

PRIVACY INVASION IN IOS LANGUAGE LEARNING APPLICATIONS

Using open-source tools to detect privacy breaches in language learning apps.



WHOAMI?



- Master's degree Computer Science
 - Digital Forensic Investigator
 - Linux hobbyist
 - Debian + Red Hat



What Is this presentation?

This presentation should serve as a brief explanation of how my Masters research integrated open-source tools for digital forensics and what my research found.



TABLE OF CONTENTS

01

Background

What I was trying to accomplish

02

The Apps

Qualities of the apps that I examined

03

OSS Tools

The tools that made the examination possible

04

Methodology

How I deployed the tools to do the research

05

Results

The results I achieved using the tools

06

Sources



01

BACKGROUND



Background

- I decided to conduct a security analysis of common language learning apps to analyze the differences between free and paid versions.
- After many iterations, I decided to focus on advertising systems and the user information they create and send out.

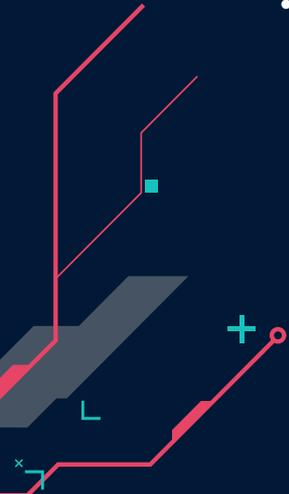


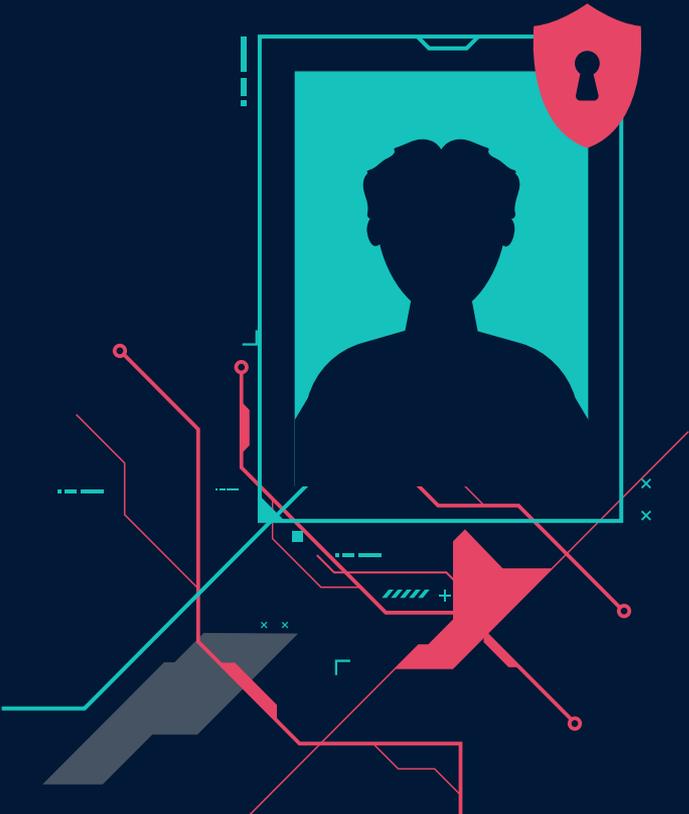
Overarching question

Is any user-identifying data packaged up and sent in a different way between the free and paid versions of common language-learning apps?

Advertising Terminology

- Demand side client: A client that is requesting the ad or being advertised to.
- Supply side client: a client that is distributing the ads (i.e. Google Ad Network)
- Real-time Bidding: The split-second process by which advertisers buy the spot that the user will see.
- Interstitial: The property of appearing in between two things.
- CDN: Content distribution network; a series of servers that allows users of a service to query for files of all types.





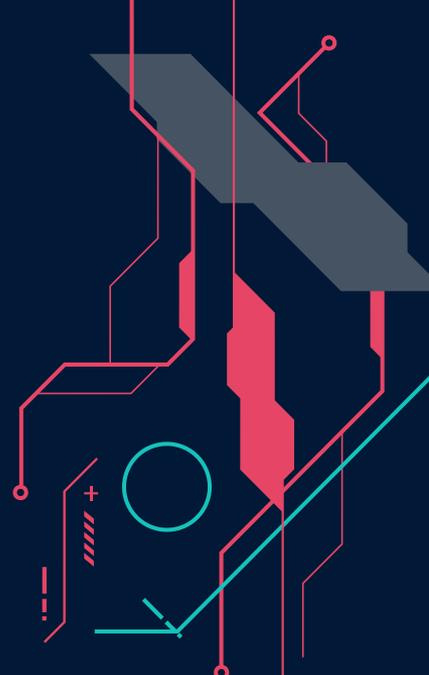
02

The Apps

Duolingo, Busuu, and Memrise

Duolingo Information

- Most well-known language learning app.
- Free and paid tier.
- Diverse set of features with many languages.
- Has AI voices that aid with pronunciation of languages.
- Has special exercises for learning foreign character sets (i.e. Korean, Greek, Cyrillic, etc)



Duolingo Information



Figure 1a: Duolingo normal exercises.



Figure 1b: Duolingo stories.

Duolingo Information



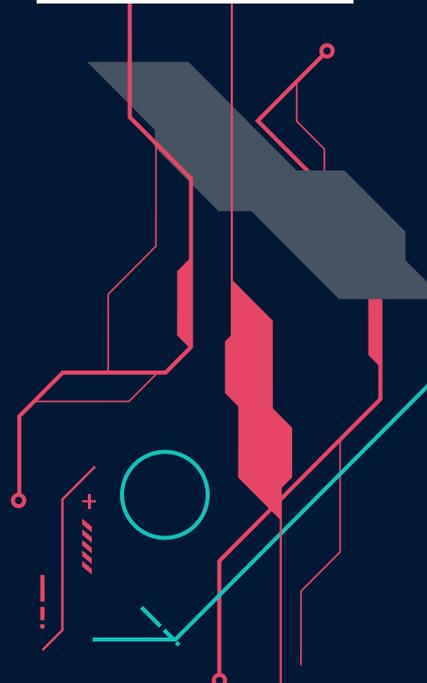
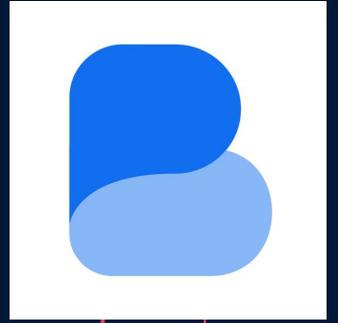
Figure 1c: Duolingo Podcast.



Figure 1d: Duolingo Streak and subscription.

Busuu Information

- Another well-known language-learning app.
- Free and paid tier, part of Chegg.
- Grammar, vocab and history lessons.
- Ads come before or after the lesson.
- Features flashcard sections of lessons like Duolingo.



