

Monitoring Network Traffic on Mobile Devices

Kristin Albright, Will Gershman, Fabricio Rua-Sanchez,
Hashir Safdar, Rudra Subramanian

Our Question

What information is your phone sending out? And to **whom**?

Why Do We Care?

- Types of Information
- Data Collection
- Personal Privacy

Why Do We Care?

- **Types of Information***

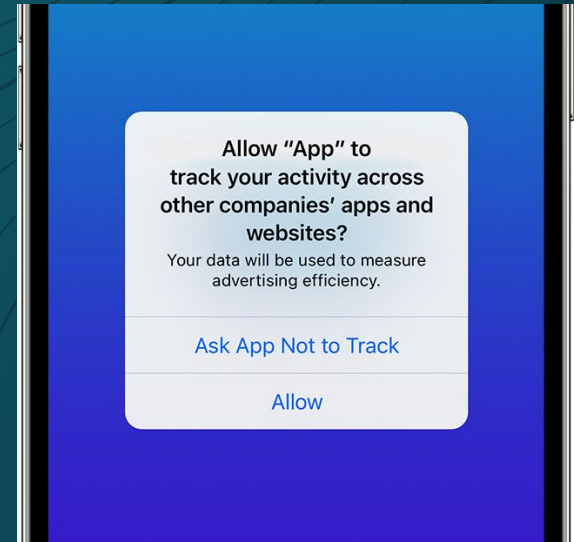
- What kind of information is sent out about you?
- Email addresses
- IP addresses
- Location information**
- Unique Device Identifier (UDID)

*(Sar 2014)

** (Das 2017) 5

Why Do We Care?

- Response from Apple/Google
 - App tracking transparency



Why Do We Care?

- Response from Apple/Google
 - App stores

The image shows a screenshot of Apple's privacy settings page, divided into two main sections: 'Data Used to Track You' and 'Data Linked to You'.

Data Used to Track You
The following data may be used to track you across apps and websites owned by other companies:

- Contact Info
- Identifiers
- Other Data

Data Linked to You
The following data may be collected and linked to your identity:




- Health & Fitness
- Financial Info
- Contact Info
- User Content
- Browsing History
- Usage Data
- Diagnostics
- Purchases
- Location
- Contacts
- Search History
- Identifiers
- Sensitive Info
- Other Data

Why Do We Care?

Facebook

Meta Platforms, Inc.

Showing permissions for all versions of this app

-  Device & app history
 - retrieve running apps
-  Storage
 - read the contents of your USB storage
 - modify or delete the contents of your USB storage
-  Location
 - precise location (GPS and network-based)
 - approximate location (network-based)

Updates to Facebook may automatically add additional capabilities within each group. [Learn more](#)

Cancel

Why Do We Care?

- **Data Collection**

- When is data collection happening?
- Idle phone
- App is in use
- After an app is deleted

Why Do We Care?

- **Personal Privacy**

- How many puzzle pieces of a person is required to build a profile?
- Facebook is known to successfully predict race, religion, and sexual orientation using other factors*

What Do We Want to Observe?

- What information is being received
 - We expect a social media app to receive feed updates
 - Is there anything unexpected we're receiving?
- What information is being sent
 - Anything unexpected to someone unexpected?

What Can We Observe?

- **The Encryption Problem**

- Where data is being sent
- Where data is coming from
- How much data is being sent
- When data is being sent

What Do We Want to Know?

- How much information is being sent out?
 - Total number of packets
 - Size of packets
 - Frequency of packets being sent
- What information is in these packets?
 - Are apps required to tell us what information they track?

What Do We Want to Know?

- Deactivation vs. Deletion
 - Is there a way to revoke consent for information gathering?
- The big players
 - Is there a way to avoid giving information to specific tech giants i.e. Amazon, Google, Facebook?

What Have Other People Done?

- (Data) packet tracing through third-party applications
- How widely used is encryption for social media information?
- Is it possible to access personal information from applications downloaded on a computer?
- Many of the same barriers that impacted us have also been problems in the past

Main Barriers

- Encryption
- Resources:
 - Number/types of devices
 - Time

□ Main Barriers

□ Encryption

- Tech companies closely guard encryption models and are not required to reveal the data they collect
- Research studies often have to exploit security risks in order to study the data*

□ Main Barriers

□ Resources

- Many platforms take long-term **inactivity** into account when it comes to data collection
- We weren't able to spend this amount of time on one platform due to the number of accounts/devices available

Methods

How do we collect data?

- ❑ What we wish we could observe
- ❑ Why we can't: encryption
- ❑ What we can observe
- ❑ Packet captures: .pcap files

```
00 1a 11 00 00 02 00 1a 11 00 00 01 08 00 45 00 .....E
01 41 db d8 40 00 40 06 54 18 0a 08 00 01 22 6b ..A-@@-T-...k
dd 52 d5 f8 00 50 c5 a3 30 1e 3a 5c cf e3 50 18 ..R.P.0-)-P
ff ff b2 1f 00 00 47 45 54 20 2f 73 75 63 63 65 .....#...Z...
73 73 2e 74 78 74 3f 69 70 76 3a 20 48 54 54 50 ..#...#...
2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 64 65 74 65 ..f...f...
63 74 70 6f 72 74 61 6c 2e 66 69 72 65 66 6f 78 ..e...e...
2e 63 6f 6d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 ..o/97.0 F irefox/9
3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 41 ..ndroid 1 2; Mobil
6e 64 72 6f 69 64 20 31 32 3b 20 4d 6f 62 69 6c ..e; rv:97 .0) Geck
65 3b 20 72 76 3a 39 37 2e 30 29 20 47 65 63 6b ..o/97.0 F irefox/9
6f 2f 39 37 2e 30 20 46 69 72 65 66 6f 78 2f 39 ..7.0-Acc ept: /*/
37 2e 30 0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 ..-Accept -Languag
0d 0a 41 63 63 65 70 74 2d 4c 61 6e 67 75 61 67 ..e: en-US -Accept
65 3a 20 65 6e 2d 55 53 0d 0a 41 63 63 65 70 74 ..-Encodin g: gzip,
2d 45 6e 63 6f 64 69 6e 67 3a 20 67 7a 69 70 2c ..deflate -Connec
20 64 65 66 6c 61 74 65 0d 0a 43 6f 6e 6e 65 63 ..tion: ke ep-alive
74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 ..-Pragma : no-cac
0d 0a 50 72 61 67 6d 61 3a 20 6e 6f 2d 63 61 63 ..he--Cach e-Contro
68 65 0d 0a 43 61 63 68 65 2d 43 6f 6e 74 72 6f ..l: no-ca che....
6c 3a 20 6e 6f 2d 63 61 63 68 65 0d 0a 0d 0a ..
```

