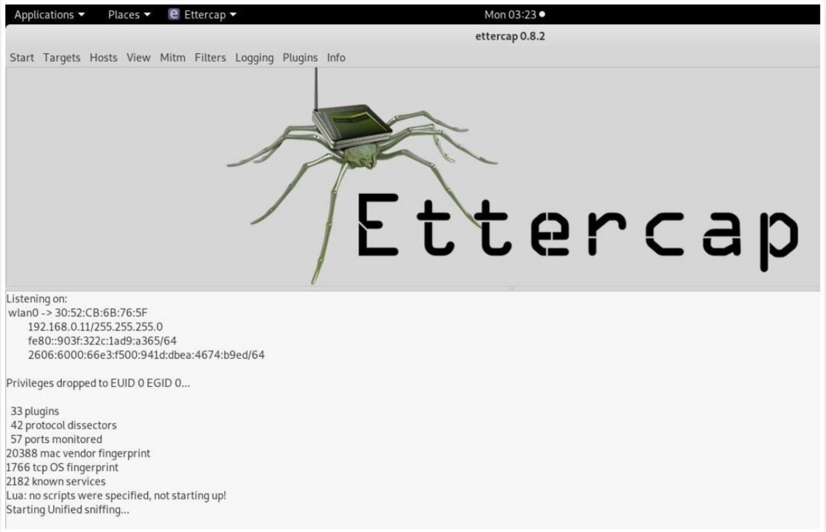


No.	Time	Source	Destination	Protocol	Info
11	15.647027	208.67.222.222	192.168.1.101	DNS	Standard query respon
12	15.647269	192.168.1.101	208.67.222.222	DNS	Standard query A www.
13	15.937059	208.67.222.222	192.168.1.101	DNS	Standard query respon
14	15.937457	192.168.1.101	75.126.43.232	TCP	45861 > www [SYN] Seq
15	16.314591	75.126.43.232	192.168.1.101	TCP	www > 45861 [SYN, ACK
16	16.314665	192.168.1.101	75.126.43.232	TCP	45861 > www [ACK] Seq
17	16.314984	192.168.1.101	75.126.43.232	TCP	[TCP segment of a rea
18	16.315020	192.168.1.101	75.126.43.232	TCP	[TCP segment of a rea
19	16.724366	75.126.43.232	192.168.1.101	TCP	www > 45861 [ACK] Seq
20	16.732070	75.126.43.232	192.168.1.101	TCP	www > 45861 [ACK] Seq
21	18.072290	192.168.1.101	208.67.222.222	DNS	Standard query A www.
22	18.360176	208.67.222.222	192.168.1.101	DNS	Standard query respon
23	18.445066	192.168.1.101	208.67.222.222	DNS	Standard query AAAA w
24	18.448504	192.168.1.101	208.67.222.222	DNS	Standard query A www.

```
▷ Frame 1 (42 bytes on wire, 42 bytes captured)
▷ Ethernet II, Src: D-Link_0a:f6:44 (00:17:9a:0a:f6:44), Dst: Cisco-Li_6a:c6:8b (00:18:39:
```

```
0000  00 18 39 6a c6 8b 00 17  9a 0a f6 44 08 06 00 01   ..9j.... ...D....
0010  08 00 06 04 00 01 00 17  9a 0a f6 44 c0 a8 01 65   ........ ...D...e
0020  00 00 00 00 00 00 c0 a8  01 01                     ........ ..
```