Busuu Information

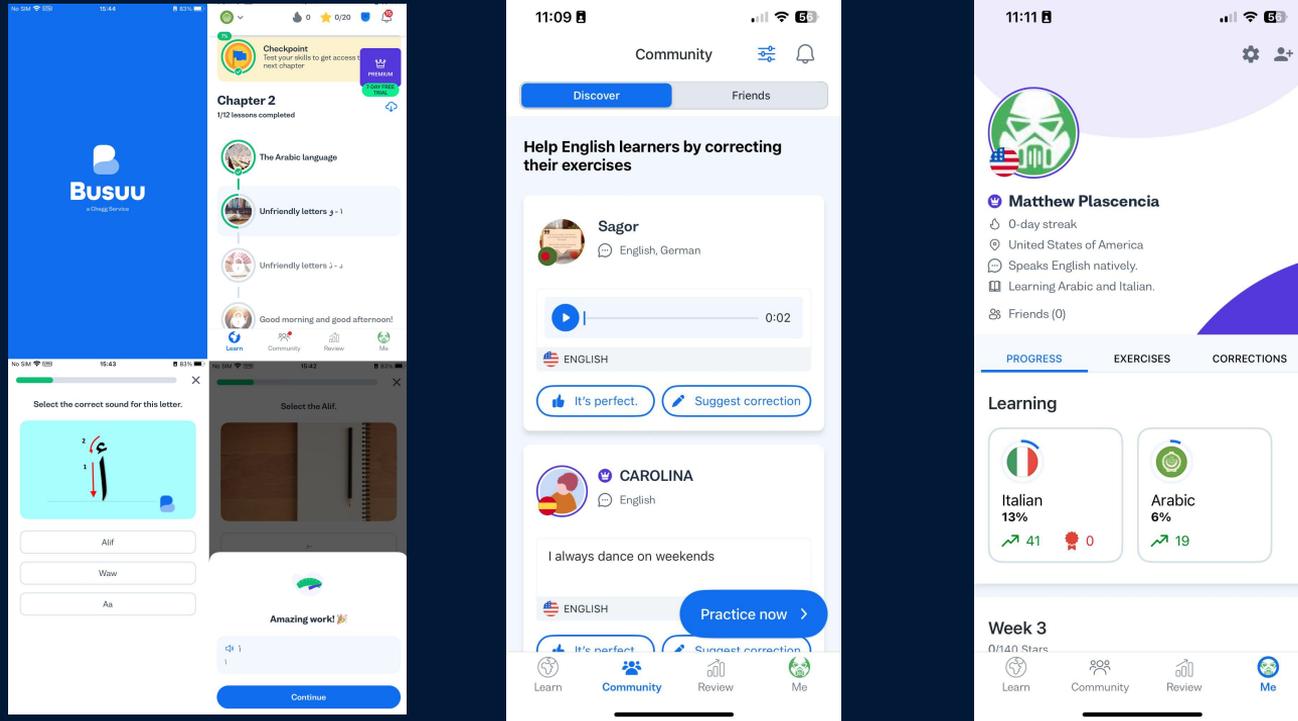
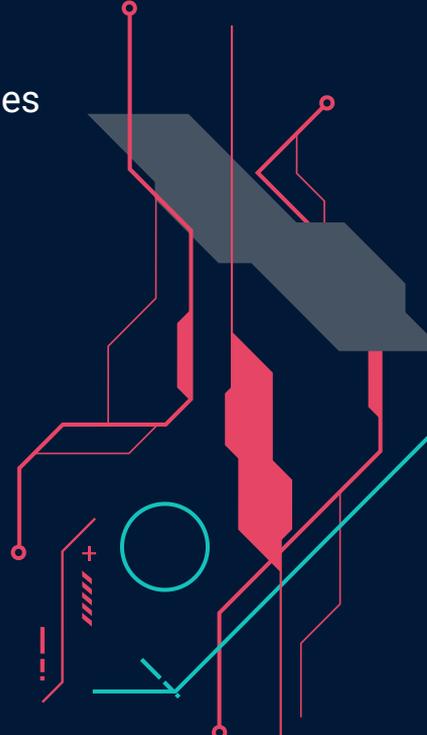


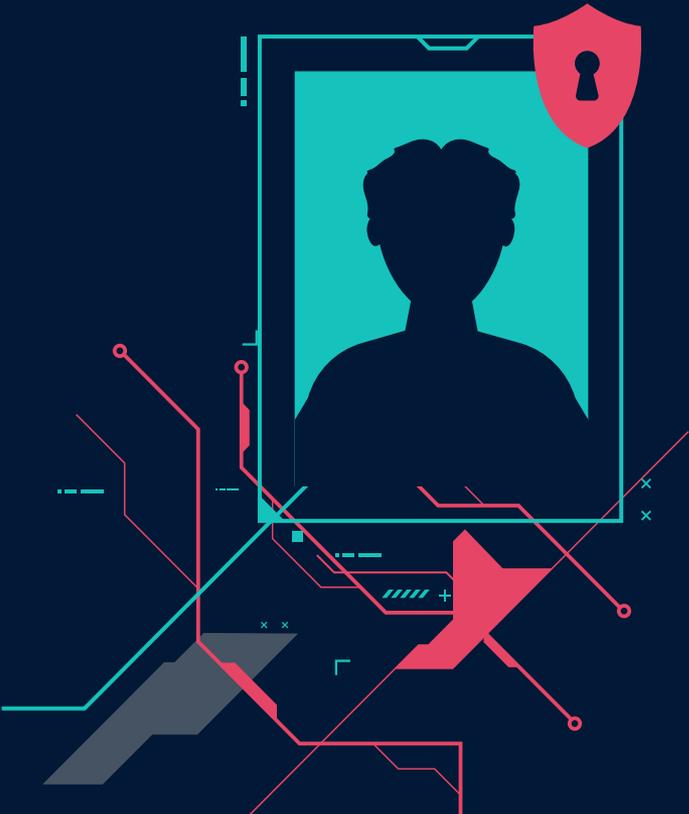
Figure 2: Busuu images.

Memrise Information

- A unique app. Spaced repetition is a noticeable part.
- Free and paid tier.
- Ads come before or after the lesson.
- Features a flexible platform, including all normal things like the vocab exercises and the grammar ones alongside things like videos and listening exercises.

MEM
RISE





03

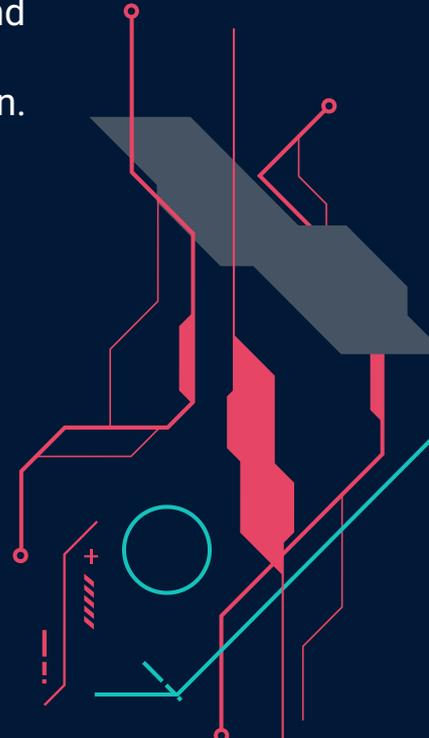
The OSS Tools

All of the OSS Tools Uses Throughout the Research.

UFADE (Christian Peter)



- A tool used to pull information from iPhones.
- Supports full file backup (with jailbreak enabled), regular iTunes backup, and logical+ backups.
 - Logical+ backups include iTunes backup and other media information.
- Can also acquire logs of all sorts.
- <https://github.com/prosch88/UFADE>
- Part of early research in finding what data was on phone.



UFADE (Christian Peter)

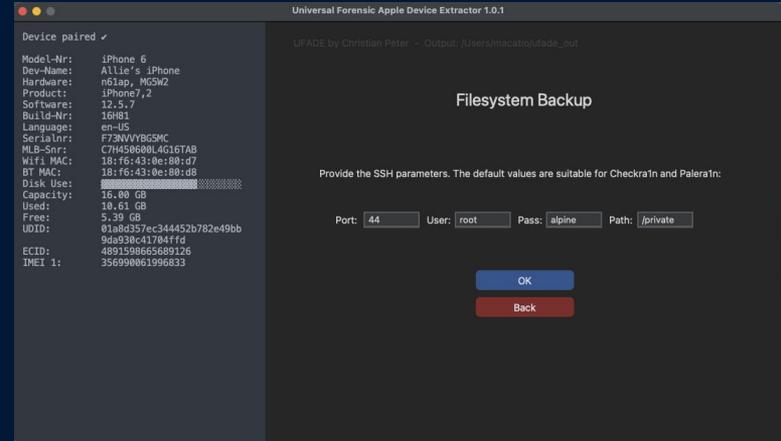
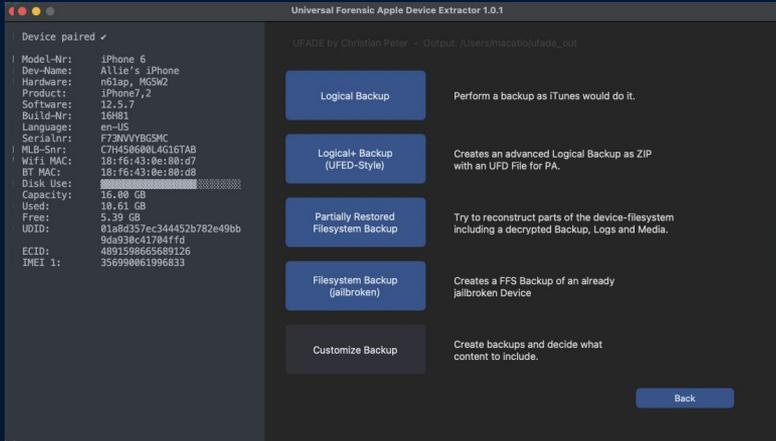


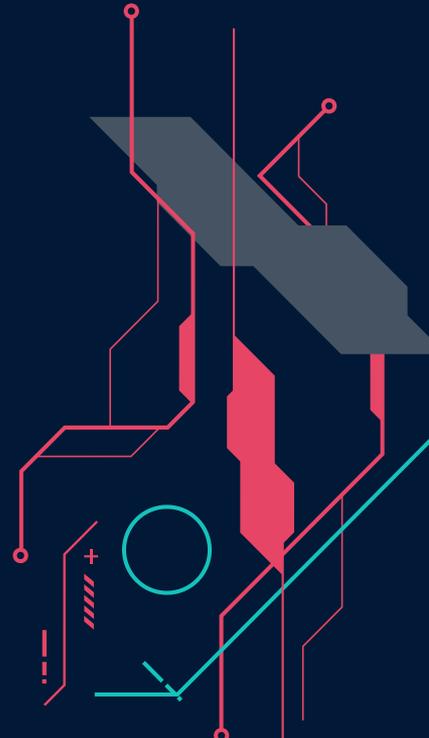
Figure 3b: UFADE Extractor selection of Jailbreak acquisition and selection of port options.