→ HTTPS request

← HTTP request

```
00 1a 11 00 00 02 00 1a 11 00 00 01 08 00 45 00 .....E
02 40 10 c6 40 00 40 06 6c d8 0a 08 00 01 9d f0 ..! .4. .... ] \ . P
13 21 80 34 01 bb f0 a3 fd 5d 0f 5c 04 c0 50 10 ..#...#...Z...
ff ff 10 84 00 00 23 c8 a7 cb b9 5a cd c7 01 c5 ..$-z-...
cf 24 b8 2d 7a 17 e8 2d 1d ff 93 af 93 d1 da 82 ..Y...ROV... "Ir-n
59 b5 f7 ba 52 4f 76 9c 97 c5 22 49 72 fa fd 6e ..s...~.y.,/I
a6 c3 f7 73 aa 9b 13 07 7e ae 79 bf 2c c7 2f 49 ..a-a{.../..J(~
16 61 e7 ed 61 7b 0b f5 e4 2f 0c 94 4a 28 7e cd ..b-b? {+Z...
e0 af e5 62 1a dd 4d 3f 7b 90 2b ee 5a 91 f0 85 ..g-`-R-...d7
67 86 ae 60 a8 f8 52 f3 02 fe bf b9 ed 64 37 9e ..AO...K...EW...d
41 4f e1 b1 99 4b 17 07 45 57 d9 fa 93 09 64 04 ..*...w...`
2a aa 8e e7 e1 c2 9f c7 77 f4 94 9d 1f 1e 60 a5 ..1 z...ed-Q...
9b bf 31 fe 7a b9 b8 0e c5 65 64 bb e5 51 bc b0 ..s-A-K- &-W-3
73 c4 41 ef 0d 4b ea 8f 26 12 97 57 af 98 a8 33 ..
```

Basic Experiment

- ❑ Prep phone
- ❑ Start observing
- ❑ Do something
- ❑ Stop observing

Experiment Procedure

- Packet capture performed in several segments
- TikTok experiment example:
 - Fresh
 - Installed, not launched
 - Logged in
 - Browsing (not idle)
 - Restarted
 - Uninstalled

Specifics

- Android and Apple devices
- Personal and factory reset devices
- Monitored in idle for control
- Third party software to monitor traffic
- Pcap files used to gather and analyze data



Android: tPacket-Capture

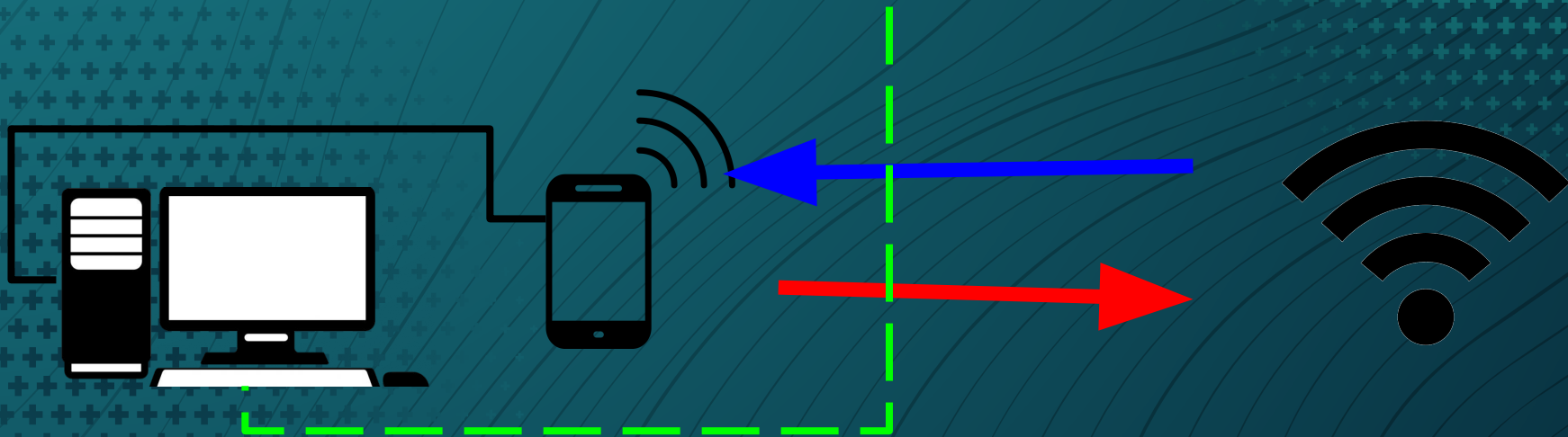
- Monitors traffic on device through built-in VPN service from Android OS
- Saves data as “packet capture”, or .pcap





Apple: Wireshark Capture

- Uses device's UDID (unique device identifier) to create a virtual interface for a device connected via USB
- Wireshark monitors traffic through the virtual interface
- Saves data as "packet capture", or .pcap



Wireshark: free & open source packet analysis

- Deeply customizable and powerful analysis tool
- Name resolution of IP addresses
- Port filtering
- Simple conversion to .csv



Ethernet · 2

IPv4 · 49

IPv6

TCP · 193

UDP · 14

Address

Packets

Bytes

Tx Packets

Tx Bytes

Rx Packets

Rx Bytes

a23-48-208-19.deploy.static.akamaitechnologies.com

34 9281

17 7167

17

a23-48-208-25.deploy.static.akamaitechnologies.com

346 768 k

163 740 k

183

a23-48-208-48.deploy.static.akamaitechnologies.com

31 6240

16 4126

15

a23-48-208-56.deploy.static.akamaitechnologies.com

349 113 k

174 21 k

175

a23-77-218-147.deploy.static.akamaitechnologies.com

901 245 k

451 33 k

450

a23-77-218-153.deploy.static.akamaitechnologies.com

40 11 k

19 9456

21

a23-77-218-225.deploy.static.akamaitechnologies.com

53 15 k

26 4165

27

99.215.102.34.bc.googleusercontent.com

24 2410

10 540

14

103.140.107.34.bc.googleusercontent.com

420 177 k

206 131 k

214

231.176.107.34.bc.googleusercontent.com

57 6959

28 3081

29

4.163.120.34.bc.googleusercontent.com

324 63 k

161 28 k

163

ec2-34-213-128-33.us-west-2.compute.amazonaws.com

48 11 k

24 7422

24

248.69.201.35.bc.googleusercontent.com

34 5500

16 2800

18

ec2-44-228-84-60.us-west-2.compute.amazonaws.com

0 1031

1 216

5

Using domains to learn about sent data: What apps are doing what?