Frame (frame), 42 bytes   P: 582 D: 582 M: 0 Drops: 0

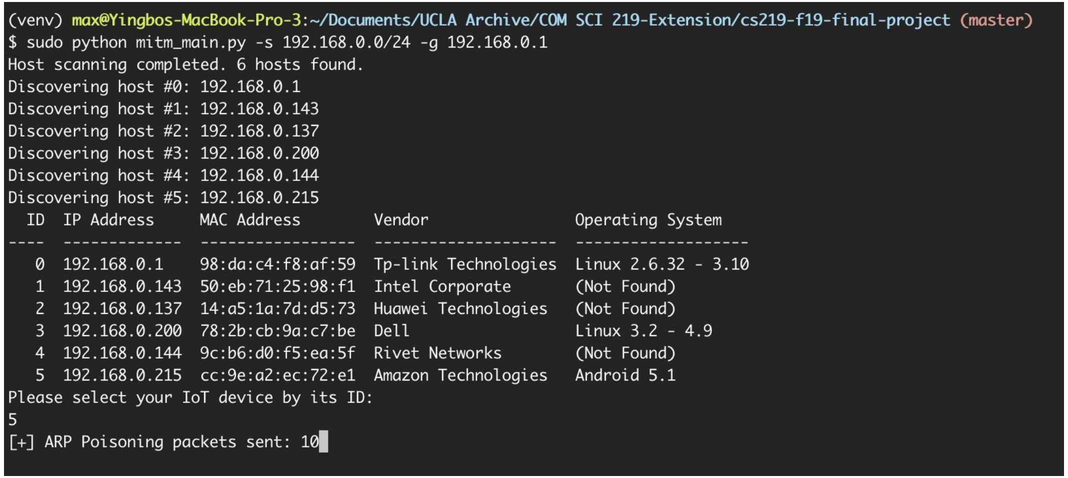


```
Listening on:
 wlan0 -> 30:52:CB:6B:76:5F
      192.168.0.11/255.255.255.0
      fe80::903f:322c:1ad9:a365/64
      2606:6000:66e3:f500:941d:dbea:4674:b9ed/64

Privileges dropped to EUID 0 EGID 0...

 33 plugins
 42 protocol dissectors
 57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...
```

IoTShark

Features - Scanning and Spoofing Network

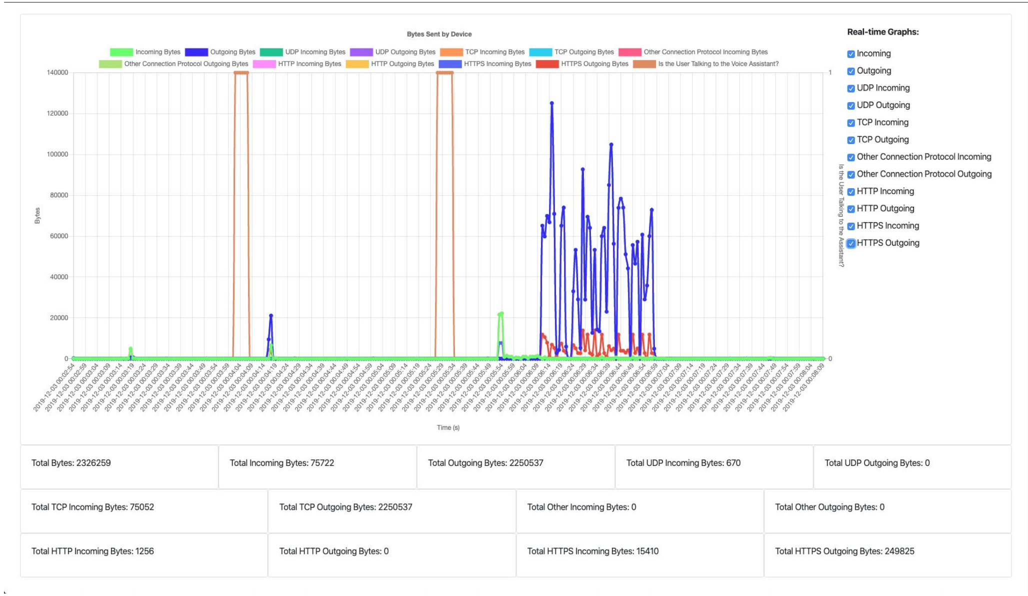
- Scan network to detect all devices via `nmap`
  - Specified subnet and gateway router IP
  - Common subnets of home Wi-Fi routers
- Present user with info on each
  - IP Address
  - MAC Address
  - Vendor
  - Operating System



```
(venv) max@Yingbos-MacBook-Pro-3:~/Documents/UCLA Archive/COM SCI 219-Extension/cs219-f19-final-project (master)
$ sudo python mitm_main.py -s 192.168.0.0/24 -g 192.168.0.1
Host scanning completed. 6 hosts found.
Discovering host #0: 192.168.0.1
Discovering host #1: 192.168.0.143
Discovering host #2: 192.168.0.137
Discovering host #3: 192.168.0.200
Discovering host #4: 192.168.0.144
Discovering host #5: 192.168.0.215
  ID  IP Address     MAC Address        Vendor               Operating System
----  -------------  -----------------  -------------------  -------------------
   0  192.168.0.1    98:da:c4:f8:af:59  Tp-link Technologies  Linux 2.6.32 - 3.10
   1  192.168.0.143  50:eb:71:25:98:f1  Intel Corporate      (Not Found)
   2  192.168.0.137  14:a5:1a:7d:d5:73  Huawei Technologies  (Not Found)
   3  192.168.0.200  78:2b:cb:9a:c7:be  Dell                 Linux 3.2 - 4.9
   4  192.168.0.144  9c:b6:d0:f5:ea:5f  Rivet Networks       (Not Found)
   5  192.168.0.215  cc:9e:a2:ec:72:e1  Amazon Technologies  Android 5.1
Please select your IoT device by its ID:
5
[+] ARP Poisoning packets sent: 10
```