Wireshark



- A very common network analysis tool.
- Gives insights into what's going through a network at any given time.
- <https://wireshark.org>



Wireshark

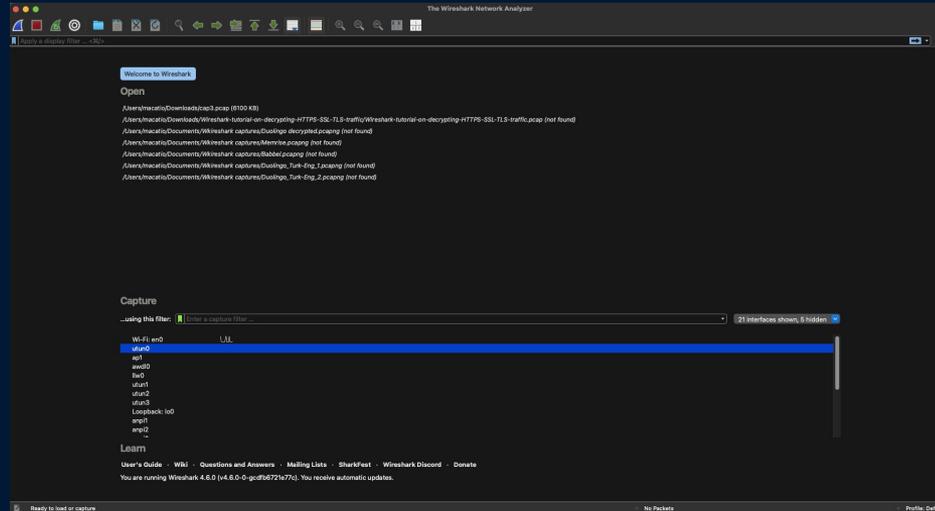


Figure 4a: Wireshark start screen.



Wireshark



No.	Time	Source	Destination	Protocol	Length	Info
1858	16.791424	2087:f908:4801:151::...	2087:f908:4801:151::...	UDP	228	443 -> 62774 Len=232
1851	16.791427	2087:f908:4801:151::...	2087:f908:4801:151::...	UDP	1294	443 -> 62774 Len=1232
1852	16.791429	2087:f908:4801:151::...	2087:f908:4801:151::...	UDP	854	443 -> 62774 Len=792
1853	16.792372	2087:f908:4801:151::...	2087:f908:4801:151::...	UDP	97	62774 -> 443 Len=95
1854	17.852326	2087:f908:4801:151::...	2084:6808:4807:81f::...	UDP	91	62676 -> 443 Len=29
1855	17.848086	192.168.12.161	192.168.12.161	HTTP	184	Standard query RRDNS PTR 1b_dns-id_www.local, "QM" question OPT
1856	17.319685	2084:6808:4807:81f::...	2087:f908:4801:151::...	UDP	91	443 -> 62676 Len=29
1857	18.822753	192.168.12.228	192.168.12.228	TLSv1.2	119	Application Data
1858	18.823892	192.168.12.228	162.159.138.234	TCP	66	58188 -> 443 [ACK] Seq=1 Acks=3357 Win=8926 Len=0 TSval=1291842996 TSecr=1222986165
1859	18.846662	Arccsys,161761616	66.848.162.1.1	HTTP	42	162.168.12.1.1 GET /acdiff/9/18/fd/1c
1860	19.968235	162.159.138.234	192.168.12.228	TLSv1.2	322	Application Data
1861	19.968718	192.168.12.228	162.159.138.234	TCP	66	58188 -> 443 [ACK] Seq=1 Acks=3611 Win=8926 Len=0 TSval=1291844941 TSecr=1222986128
1862	20.171368	Arccsys,161761616	66.848.162.1.1	HTTP	42	Who has 192.168.12.161? Tell 192.168.12.1
1863	20.539724	2087:f908:4801:151::...	2084:6808:4807:81f::...	TLSv1.2	125	Application Data
1864	20.788875	2087:f908:4801:151::...	2087:f908:4801:151::...	UDP	1294	62774 -> 443 Len=1232
1865	20.788328	2087:f908:4801:151::...	2087:f908:4801:151::...	UDP	1294	62774 -> 443 Len=1232
1866	20.788545	2087:f908:4801:151::...	2087:f908:4801:151::...	UDP	1294	62774 -> 443 Len=1232
1867	20.782929	2084:6808:4807:81f::...	2087:f908:4801:151::...	TCP	66	443 -> 58032 [ACK] Seq=1 Acks=1849 Len=0 TSval=173988479 TSecr=396426258
1868	20.783557	2087:f908:4801:151::...	2087:f908:4801:151::...	UDP	1294	62774 -> 443 Len=1232
1869	20.784489	2084:6808:4807:81f::...	2087:f908:4801:151::...	TLSv1.2	125	Application Data
1870	20.783652	2087:f908:4801:151::...	2084:6808:4807:81f::...	TCP	66	58032 -> 443 [ACK] Seq=0 Acks=0 Win=2848 Len=0 TSval=3964262765 TSecr=173988479
1871	20.787361	2087:f908:4801:151::...	2087:f908:4801:151::...	UDP	1294	62774 -> 443 Len=1232
1872	20.798181	2087:f908:4801:151::...	2087:f908:4801:151::...	UDP	772	82774 -> 443 Len=710

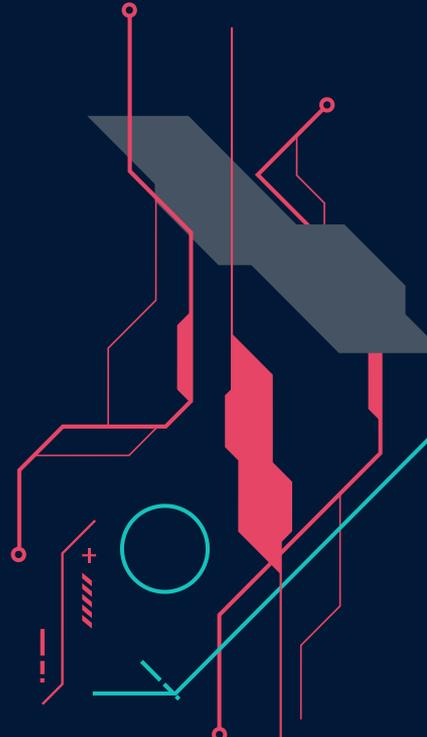
```
> Frame 1: Packet, 181 bytes on wire (808 bits), 181 bytes captured (808 bits) on interface eth0, id 0
  Ethernet II, Src: Arccsys_161761616, (ac:0f:9f:16:fa:1c), Dst: 66:84:8f:16:1c:00, (66:84:8f:16:1c:00)
  Internet Protocol Version 4, Src: 2084:6808:4807:81f::204, Dst: 2087:f908:4801:151::c204
  User Datagram Protocol, Src Port: 443, Dst Port: 62676
  Data (129 bytes)
```

Figure 4b: Wireshark user interface.



WiresharkHelper

- App for MacOS/iOS.
- Helps to bridge the gap between Wireshark and iOS.
- Allows Man in the Middle Proxy so that the Mac can capture the iOS traffic.
- Uses the Remote interface (rvi[x]) to capture the iOS traffic.
- WiresharkHelper is free on iOS and was free on GitHub when I did the research. It is no longer available on GitHub; \$10 on Mac App Store.