Wireshark · Endpoints · 1.19 Will FB 1.pcap

Ethernet · 2

IPv4 · 36

IPv6

TCP · 76

UDP · 20

Address

Packets

Bytes

instagram-p3-shv-01-msp1.fbcdn.net

2 108

edge-mqtt-shv-02-ort2.facebook.com

56 12 k

whatsapp-chatd-msgr-mini-edge-shv-01-ort2.facebook.com

24 2849

157.185.177.248

4 240

151.101.193.35

20 10 k

151.101.66.133

24 8134

151.101.2.133

6 4927



Apple: Factory Reset Device

- Goal: Isolate traffic to a targeted application
- Process:
 - Reset iPhone with as minimal external connections as possible
 - Monitor idle traffick for control
 - Download targeted app and create account with google voice number
 - Monitor traffic throughout experiments
- Experiments were repeated to observe consistency of results

Data Analysis

- Import CSV to Pandas
- Structure data
- Graph!

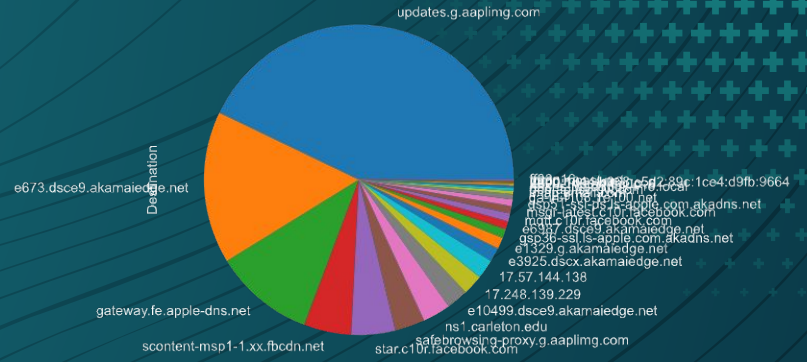
The logo for matplotlib, featuring the word "matplotlib" in a blue sans-serif font. The "o" in "plot" is replaced by a circular icon containing a colorful pie chart with segments in yellow, green, and red.The logo for Jupyter, consisting of a stylized orange and grey circular icon on the left and the word "jupyter" in a grey sans-serif font on the right.The logo for pandas, featuring a stylized icon of vertical bars in blue and yellow on the left and the word "pandas" in a blue sans-serif font on the right.

Data Analysis

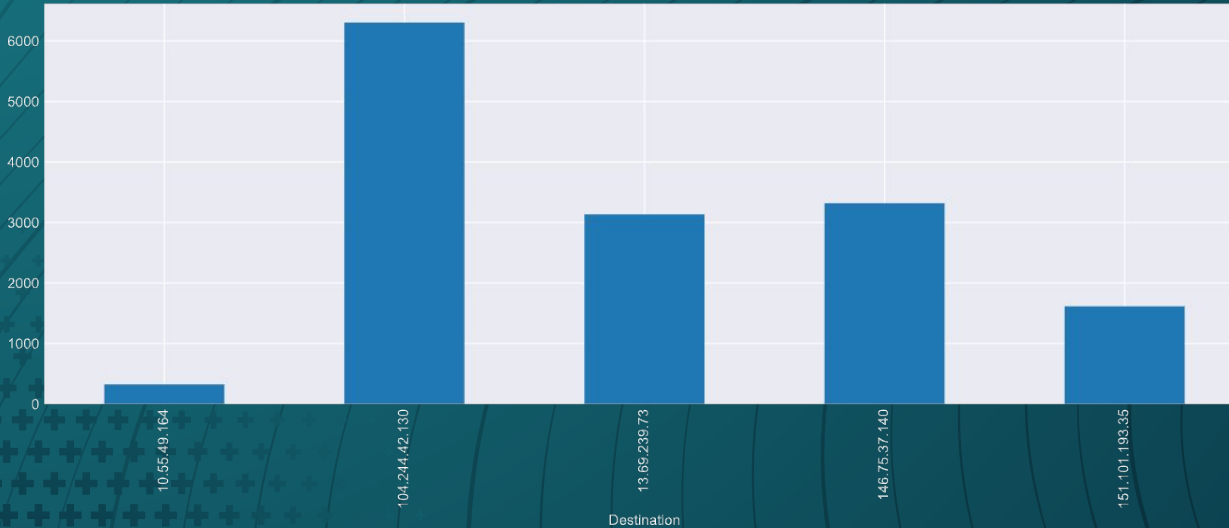
| Time | Source | Destination | Protocol | Length |
|------|---|--------------------------|----------|--------|
| 72.4 | 10.133.147.141 | ord38s32-in-f2.1e100.net | TLSv1.2 | 438 |
| 72.4 | ord38s32-in-f2.1e100.net | 10.133.147.141 | TLSv1.2 | 1000 |
| 76.2 | 10.133.147.141 | ns1.carleton.edu | DNS | 55 |
| 78.9 | geo-applefinance-cache.internal.query.g03.yahoo.com | 10.133.147.141 | TCP | 611 |