Features - Sniffing and Dynamic Graph

- Intercepts packets of selected device
- Produces real-time graph of traffic
  - Indicate whether user is speaking
  - Toggle incoming vs outgoing bytes for:
    - UDP
    - TCP
    - HTTP
    - HTTPs
  - Aggregated data transmission statistics
- Creates csv dump of traffic



Real-time Graphs:

☑ Incoming
☑ Outgoing
☑ UDP Incoming
☑ UDP Outgoing
☑ TCP Incoming
☑ TCP Outgoing
☑ Other Connection Protocol Incoming
☑ Other Connection Protocol Outgoing
☑ HTTP Incoming
☑ HTTP Outgoing
☑ HTTPS Incoming
☑ HTTPS Outgoing

Total Bytes: 2326259

Total Incoming Bytes: 75722

Total Outgoing Bytes: 2250537

Total UDP Incoming Bytes: 670

Total UDP Outgoing Bytes: 0

Total TCP Incoming Bytes: 75052

Total TCP Outgoing Bytes: 2250537

Total Other Incoming Bytes: 0

Total Other Outgoing Bytes: 0

Total HTTP Incoming Bytes: 1256

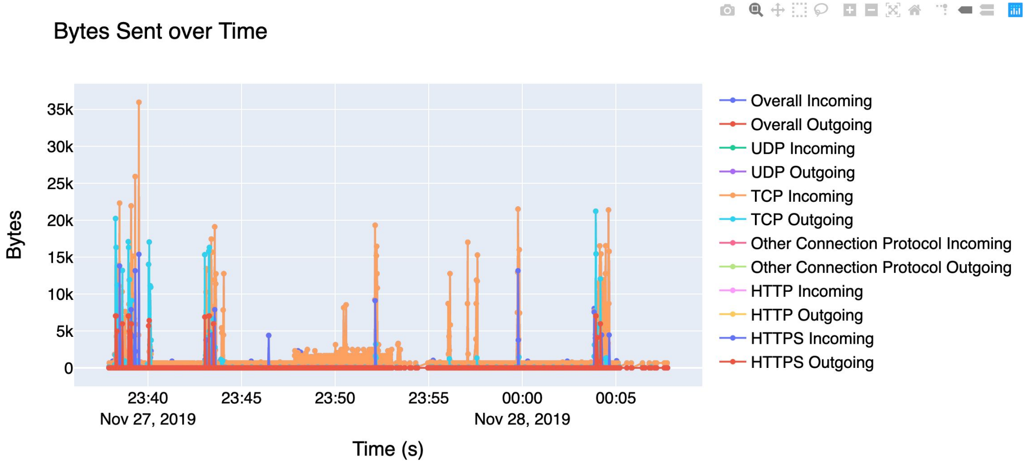
Total HTTP Outgoing Bytes: 0

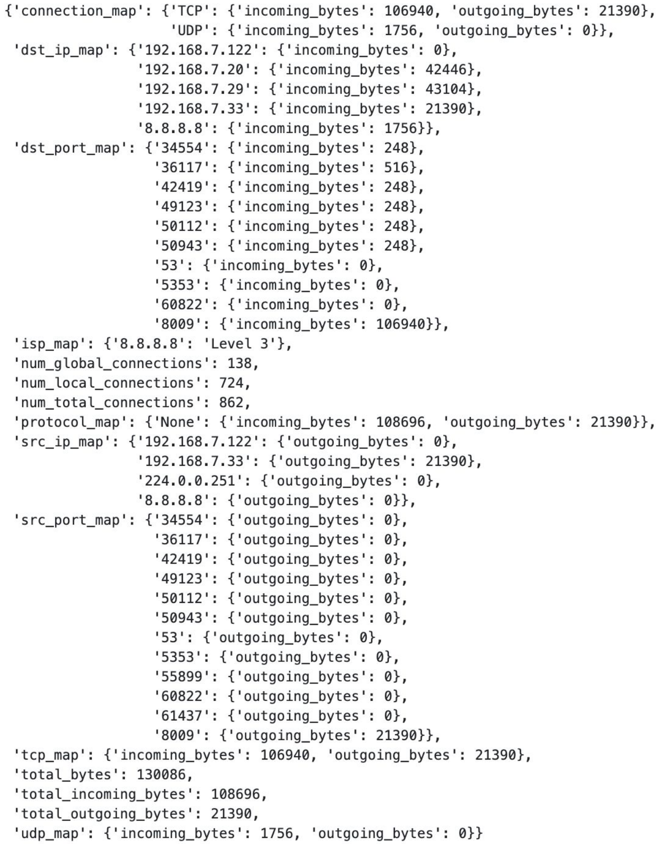
Total HTTPS Incoming Bytes: 15410

Total HTTPS Outgoing Bytes: 249825

Features - Static Graphs and Metrics

- Static graph based on historic csv
- Static analysis on data
  - ○ Bytes per port
  - ○ Bytes per ip
  - ○ ISP mapping



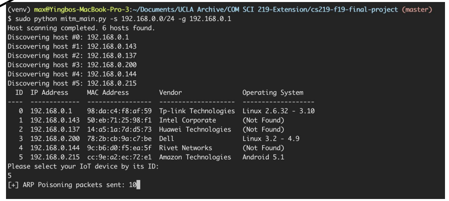


```
{'connection_map': {'TCP': {'incoming_bytes': 106940, 'outgoing_bytes': 21390},
                    'UDP': {'incoming_bytes': 1756, 'outgoing_bytes': 0}},
 'dst_ip_map': {'192.168.7.122': {'incoming_bytes': 0},
                '192.168.7.20': {'incoming_bytes': 42446},
                '192.168.7.29': {'incoming_bytes': 43104},
                '192.168.7.33': {'incoming_bytes': 21390},
                '8.8.8.8': {'incoming_bytes': 1756}},
 'dst_port_map': {'34554': {'incoming_bytes': 248},