WiresharkHelper

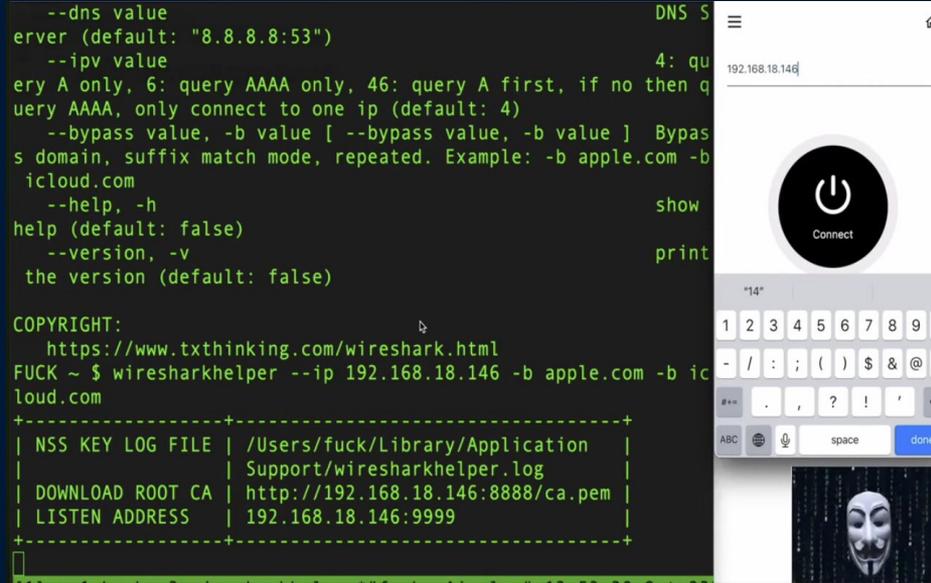


Figure 5a: WiresharkHelper iOS + MacOS



WiresharkHelper

No.	Time	Source	Destination	Protocol	Length	Info
1454	43.368925	192.168.18.241	192.168.18.146	TCP	666	53656 → 9999 [PSH, ACK] Seq=2061 Ack=2505 Win=131072 Len=600 TSval=222803
1455	43.368925	192.168.18.241	192.168.18.146	TCP	1514	53656 → 9999 [ACK] Seq=2661 Ack=2505 Win=131072 Len=1448 TSval=2228037870
1456	43.369003	192.168.18.146	192.168.18.241	TCP	66	9999 → 53656 [ACK] Seq=2505 Ack=4109 Win=127616 Len=0 TSval=3111490263 TS
1457	43.369097	192.168.18.146	192.168.18.241	TCP	66	[TCP Window Update] 9999 → 53656 [ACK] Seq=2505 Ack=4109 Win=131072 Len=0
1458	43.369155	192.168.18.241	192.168.18.146	HTTP	291	GET /2017-06-30/config?bundle_id=com.duolingo.DuolingoMobile&country_code
1459	43.369198	192.168.18.146	192.168.18.241	TCP	66	9999 → 53656 [ACK] Seq=2505 Ack=4334 Win=130816 Len=0 TSval=3111490263 TS
1495	44.184989	192.168.18.146	192.168.18.241	TLSv1.3	1274	[TLS segment of a reassembled PDU]
1496	44.185267	192.168.18.146	192.168.18.241	HTTP/JSON	761	HTTP/1.1 200 OK, JavaScript Object Notation (application/json)
1499	44.200419	192.168.18.146	192.168.18.241	TCP	1514	[TCP Retransmission] 9999 → 53656 [PSH, ACK] Seq=2960 Ack=4334 Win=131072
1501	44.293555	192.168.18.241	192.168.18.146	TCP	66	53656 → 9999 [ACK] Seq=4334 Ack=4408 Win=129152 Len=0 TSval=2228038793 TS
1502	44.293556	192.168.18.241	192.168.18.146	TCP	78	[TCP Dup ACK 1501#1] 53656 → 9999 [ACK] Seq=4334 Ack=4408 Win=129152 Len=
1635	50.072617	192.168.18.241	192.168.18.146	HTTP	405	GET /2017-06-30/attribution/survey/custom?uiLanguage=en HTTP/1.1
1636	50.072758	192.168.18.146	192.168.18.241	TCP	66	9999 → 53656 [ACK] Seq=4408 Ack=4673 Win=130688 Len=0 TSval=3111496966 TS
1670	50.480159	192.168.18.146	192.168.18.241	HTTP/JSON	1180	HTTP/1.1 200 OK, JavaScript Object Notation (application/json)
1672	50.543431	192.168.18.241	192.168.18.146	TCP	66	53656 → 9999 [ACK] Seq=4673 Ack=5522 Win=129952 Len=0 TSval=2228045044 TS
2003	60.019058	192.168.18.146	192.168.18.146	TLSv1.3	698	[TLS segment of a reassembled PDU]
2004	60.019058	192.168.18.241	192.168.18.146	HTTP/JSON	118	PATCH /2017-06-30/users/1028072710/experiments/poseidon_ios_live_ops_rout
2005	60.019181	192.168.18.146	192.168.18.241	TCP	66	9999 → 53656 [ACK] Seq=5522 Ack=5357 Win=130368 Len=0 TSval=3111506913 TS
2297	60.361550	192.168.18.146	192.168.18.241	HTTP/JSON	709	HTTP/1.1 200 OK, JavaScript Object Notation (application/json)
2310	60.399252	192.168.18.241	192.168.18.146	TCP	66	53656 → 9999 [ACK] Seq=5357 Ack=6165 Win=130400 Len=0 TSval=2228054870 TS
2311	60.399809	192.168.18.241	192.168.18.146	HTTP	670	GET /2017-06-30/users/1028072710/xp_summaries?endDate=2022-10-20&startDate
2318	60.399899	192.168.18.146	192.168.18.241	TCP	66	9999 → 53656 [ACK] Seq=6165 Ack=5961 Win=130432 Len=0 TSval=3111507293 TS

Frame 2318: 66 bytes on wire (528 bits) ... 0000 f2 11 93 9b af 73 80 65 7c d7 6f 3b 08 00 45 00 ... :s:e :Lp::F:

Figure 5b: Wireshark Helper in action: Duolingo packets decrypted.

StormSniffer



- iOS app, (not really open-source).
- All-in-one packet sniffer + HTTPS decryptor.
- Also not fully free: Packet decryptor not completely free.
- User-friendly interface.





StormSniffer

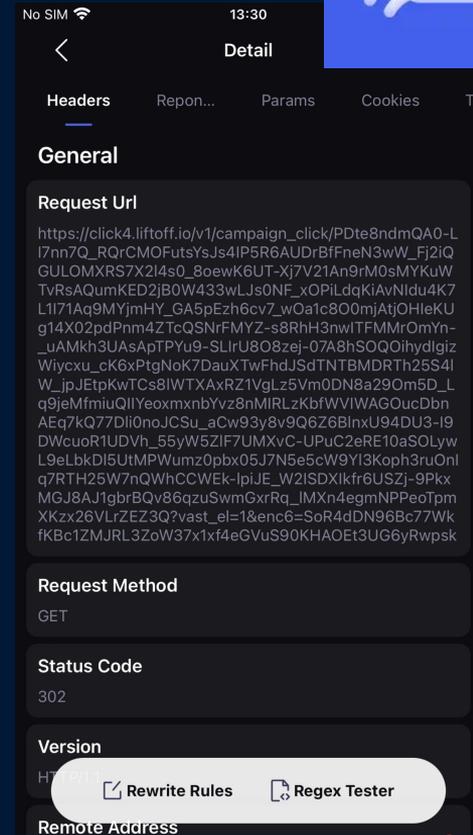
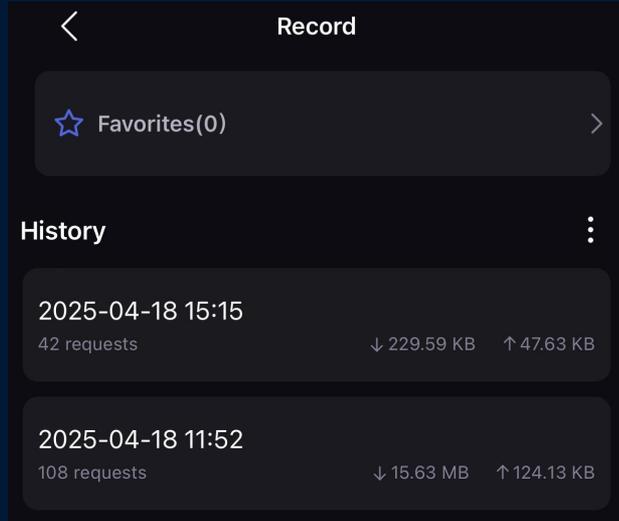
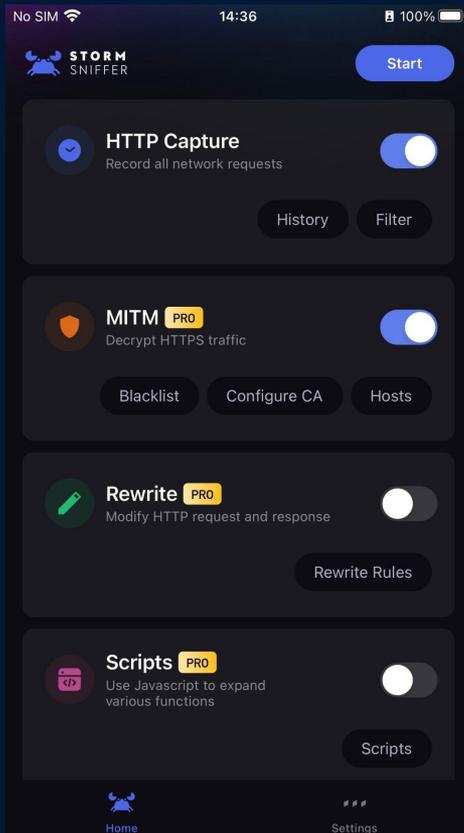
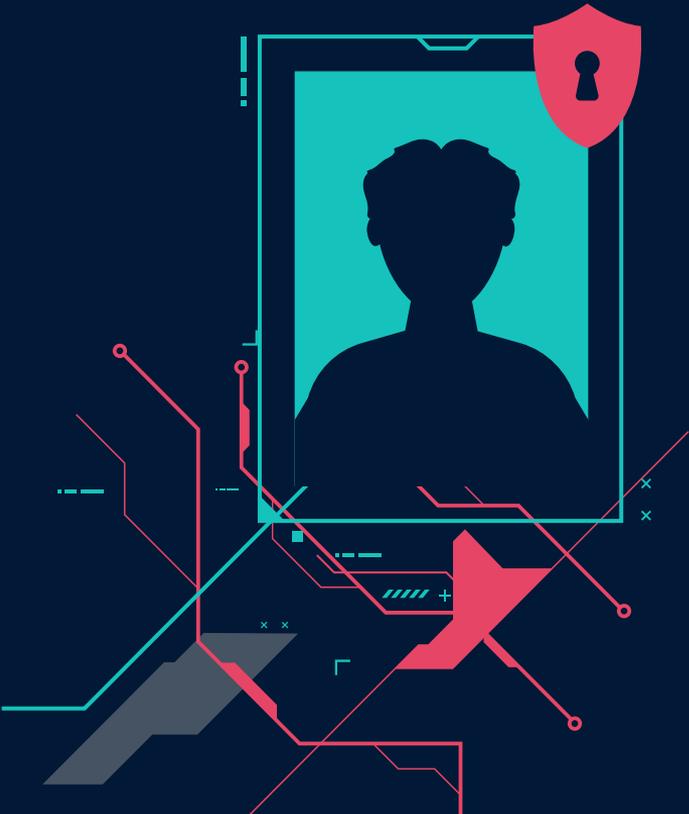