Data Analysis

Outgoing packets



Average packet size of top 5 destinations

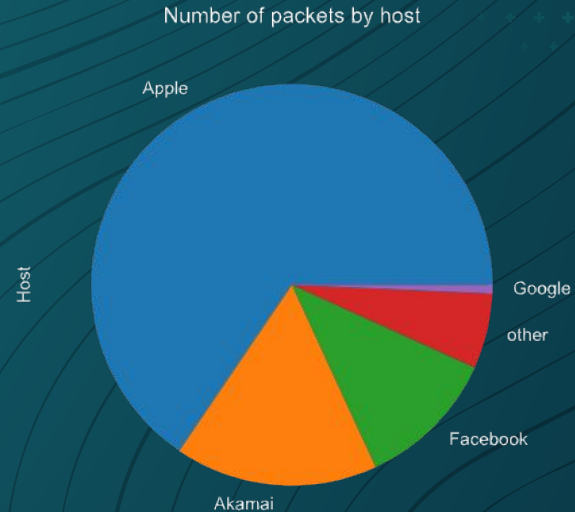


Data Analysis

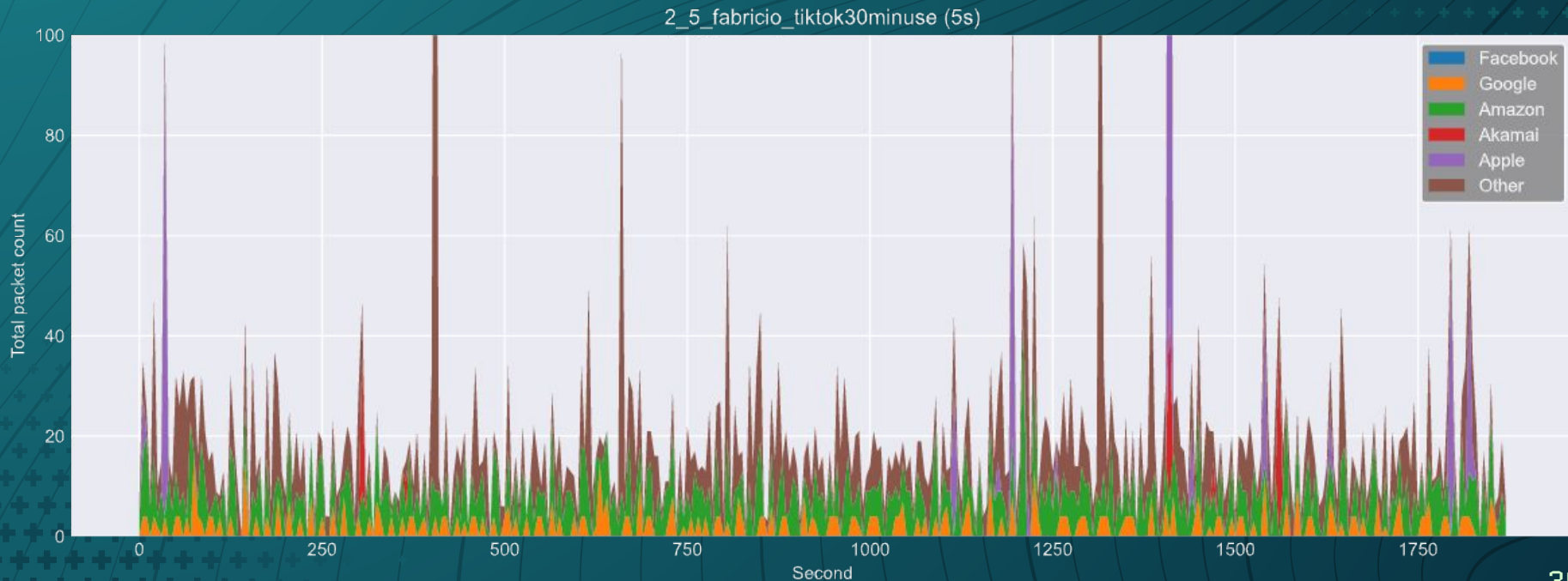
| Time | Source | Destination | Protocol | Length | Host |
|------|---|--------------------------|----------|--------|--------|
| 72.4 | 10.133.147.141 | ord38s32-in-f2.1e100.net | TLSv1.2 | 438 | Google |
| 72.4 | ord38s32-in-f2.1e100.net | 10.133.147.141 | TLSv1.2 | 1000 | Google |
| 76.2 | 10.133.147.141 | ns1.carleton.edu | DNS | 55 | other |
| 78.9 | ec2-52-17-143-157.eu-west-1.compute.amazonaws.com | 10.133.147.141 | TCP | 611 | Amazon |

Data Analysis

- Pie charts - major hosts
 - Facebook/Meta
 - Apple
 - Google/Alphabet
 - Amazon
 - Akamai
- Time series graphs



Data Analysis





Akamai

- ❑ Leading content delivery network (CDN) services provider
- ❑ Several different domains - akamaitechnologies, akamaiedge, etc.
- ❑ Connections with TikTok, Google, Microsoft