                  '36117': {'incoming_bytes': 516},
                  '42419': {'incoming_bytes': 248},
                  '49123': {'incoming_bytes': 248},
                  '50112': {'incoming_bytes': 248},
                  '50943': {'incoming_bytes': 248},
                  '53': {'incoming_bytes': 0},
                  '5353': {'incoming_bytes': 0},
                  '60822': {'incoming_bytes': 0},
                  '8009': {'incoming_bytes': 106940}},
 'isp_map': {'8.8.8.8': 'Level 3'},
 'num_global_connections': 138,
 'num_local_connections': 724,
 'num_total_connections': 862,
 'protocol_map': {'None': {'incoming_bytes': 108696, 'outgoing_bytes': 21390}},
 'src_ip_map': {'192.168.7.122': {'outgoing_bytes': 0},
                '192.168.7.33': {'outgoing_bytes': 21390},
                '224.0.0.251': {'outgoing_bytes': 0},
                '8.8.8.8': {'outgoing_bytes': 0}},
 'src_port_map': {'34554': {'outgoing_bytes': 0},
                  '36117': {'outgoing_bytes': 0},
                  '42419': {'outgoing_bytes': 0},
                  '49123': {'outgoing_bytes': 0},
                  '50112': {'outgoing_bytes': 0},
                  '50943': {'outgoing_bytes': 0},
                  '53': {'outgoing_bytes': 0},
                  '5353': {'outgoing_bytes': 0},
                  '55899': {'outgoing_bytes': 0},
                  '60822': {'outgoing_bytes': 0},
                  '61437': {'outgoing_bytes': 0},
                  '8009': {'outgoing_bytes': 21390}},
 'tcp_map': {'incoming_bytes': 106940, 'outgoing_bytes': 21390},
 'total_bytes': 130086,
 'total_incoming_bytes': 108696,
 'total_outgoing_bytes': 21390,
 'udp_map': {'incoming_bytes': 1756, 'outgoing_bytes': 0}}
```