Figure 5: StormSniffer UI



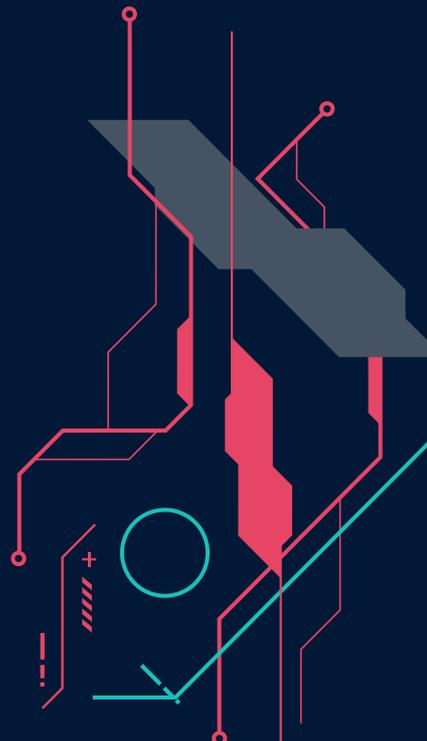
04

Experimentation

Methodologies and Trials + Tribulation

UFIDE Usage

- Very beginning phase.
- Extracted full file system after jailbreaking iPhone 8 Plus.
- I wanted to look at what the apps looked like on their file structure levels.
- Found nothing relevant.



Network Sniffing Prep

- Installed CA certs for each.
 - Settings -> Device Management -> Install MDM/VPN Profile

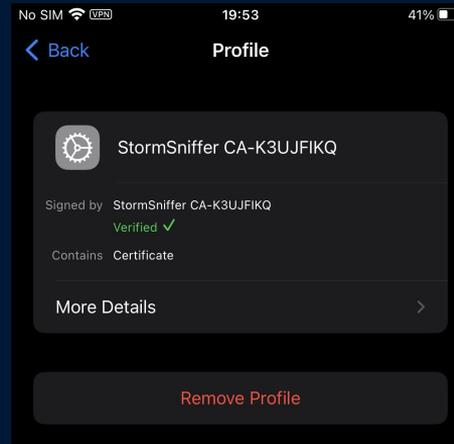
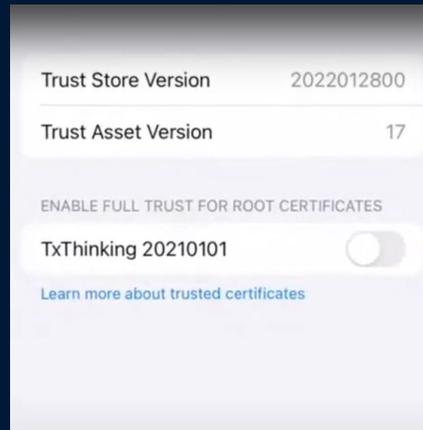


Figure 6: CA Certificate profiles



Sniffing: Successes and Failures

- Both solutions captured web traffic + ads well.
- Both caught everything from normal Duolingo/Busuu/Memrise lessons.
- Storm Sniffer didn't interfere with mic usage; WSH did.

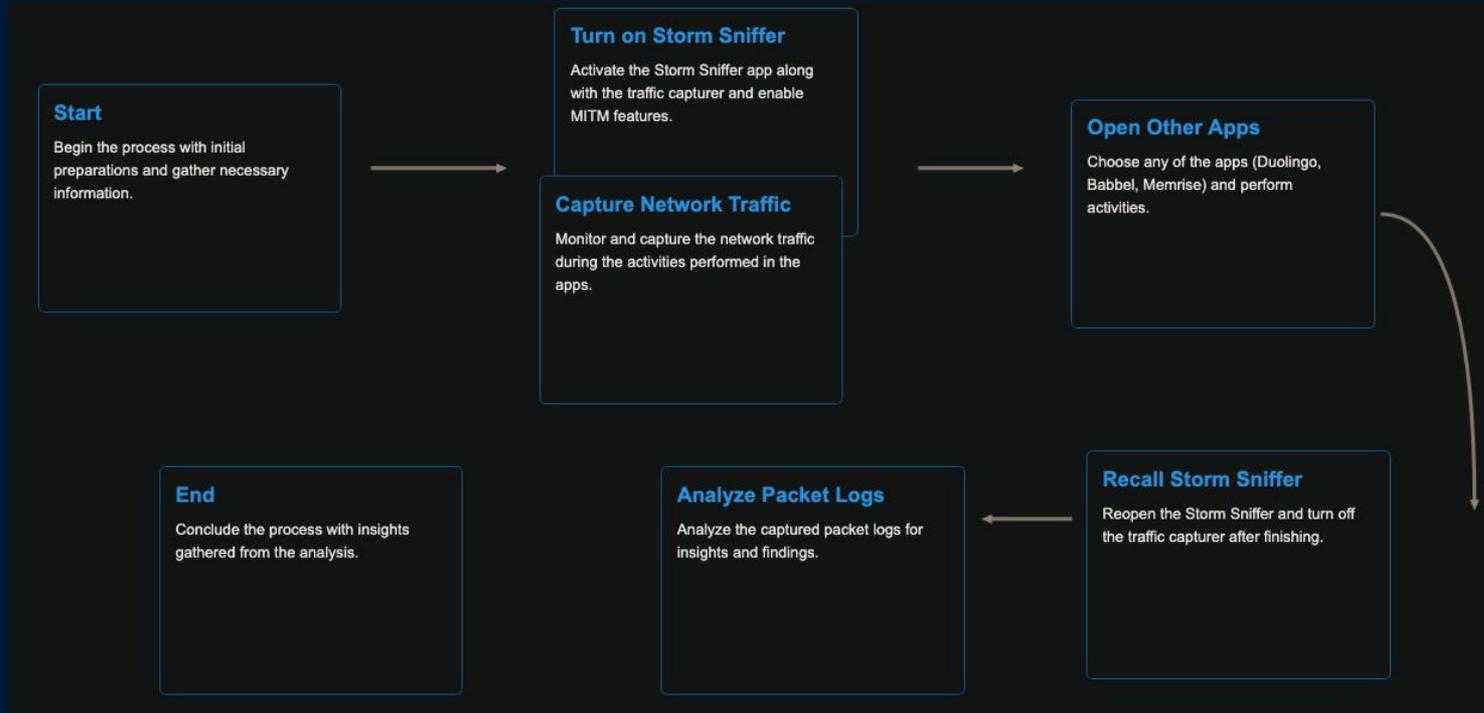


Modifications to Sniffing Process

- When adapted to using tools, modifications were made
 - WSH dropped; Storm Sniffer preferred.
 - Process refined to preferring using the software at the end of lessons.
 - Added in analyzing ad-free traffic after thoroughly analyzing ad traffic.
- Analyzed some traffic files in Wireshark by converting files from HAR2PCAP