Results

Apps opening on startup

Fresh reset IOS vs Android

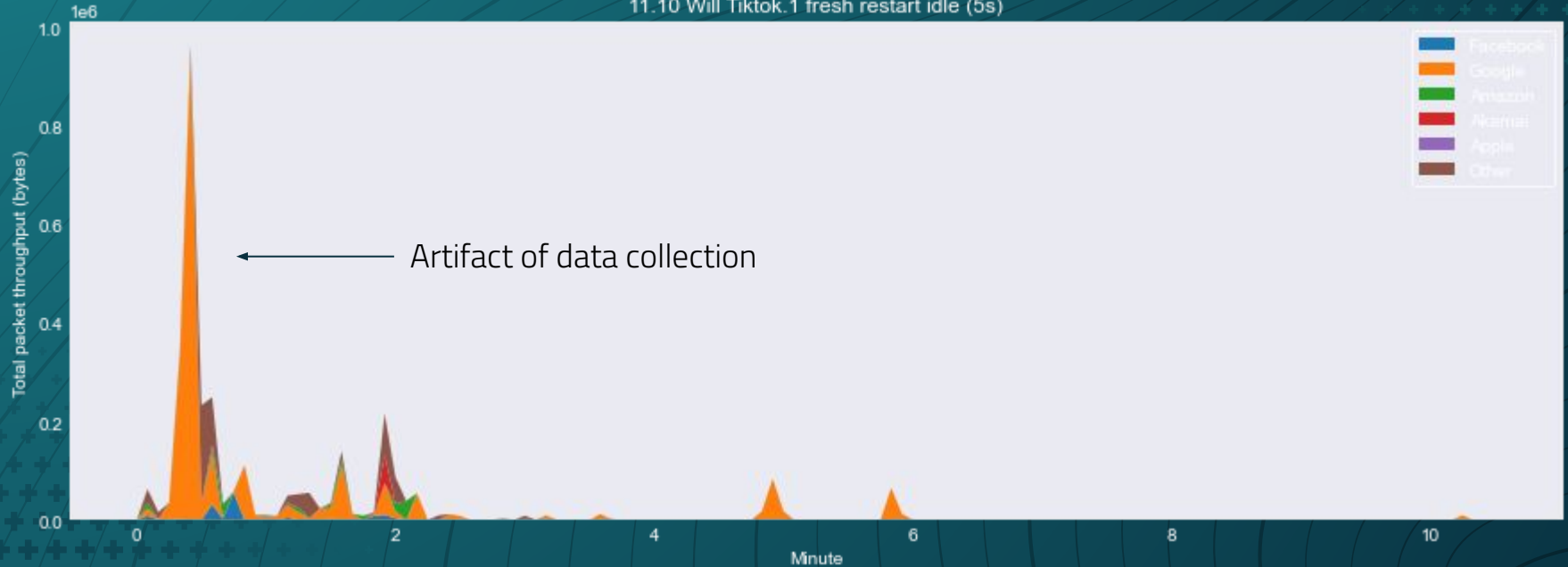


Fresh reset iOS vs Android



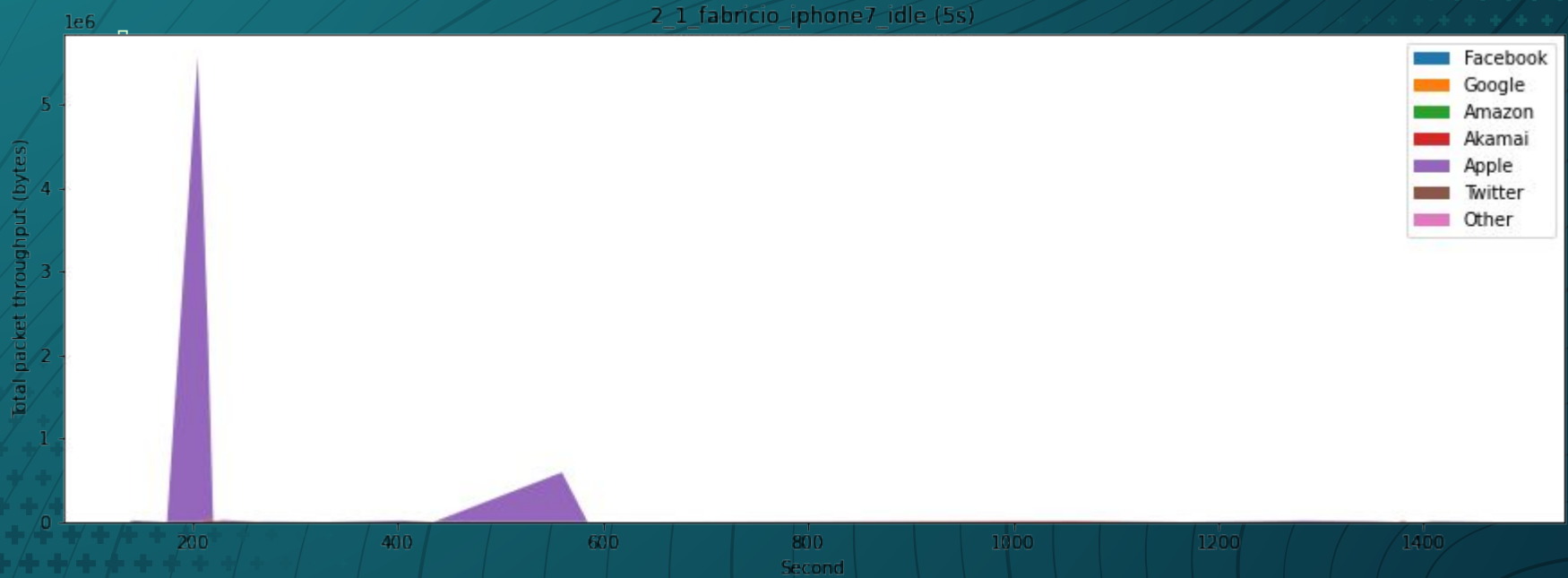


Fresh reset iOS vs Android





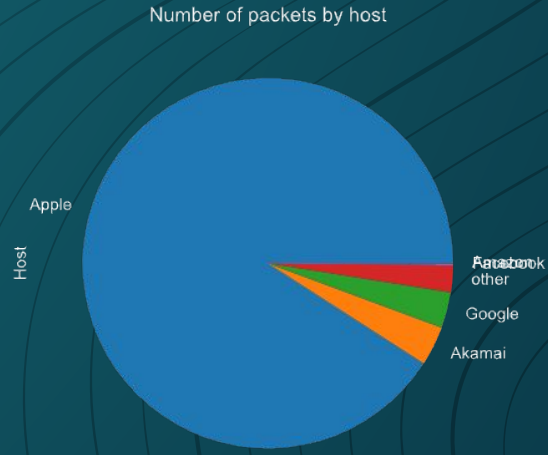
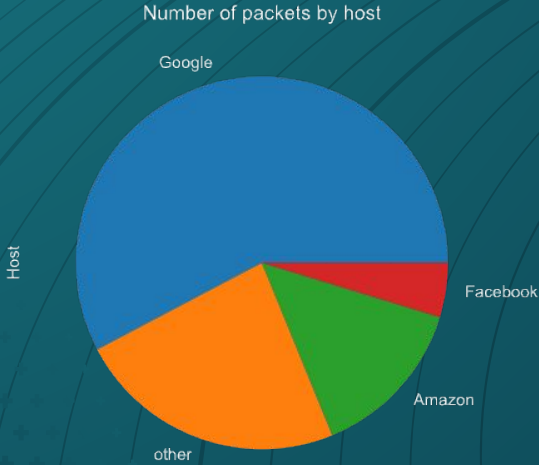
Fresh reset iOS vs Android



Fresh reset IOS vs Android



- Both have startup but mainly apple and google
- We have a clean slate to experiment

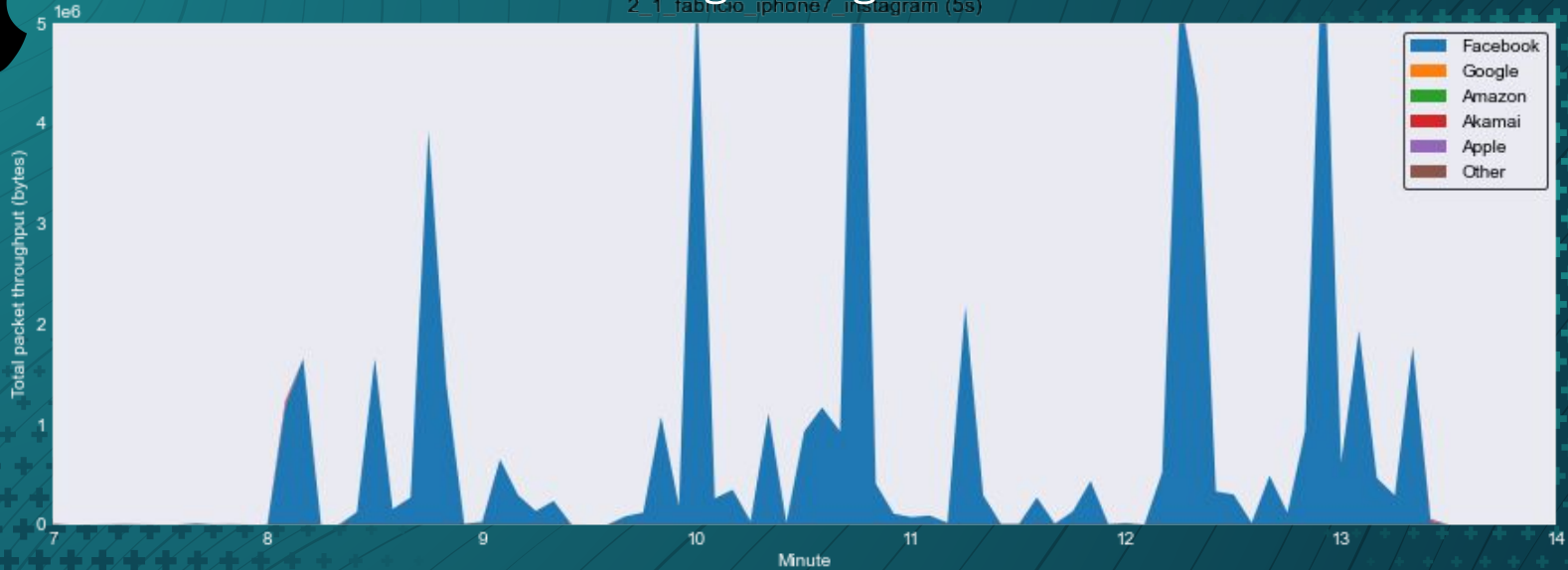


How are apps
communicating with our
phones?