Implementation

Python

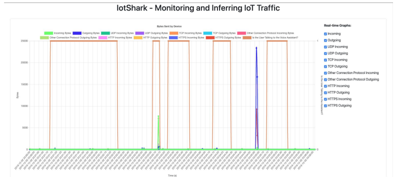
scapy
PyShark

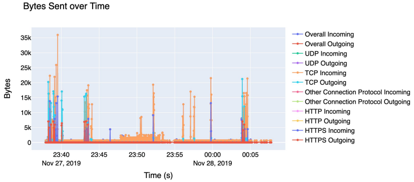


```
(venv) max@Yingbos-MacBook-Pro-3:~/Documents/UCLA Archive/COM SCI 219-Extension/cs219-f19-final-project (master)
$ sudo python mitm_main.py -s 192.168.0.0/24 -g 192.168.0.1
Host scanning completed. 6 hosts found.
Discovering host #0: 192.168.0.1
Discovering host #1: 192.168.0.143
Discovering host #2: 192.168.0.137
Discovering host #3: 192.168.0.200
Discovering host #4: 192.168.0.144
Discovering host #5: 192.168.0.215
  ID  IP Address     MAC Address        Vendor                Operating System
----  -------------  -----------------  --------------------  ------------------
   0  192.168.0.1    98:da:c4:f8:af:59  Tp-link Technologies  Linux 2.6.32 - 3.10
   1  192.168.0.143  50:eb:71:25:98:f1  Intel Corporate       (Not Found)
   2  192.168.0.137  14:a5:1a:7d:d5:73  Huawei Technologies   (Not Found)
   3  192.168.0.200  78:2b:cb:9a:c7:be  Dell                  Linux 3.2 - 4.9
   4  192.168.0.144  9c:b6:d0:f5:ea:5f  Rivet Networks        (Not Found)
   5  192.168.0.215  cc:9e:a2:ec:72:e1  Amazon Technologies   Android 5.1
Please select your IoT device by its ID:
5
[+] ARP Poisoning packets sent: 10
```