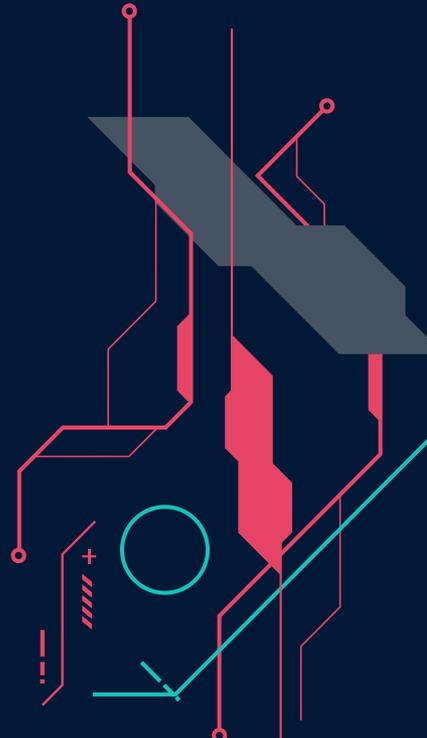


Process Flowchart



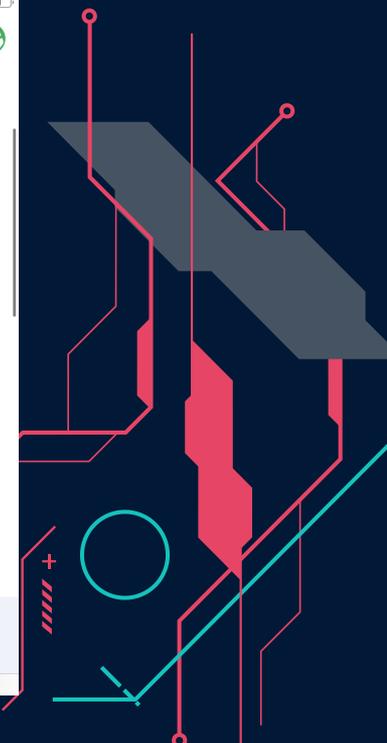
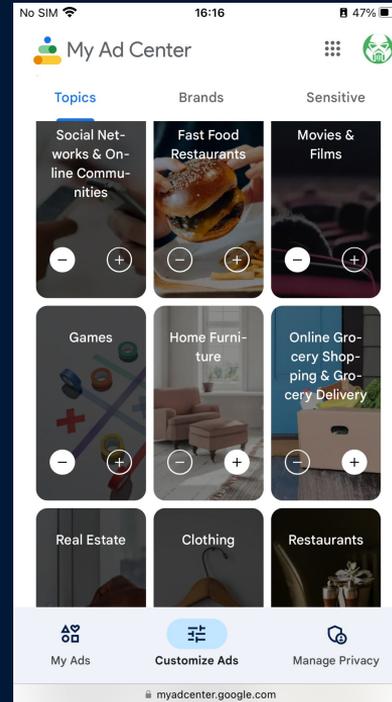
Where does data go on ads?

- [*.unityads.unity3d.com](https://unityads.unity3d.com)
- o-sdk.mediation.unity3d.com
- consent-adjust.com
- *.applovin.com
- pubads.g.doubleclick.net



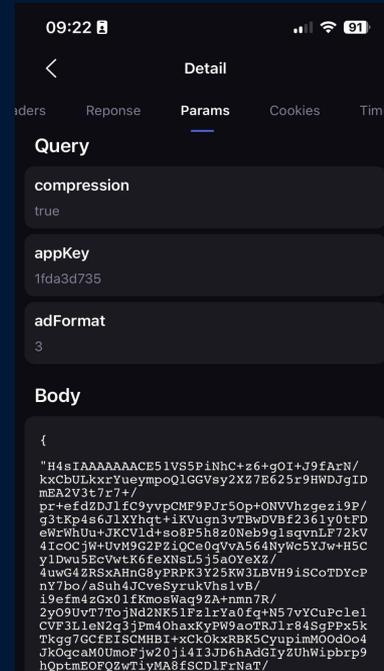
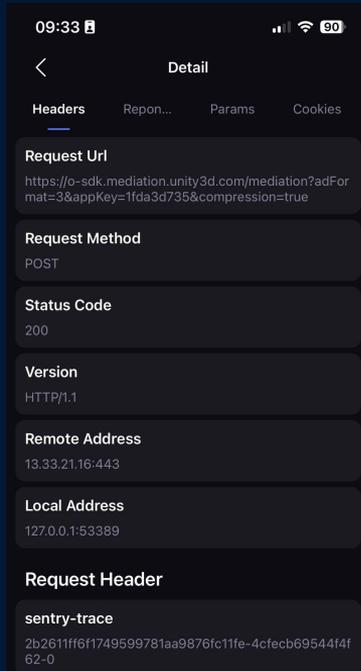
Where are ads from?

- Unity3d ads
- Google ads net
- Google Ad Center controls what ads you see!



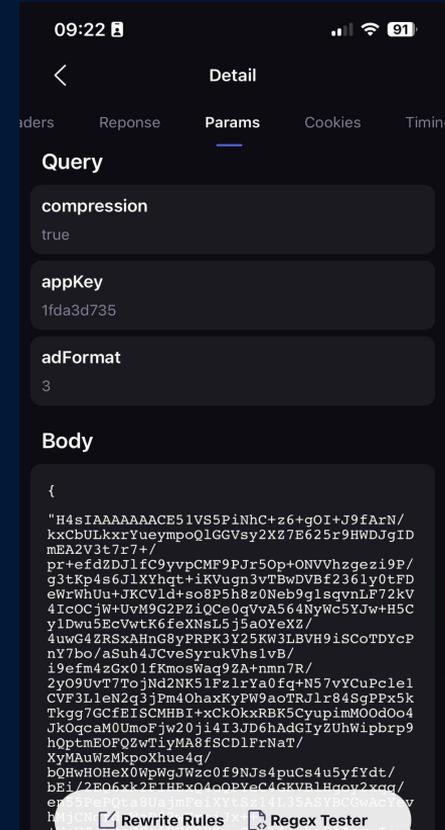
What data goes to ad networks?

- Data about the device in question is sent towards the ad service and an ad appropriate for that device is returned.



What data goes to ad networks?

- Packet contains Base64 encoded JSON information.
- *nix systems have the base64 command to decode this
- `base64 -Di inputfile | zcat` to unroll it.



What does this data look like?

```
{
  "xCodeVersion": "1680",
  "osVersion": "16.7.10",
  "connectionType": "wifi",
  "jb": "false",
  "bundleId": "com.duolingo.DuolingoMobile",
  "events": [
    {
      "eventSessionId": "9E60256B-C2FD-410A-9E5F-A7FF85533F7E",
      "firstSessionTimestamp": 1738015217402,
      "timestamp": 1743644258886,
      "eventId": 44,
      "rawConnectionType": "wifi",
      "duration": 46223
    }
  ],
  "mobileCarrier": "—",
  "groupNameBN": "All Countries",
  "abGroup": "NONE",
  "mt": "AdMob87000SDK1200iAds510",
  "groupIdRV": "5814759",
  "abInternal": "lpmm_abc_0331_disable",
  "tz": "America/Los_Angeles",
  "xCodeBuildVersion": "16A242d",
  "mcc": 65535,
  "advertisingIdType": "IDFA",
  "abHashValue": "0",
  "internalFreeMemory": 29950,
  "att": 3,
  "idfv": "F010F50F-0AC9-48DC-9BE9-21B35021EE78",
  "controllerABValue": "4",
  "deviceOEM": "Apple",
  "sdkVersion": "8.7.0",
  "advertisingId": "D991D864-A78D-4600-B8E0-1B2D45D43BB5",
  "xCodeSdkBuild": "22A3362",
  "internalTestId": {
    "99": "129"
  }
}
```