Using Instagram

2_1_fabrizio_iphone7_instagram (5s)



- ❑ Packets always being sent
- ❑ irregular peak height

When Open In Background



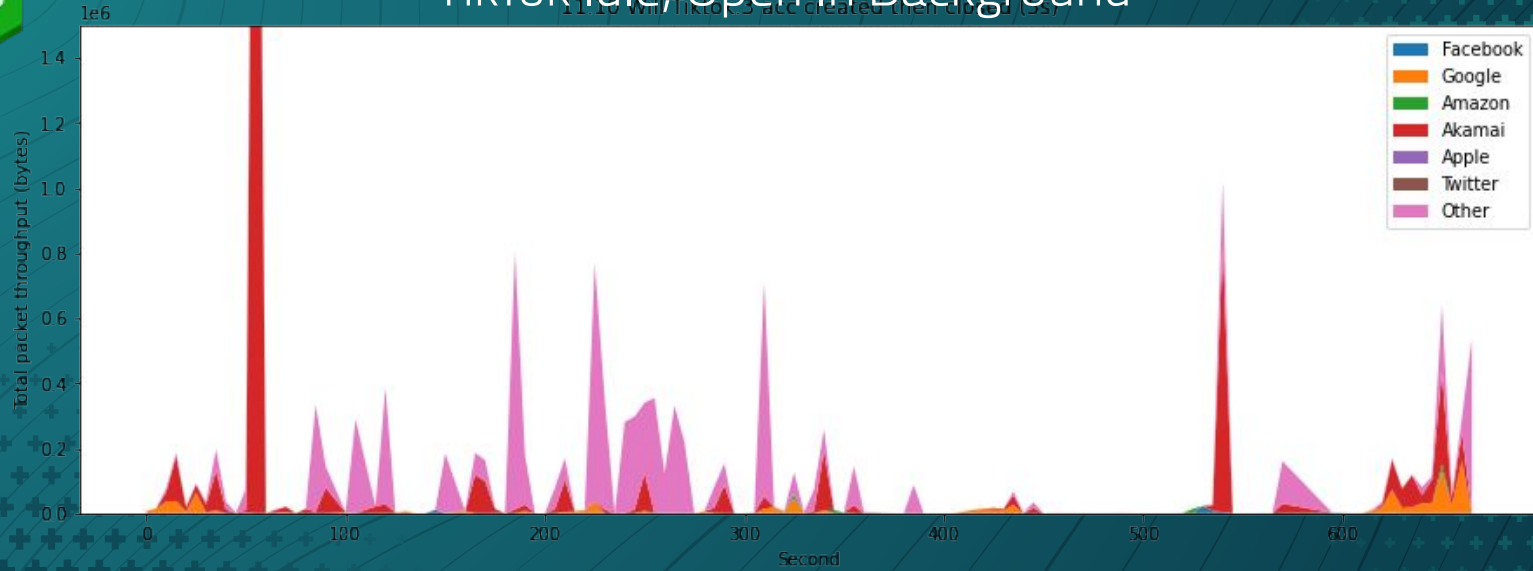
Instagram Idle, Open In Background



- ❑ Regular intervals between data sent
- ❑ Constant peak height
- ❑ Feed based app



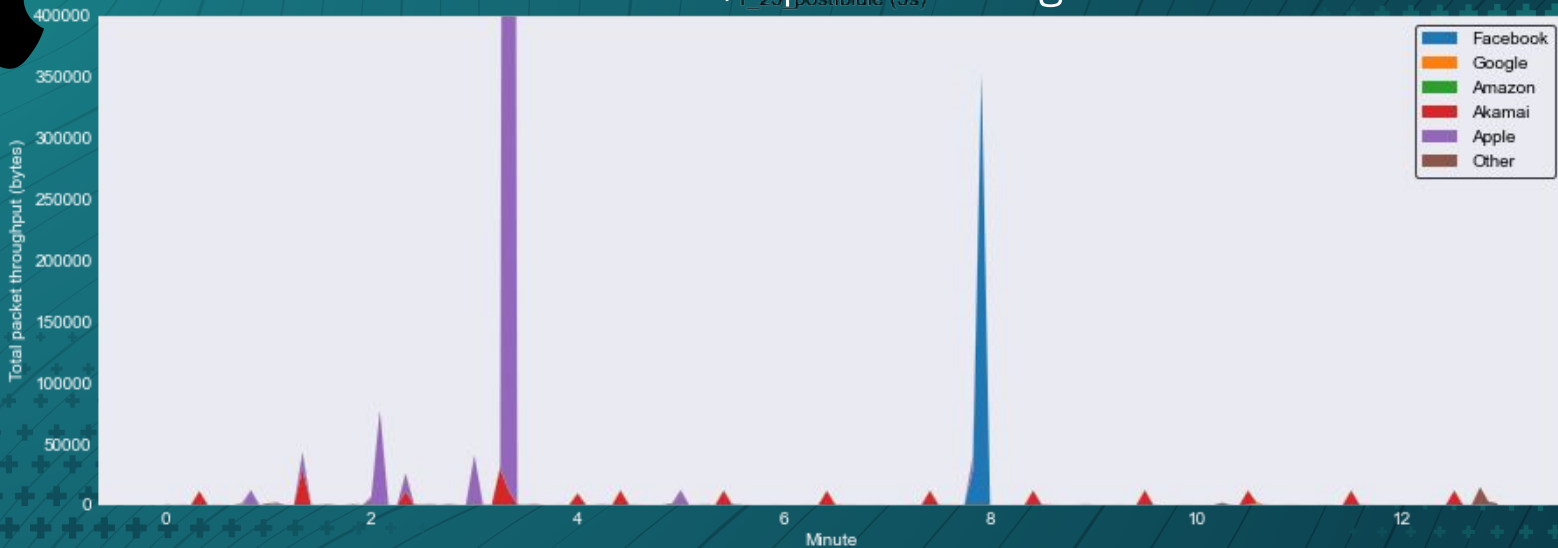
TikTok Idle, Open In Background



- ❑ Regular intervals between data sent
- ❑ Constant peak height
- ❑ Feed based apps need data
- ❑ Many differences between apps



Facebook Idle, Open In Background



- ❑ Regular intervals between data sent
- ❑ Constant peak height
- ❑ Feed based apps need data
- ❑ Many differences between apps

Akamai and TikTok Experiment Oddities

- Over 90 different akamai domains:
load-balancing?
- Much more data sent proportionally
while browsing or interacting with app