Flask, JavaScript, HTML/CSS

plotly
chart.js



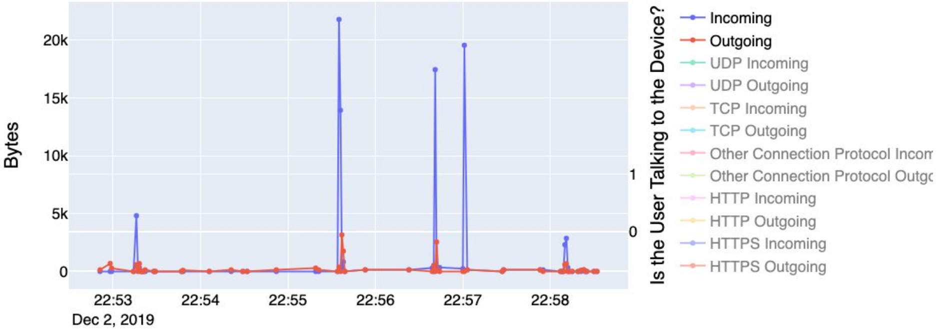


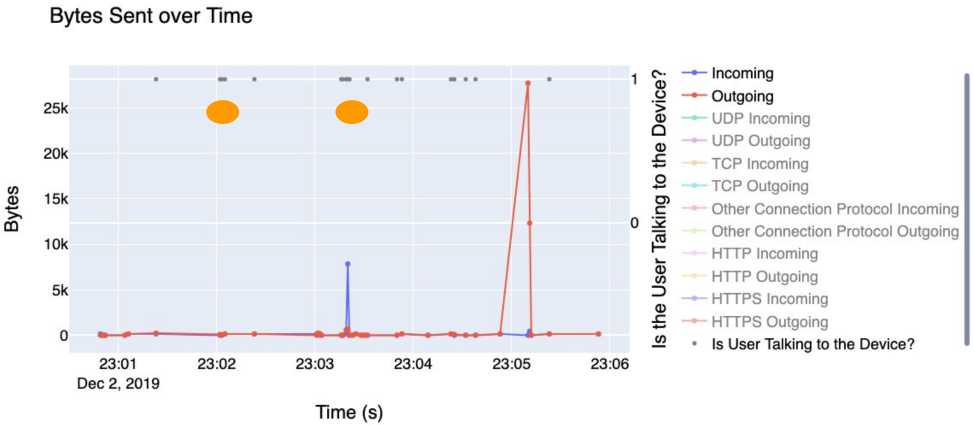
~1500 LOC + HTML/CSS

Evaluation:
Amazon Echo vs. Google Home

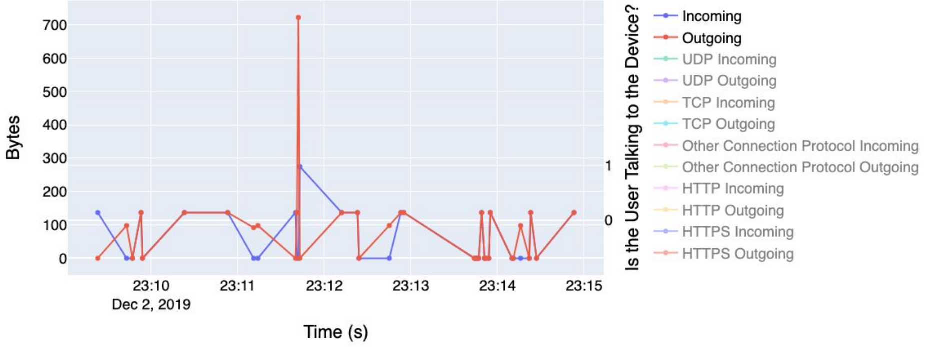
Echo Dot Traces

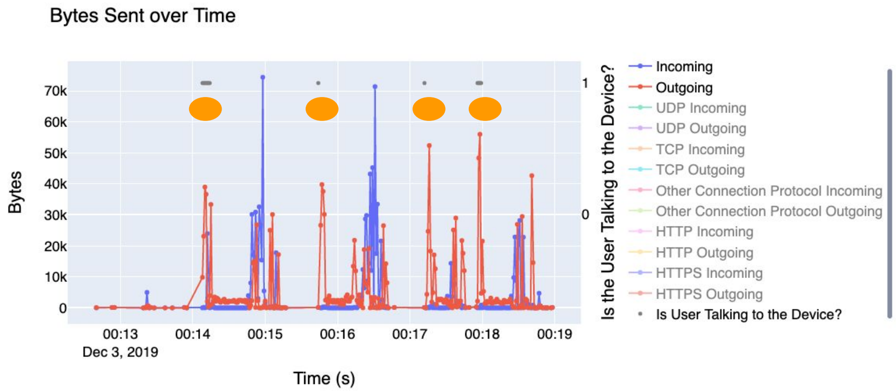
Mic Off



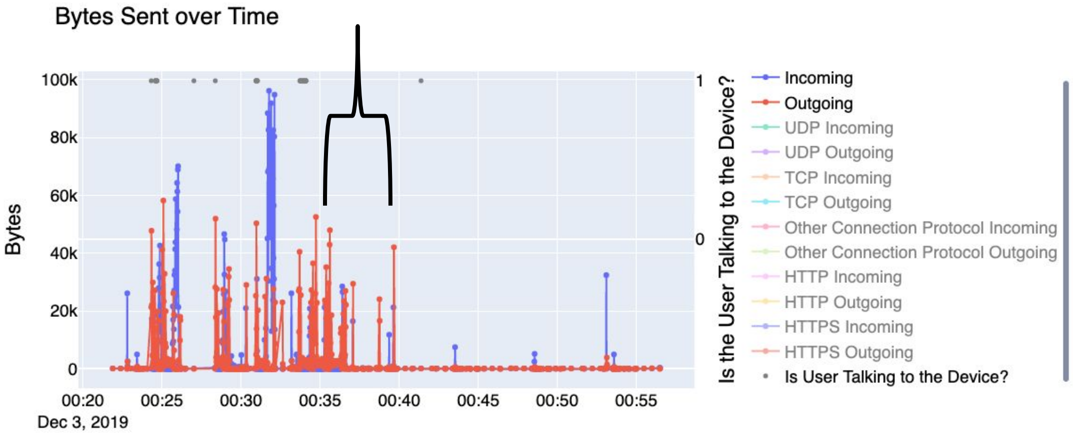


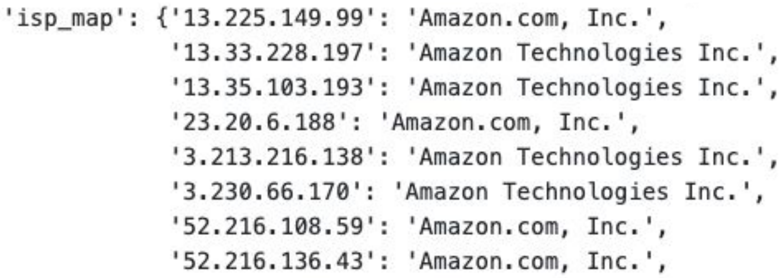
Mic On





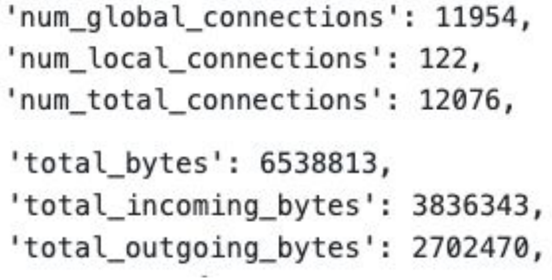
Echo Dot Traces (cont’d)





```
'isp_map': {'13.225.149.99': 'Amazon.com, Inc.',
            '13.33.228.197': 'Amazon Technologies Inc.',