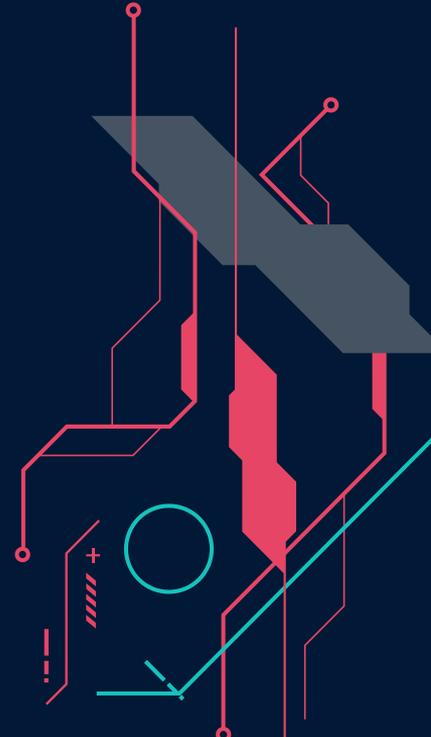
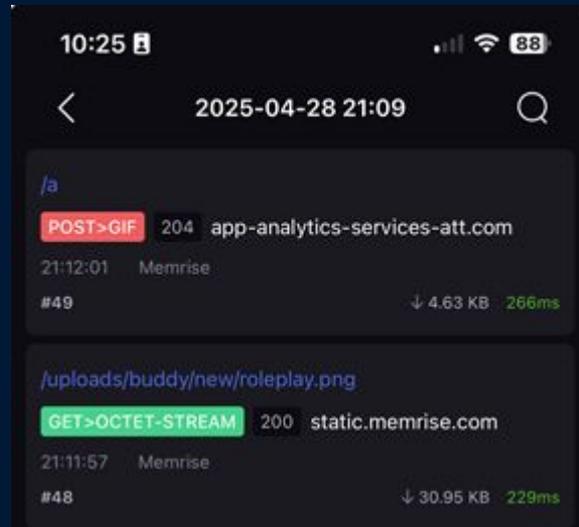
```
},
  "mobileCarrier": "—",
  "groupNameBN": "All Countries",
  "abGroup": "NONE",
  "mt": "AdMob87000SDK1200iAds510",
  "groupIdRV": "5814759",
  "abInternal": "lpmm_abc_0331_disable",
  "tz": "America/Los_Angeles",
  "xCodeBuildVersion": "16A242d",
  "mcc": 65535,
  "advertisingIdType": "IDFA",
  "abHashValue": "0",
  "internalFreeMemory": 29950,
  "att": 3,
  "idfv": "F010F50F-0AC9-48DC-9BE9-21B35021EE78",
  "controllerABValue": "4",
  "deviceOEM": "Apple",
  "sdkVersion": "8.7.0",
  "advertisingId": "D991D864-A78D-4600-B8E0-1B2D45D43BB5",
  "xCodeSdkBuild": "22A3362",
  "internalTestId": {
    "99": "129"
  }
},
  "groupIdNT": "5814765",
  "groupNameIS": "All Countries",
  "groupNameRV": "All Countries",
  "battery": 12,
  "serverInitTimestamp": "1743621446061",
  "gmtMinutesOffset": -420,
  "mnc": 65535,
  "isLimitAdTrackingEnabled": "false",
  "abt": "A",
  "sessionId": "9E60256B-C2FD-410A-9E5F-A7FF85533F7E",
  "appKey": "1fda3d735",
  "deviceOS": "ios",
  "appVersion": "7.66.0",
  "bannerSamplingMultiplier": "10",
  "groupNameNT": "All Countries",
  "icc": "—",
  "idfi": "a869f4dc-be3a-425d-8833-567806ac6d9d",
  "bannerSampling": "false",
  "timestamp": 1743644258954,
  "deviceModel": "iPhone10,2",
  "aid": "FC84A751-39C2-4BFB-B4B0-3E8582B17142",
  "xCodeSdkName": "iphonios18.0",
  "firstSession": "false",
  "language": "EN-US",
  "groupIdBN": "5814763",
  "is_coppa": "false",
  "deviceOS": "ios",
  "appVersion": "7.66.0",
  "bannerSamplingMultiplier": "10",
```

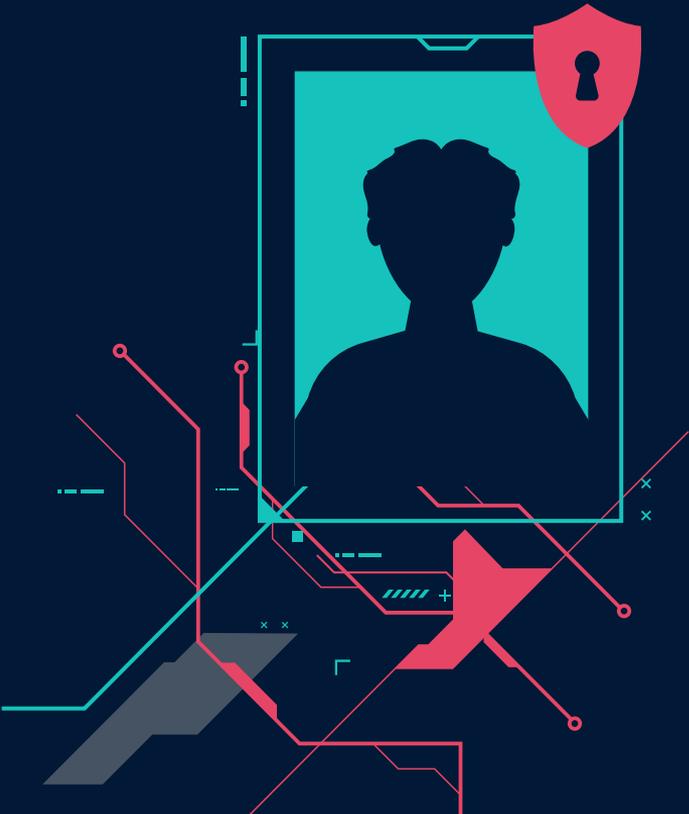
```
},
  "groupIdNT": "5814765",
  "groupNameIS": "All Countries",
  "groupNameRV": "All Countries",
  "battery": 12,
  "serverInitTimestamp": "1743621446061",
  "gmtMinutesOffset": -420,
  "mnc": 65535,
  "isLimitAdTrackingEnabled": "false",
  "abt": "A",
  "sessionId": "9E60256B-C2FD-410A-9E5F-A7FF85533F7E",
  "appKey": "1fda3d735",
  "deviceOS": "ios",
  "appVersion": "7.66.0",
  "bannerSamplingMultiplier": "10",
  "groupNameNT": "All Countries",
  "icc": "—",
  "idfi": "a869f4dc-be3a-425d-8833-567806ac6d9d",
  "bannerSampling": "false",
  "timestamp": 1743644258954,
  "deviceModel": "iPhone10,2",
  "aid": "FC84A751-39C2-4BFB-B4B0-3E8582B17142",
  "xCodeSdkName": "iphonios18.0",
  "firstSession": "false",
  "language": "EN-US",
  "groupIdBN": "5814763",
  "is_coppa": "false",
  "deviceOS": "ios",
  "appVersion": "7.66.0",
  "bannerSamplingMultiplier": "10",
```



What does this data look like?

- Data going to advertisers look like above. There is also Ad Tracking Transparency.
- This happens for both free and paid situations.
- **POST request to app-analytics-services-att.com**





05

Results

What I found and what its impact is.