Wireshark · Endpoints · 11.10 Will Tiktok.3 acc created then closed.pcap

Ethernet · 2 IPv4 · 128 IPv6 TCP · 775 UDP · 51

| Address | Packets | Bytes |
|---|---------|--------|
| a23-48-208-10.deploy.static.akamaitechnologies.com | 36 | 12 k |
| a23-48-208-16.deploy.static.akamaitechnologies.com | 17 | 1515 |
| a23-48-208-17.deploy.static.akamaitechnologies.com | 3 | 182 |
| a23-48-208-18.deploy.static.akamaitechnologies.com | 9 | 546 |
| a23-48-208-19.deploy.static.akamaitechnologies.com | 32 | 2922 |
| a23-48-208-25.deploy.static.akamaitechnologies.com | 176 | 354 k |
| a23-48-208-26.deploy.static.akamaitechnologies.com | 223 | 77 k |
| a23-48-208-32.deploy.static.akamaitechnologies.com | 231 | 69 k |
| a23-48-208-33.deploy.static.akamaitechnologies.com | 3 | 182 |
| a23-48-208-34.deploy.static.akamaitechnologies.com | 126 | 35 k |
| a23-48-208-35.deploy.static.akamaitechnologies.com | 467 | 670 k |
| a23-48-208-40.deploy.static.akamaitechnologies.com | 3 | 182 |
| a23-48-208-41.deploy.static.akamaitechnologies.com | 9 | 546 |
| a23-48-208-42.deploy.static.akamaitechnologies.com | 3 | 182 |
| a23-48-208-43.deploy.static.akamaitechnologies.com | 97 | 19 k |
| a23-48-208-48.deploy.static.akamaitechnologies.com | 18 | 1092 |
| a23-48-208-50.deploy.static.akamaitechnologies.com | 27 | 2055 |
| a23-48-208-56.deploy.static.akamaitechnologies.com | 23 | 6578 |
| a23-48-208-57.deploy.static.akamaitechnologies.com | 50 | 10 k |
| a23-48-208-58.deploy.static.akamaitechnologies.com | 48 | 4403 |
| a23-63-73-144.deploy.static.akamaitechnologies.com | 171 | 28 k |
| a23-63-73-155.deploy.static.akamaitechnologies.com | 916 | 4557 k |
| a23-77-218-136.deploy.static.akamaitechnologies.com | 147 | 32 k |
| a23-77-218-137.deploy.static.akamaitechnologies.com | 44 | 3690 |
| a23-77-218-138.deploy.static.akamaitechnologies.com | 29 | 8733 |
| a23-77-218-139.deploy.static.akamaitechnologies.com | 106 | 32 k |
| a23-77-218-144.deploy.static.akamaitechnologies.com | 139 | 28 k |
| a23-77-218-145.deploy.static.akamaitechnologies.com | 30 | 1820 |
| a23-77-218-146.deploy.static.akamaitechnologies.com | 24 | 1456 |
| a23-77-218-147.deploy.static.akamaitechnologies.com | 15 | 910 |
| a23-77-218-152.deploy.static.akamaitechnologies.com | 586 | 148 k |
| a23-77-218-153.deploy.static.akamaitechnologies.com | 32 | 11 k |
| a23-77-218-154.deploy.static.akamaitechnologies.com | 58 | 12 k |
| a23-77-218-155.deploy.static.akamaitechnologies.com | 120 | 20 k |

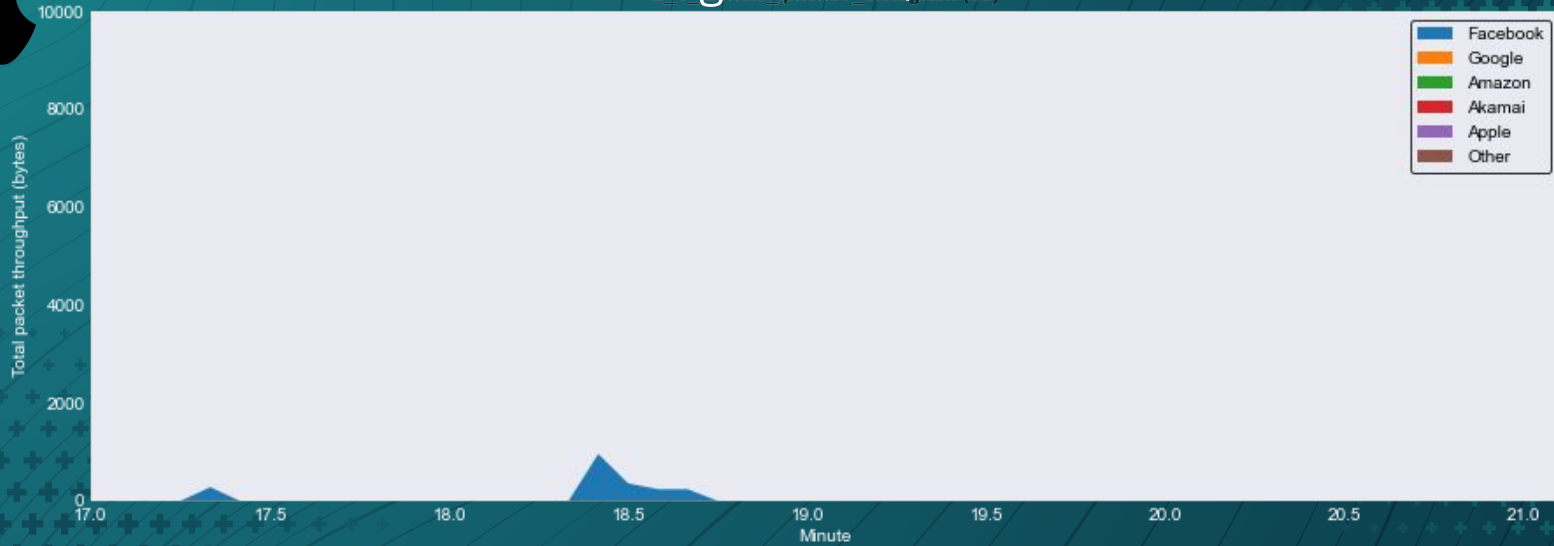
Akamai presence before installing?