            '13.35.103.193': 'Amazon Technologies Inc.',
            '23.20.6.188': 'Amazon.com, Inc.',
            '3.213.216.138': 'Amazon Technologies Inc.',
            '3.230.66.170': 'Amazon Technologies Inc.',
            '52.216.108.59': 'Amazon.com, Inc.',
            '52.216.136.43': 'Amazon.com, Inc.',
```

…… (33 IP addresses in total)

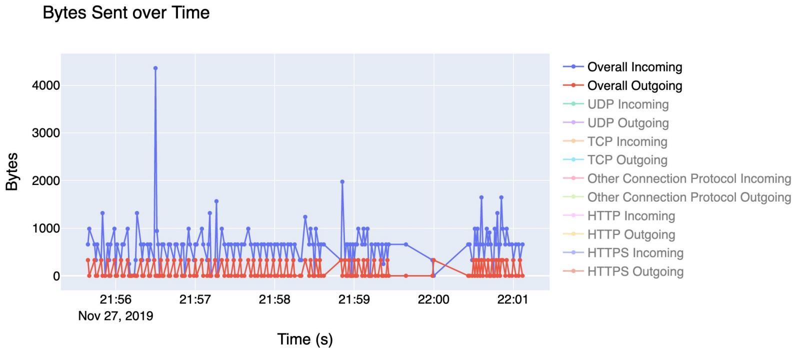


```
'num_global_connections': 11954,
'num_local_connections': 122,
'num_total_connections': 12076,

'total_bytes': 6538813,
'total_incoming_bytes': 3836343,
'total_outgoing_bytes': 2702470,
```