Mediation Contents (Duo Paid)

```
{
  "xCodeVersion": "1600",
  "osVersion": "16.7.10",
  "connectionType": "wifi",
  "jb": "false",
  "bundleId": "com.duolingo.DuolingoMobile",
  "events": [
    {
      "eventSessionId": "9E60256B-C2FD-410A-9E5F-A7FF85533F7E",
      "firstSessionTimestamp": 1730015217402,
      "timestamp": 1743644258886,
      "eventId": 44,
      "rawConnectionType": "wifi",
      "duration": 45223
    }
  ],
  "mobileCarrier": "--",
  "groupNameBN": "All Countries",
  "abGroup": "NONE",
  "mt": "AdMob87000SDK1200iAds510",
  "groupIdRV": "5814759",
  "abInternal": "lpmm_abc_0331_disable",
  "tz": "America/Los_Angeles",
  "xCodeBuildVersion": "16A242d",
  "mcc": 65535,
  "advertisingIdType": "IDFA",
  "abHashValue": "0",
  "internalFreeMemory": 29950,
  "att": 3,
  "idfv": "F010F50F-0AC9-48DC-9BE9-21B35021EE78",
  "controllerABValue": "4",
  "deviceOEM": "Apple",
  "sdkVersion": "8.7.0",
  "advertisingId": "D991D864-A78D-4600-B8E0-1B2D45D438B5",
  "xCodeSdkBuild": "22A3362",
  "internalTestId": {
    "99": "129"
  }
}
```

```
},
  "mobileCarrier": "--",
  "groupNameBN": "All Countries",
  "abGroup": "NONE",
  "mt": "AdMob87000SDK1200iAds510",
  "groupIdRV": "5814759",
  "abInternal": "lpmm_abc_0331_disable",
  "tz": "America/Los_Angeles",
  "xCodeBuildVersion": "16A242d",
  "mcc": 65535,
  "advertisingIdType": "IDFA",
  "abHashValue": "0",
  "internalFreeMemory": 29950,
  "att": 3,
  "idfv": "F010F50F-0AC9-48DC-9BE9-21B35021EE78",
  "controllerABValue": "4",
  "deviceOEM": "Apple",
  "sdkVersion": "8.7.0",
  "advertisingId": "D991D864-A78D-4600-B8E0-1B2D45D438B5",
  "xCodeSdkBuild": "22A3362",
  "internalTestId": {
    "99": "129"
  }
},
  "groupIdNT": "5814765",
  "groupNameIS": "All Countries",
  "groupNameRV": "All Countries",
  "battery": 12,
  "serverInitTimestamp": "1743621446061",
  "gmtMinutesOffset": -420,
  "mnc": 65535,
  "isLimitAdTrackingEnabled": "false",
  "abt": "A",
  "sessionId": "9E60256B-C2FD-410A-9E5F-A7FF85533F7E",
  "appKey": "1fda3d735",
  "deviceOS": "ios",
  "appVersion": "7.66.0",
  "bannerSamplingMultiplier": "10",
  "groupNameNT": "All Countries",
  "icc": "--",
  "idfi": "a869f4dc-be3a-425d-8833-567806ac6d9d",
  "bannerSampling": "false",
  "timestamp": 1743644258954,
  "deviceModel": "iPhone10,2",
  "aid": "FC84A751-39C2-4BFB-B4B0-3E8582B17142",
  "xCodeSdkName": "iphoneos18.0",
  "firstSession": "false",
  "language": "EN-US",
  "groupIdBN": "5814763",
  "is_coppa": "false",
  "groupIdIS": "5814761"
},
```

```
},
  "groupIdNT": "5814765",
  "groupNameIS": "All Countries",
  "groupNameRV": "All Countries",
  "battery": 12,
  "serverInitTimestamp": "1743621446061",
  "gmtMinutesOffset": -420,
  "mnc": 65535,
  "isLimitAdTrackingEnabled": "false",
  "abt": "A",
  "sessionId": "9E60256B-C2FD-410A-9E5F-A7FF85533F7E",
  "appKey": "1fda3d735",
  "deviceOS": "ios",
  "appVersion": "7.66.0",
  "bannerSamplingMultiplier": "10",
  "groupNameNT": "All Countries",
  "icc": "--",
  "idfi": "a869f4dc-be3a-425d-8833-567806ac6d9d",
  "bannerSampling": "false",
  "timestamp": 1743644258954,
  "deviceModel": "iPhone10,2",
  "aid": "FC84A751-39C2-4BFB-B4B0-3E8582B17142",
  "xCodeSdkName": "iphoneos18.0",
  "firstSession": "false",
  "language": "EN-US",
  "groupIdBN": "5814763",
  "is_coppa": "false",
  "groupIdIS": "5814761"
},
```

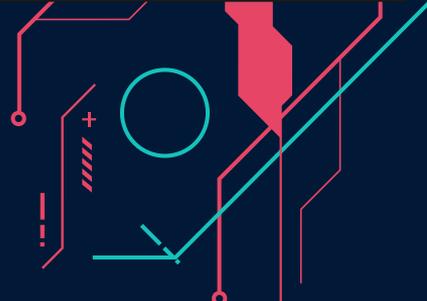


Mediation Contents (Busuu Paid)

```
"deviceModel" : "iPhone10,2",
"bannerSamplingMultiplier" : "10",
"jb" : "false",
"firstSession" : "false",
"mcc" : 65535,
"groupIdBN" : "3801541",
"bannerSampling" : "false",
"att" : 3,
"bundleId" : "com.busuu.english.app",
"appVersion" : "28.31.0",
"appKey" : "1af944565",
"xCodeSdkName" : "iphoneos18.1",
"deviceOEM" : "Apple",
"is_coppa" : "false",
"abGroup" : "NONE",
"internalTestId" : {
},
"abHashValue" : "0",
"connectionType" : "wifi",
"gmtMinutesOffset" : -420,
"advertisingId" : "D991D864-A78D-4600-B8E0-1B2D45D43BB5",
"mnc" : 65535,
"icc" : "-",
"osVersion" : "16.7.10",
"controllerABValue" : "13",
"deviceOS" : "ios",
"mobileCarrier" : "-",
"advertisingIdType" : "IDFA",
"battery" : 30,
"mt" : "MAX",
"isLimitAdTrackingEnabled" : "false",
"idfv" : "E8BAEEC1-41AC-463D-A603-768C4D66ED12",
"groupIdRV" : "3801537",
"serverInitTimestamp" : "1743458042356",
```

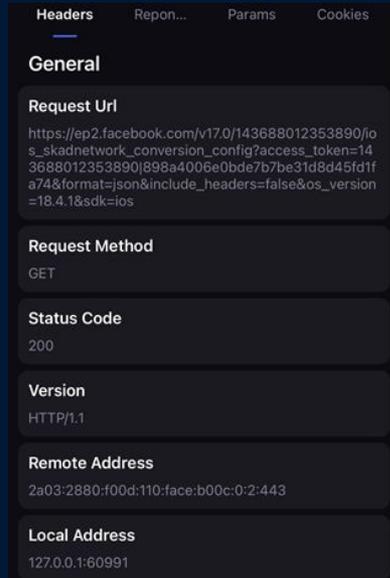
```
"xCodeVersion" : "1610",
"tz" : "America/Los_Angeles",
"groupIdIS" : "3801539",
"internalFreeMemory" : 30447,
"groupIdNT" : "5124423",
"xCodeSdkBuild" : "22B74",
"groupNameRV" : "All Countries",
"sdkVersion" : "8.1.0",
"xCodeBuildVersion" : "16B40",
"groupNameNT" : "All Countries",
"abt" : "A",
"events" : [
  {
    "eventSessionId" : "7562F58F-209B-4C77-924C-7E79569246D6",
    "timestamp" : 1743458180909,
    "eventId" : 44,
    "firstSessionTimestamp" : 1738972311000,
    "duration" : 70622
  }
],
"sessionId" : "7562F58F-209B-4C77-924C-7E79569246D6",
"groupNameIS" : "All Countries",
"language" : "EN-US",
"aid" : "1D47F676-AF79-4AA4-9647-25D5C5D7B22E",
"groupNameBN" : "All Countries",
"timestamp" : 1743458180981
```

```
{
  "d": {
    "ac": "4293181",
    "ap": "538681648",
    "id": "8f34849cea3ed670",
    "ti": 1743628952225,
    "tk": "4257740",
    "tr": "6bd9b11916e81ac97d871adb0053789c",
    "ty": "Mobile"
  },
  "v": [
    0,
    2,
    1
```



Ping Contents (Memrise Paid)

- Memrise did not have any ads mediation transferred in the test period.
- Free and Paid versions were the same.
- ep2.facebook.com (facebook ads service) was present.



Headers Repon... Params Cookies

General

Request Url
https://ep2.facebook.com/v17.0/143688012353890/ios_skadnetwork_conversion_config?access_token=143688012353890j898a4006e0bde7b7be31d8d45fd1fa74&format=json&include_headers=false&os_version=18.4.1&sdk=ios

Request Method
GET

Status Code
200

Version
HTTP/1.1

Remote Address
2a03:2880:f00d:110:face:b00c:0:2:443

Local Address
127.0.0.1:60991



Headers Reponse Params Cookies

Preview Copy

```
{
  "data": [
    {
      "cutoff time": 2,
      "timer_buckets": 0,
      "is_coarse_cv_accumulative":
false,
      "timer interval": 82800,
      "conversion_value_rules": [
        {
          "conversion value": 58,
          "events": [
            {
              "event_name":
"fb_mobile_activate_app"
            }
          ]
        },
        {
          "conversion value": 59,
          "events": [
            {
              "event_name":
"fb_mobile_complete_registration"
            }
          ]
        },
        {
          "conversion value": 60,
          "events": [
            {
              "event_name":
"fb_mobile_purchase"
            }
          ]
        }
      ]
    }
  ]
}
```

<> View File



Impact

- Mobile apps with subscriptions say you are not getting ads when you're using them on paid mode.
- Categorically true, but they still can sell your data.
- Advertisers can also get a piece if their APIs are still included.
- Even if the data leakage is small, stay away from companies that leak your data when they say they're not.



Future Work

- See how Android versions of the apps operate
- Do further research into the ad formats on Unity3D mediation
- Find a way to get a copy of what is being POSTed to the ATT servers at the end of lessons
- And much more...



Summary

- Language learning apps are new ways to learn languages.
- Online advertising has many moving parts
- Network sniffers with MITM attacks are useful for reading most web traffic
 - Storm Sniffer is a cheap all-in-one network sniffer.
- Duolingo and Busuu send user info to Unity3D mediation in their paid versions when they're not supposed to.





THANKS FOR WATCHING!

Do you have any questions?

plascencia.matt.31@gmail.com

<https://substack.com/@matthewplascencia>

<https://www.youtube.com/@forensicswithmatt>