When Closed



Instagram Idle, Closed



- ❑ Not as much data
- ❑ Tapers off after some time



TikTok Idle, Closed



Not as much data

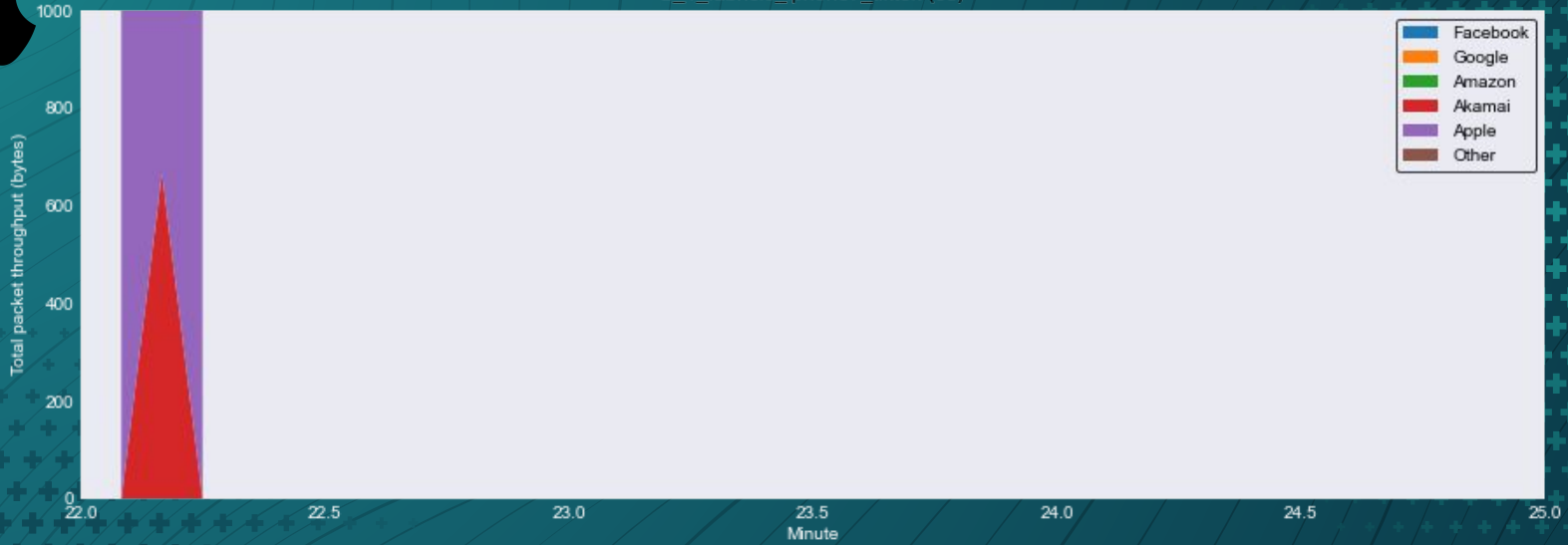


Tapers off after some time

How do we stop apps
communicating with our
phones



TikTok deleted



- ❑ Waited 3 minutes
- ❑ No data



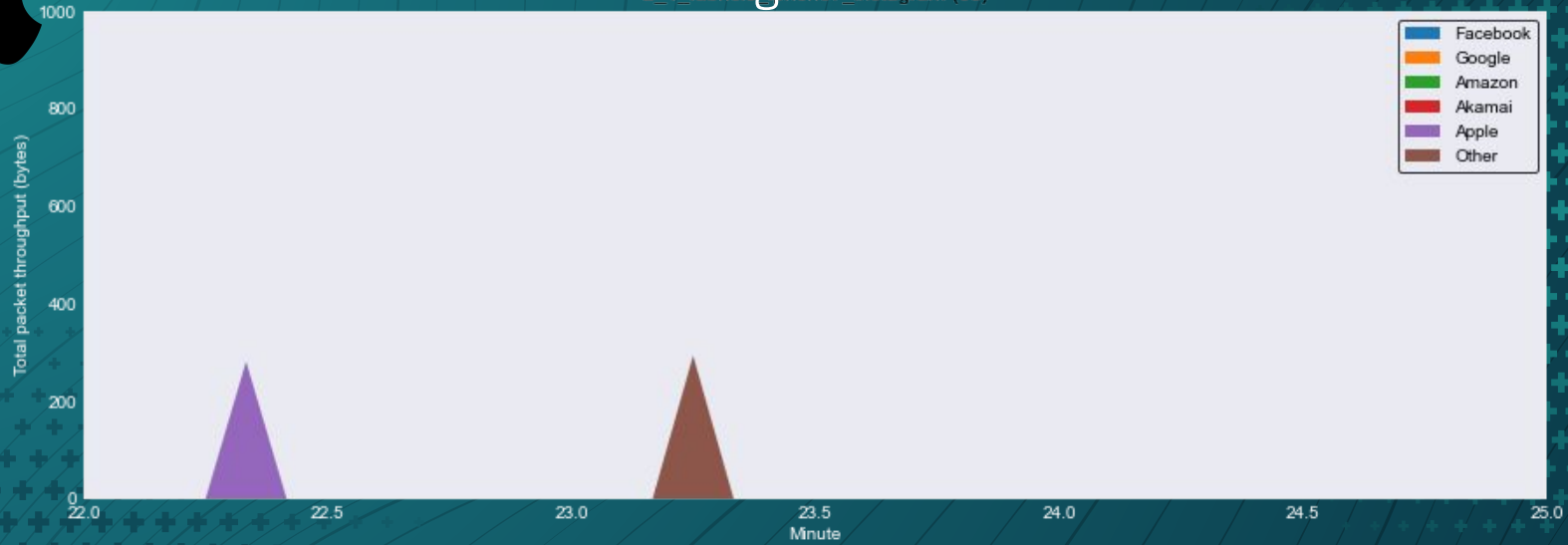
Facebook deleted



- ❑ Waited 3 minutes
- ❑ No data



Instagram deleted



- ❑ Waited 3 minutes
- ❑ No data

How do we stop apps communicating?

- Close the app
- Delete the app
- Still takes some data when closed
- Big companies own multiple applications

What's Next?

What's Next?

- Meta Pixel
- Mozilla Rally
- Future Research

What's Next?

- **Meta Pixel**

- Publicly available to **purchase** ad software
- Directs internet users to specific websites based on their Facebook/Meta data **profile***
- Allows Facebook/Meta to **profit** off of data collection and expand their network

What's Next?

- **Mozilla Rally**

- A response to Pixel by Mozilla and The Markup
- Attempts to uncover Facebook's data network to see what data and how much is **used** and **shared** and **sold***

What's Next?

- **Future Research**

- Solving the “problem” of encryption
- How can we get transparency from tech companies without endangering personal information?

What's Next?

- **Future Research**

- Consolidation of cloud providers
- Microservices/specific app traffic

Bibliography

Apple. "App Privacy Details - App Store." Apple Developer, <https://developer.apple.com/app-store/app-privacy-details/>. Accessed 17 Feb. 2022.

Das, Resul & Tuna, Gurkan. (2017). Packet tracing and analysis of network cameras with Wireshark. 1-6. 10.1109/ISDFS.2017.7916510.

Nicholson, Stacy. (2021). Data Sharing and Exposure: Findings from Descriptive and Network Analysis of Instant Games on Facebook.

Sar, Rath Kanha. "The Tracking of Users' Unintentionally Shared Information by Social Network Sites." (2014).

Williams, Laurence. "What Kind of Data Does Facebook Collect?" Boldist, Boldist, 14 May 2021, <https://boldist.co/analytics/facebook-data-collection/>.

Woollacott, Emma. "New Mozilla Project Aims to Reveal Facebook's Tracking and Data Collection Practices." Forbes, Forbes Magazine, 11 Jan. 2022, <https://www.forbes.com/sites/emmawoollacott/2022/01/10/new-mozilla-project-aims-to-reveal-facebooks-tracking-and-data-collection-practices/?ss=cybersecurity&sh=7b70394bc78a>.

Special thanks to Armira Nance and Jeff Ondich