Home Mini Traces

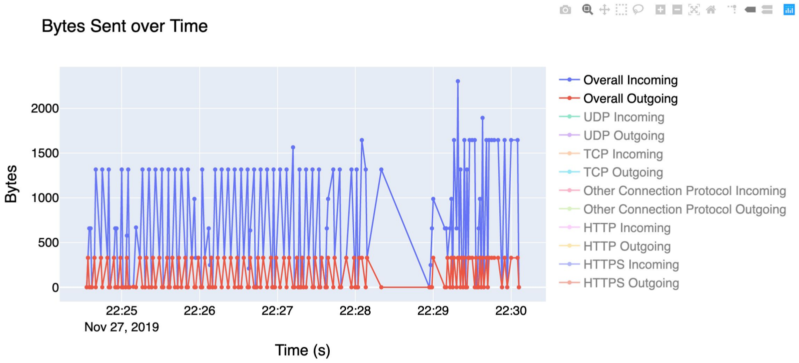
Mic Off

csv/packetdump_192.168.7.122_1574920530_5MinMicOffNoTalk.csv

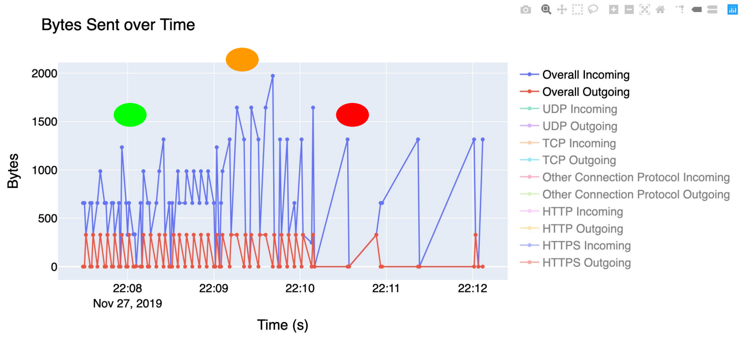


Mic On

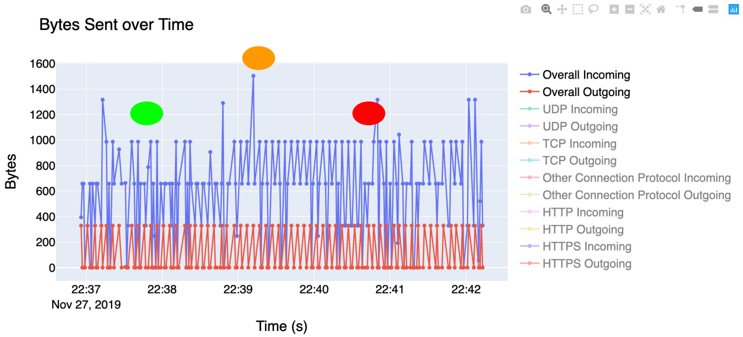
csv/packetdump_192.168.7.122_1574922266_5MinMicOnNoTalk.csv



csv/packetdump_192.168.7.122_1574921243_5MinMicOffYesTalk.csv

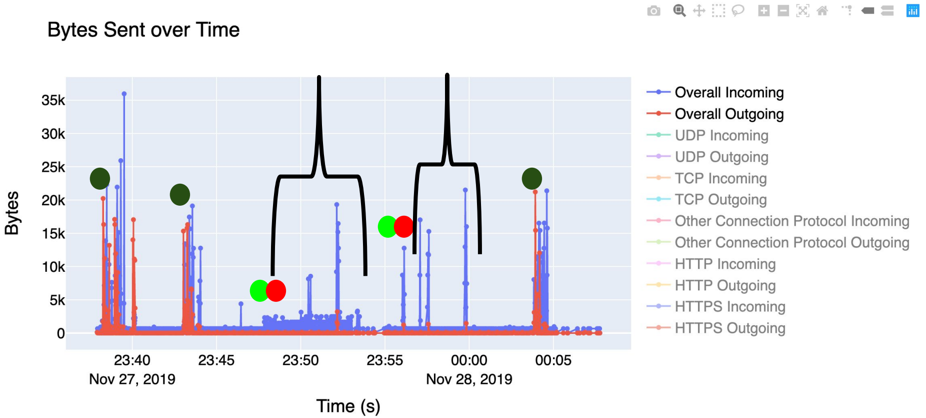


csv/packetdump_192.168.7.122_1574923008_5MinMicOnYesTalk.csv



Home Mini Traces (cont’d)

csv/packetdump_192.168.7.122_1574926667_30MinMicOnYesTalk.csv



```
'isp_map': {'104.154.127.47': 'Google LLC',
            '151.101.52.246': 'Fastly',
            '35.186.224.44': 'Google LLC',
            '35.186.224.53': 'Google LLC',
            '8.8.8.8': 'Level 3'},
'num_global_connections': 6568,
'num_local_connections': 2460,
'num_total_connections': 9028,
'total_bytes': 1973534,
'total_incoming_bytes': 1558260,
'total_outgoing_bytes': 415274,
```

Future Work/Discussion

- Automatic trace Inference
  - Eg. Spotify trace, class of questions, pre-fetching
  - Requires:
    - More data
    - ML Model
- Anomaly Detection
  - Eg. Random spikes of traffic
  - Requires:
    - More data!
    - Comparison thresholds
- Interpretable for average IoT user
- Trace other devices
  - Eg. Apple HomePod, Phone Assistants, Ring

Questions?