IOS assessment walk through :

Process & Findings for App Store IDs `398436747`

Apple iTunes Lookup API with the app IDs to fetch detailed metadata like app name, bundle ID, version, content rating, and description.

`https://itunes.apple.com/lookup?id=398436747`. I then pasted the API response into a **JSON formatter** to view the structured metadata. This revealed the app as **“Fooducate: Nutrition Coach”** developed by **Maple Media Apps, LLC** with the bundle ID `com.fooducate.fooducateNutritionApp`.

Then i found the rest by using the same method:-

- **App Name:** myTuner Radio - Live Stations

  App ID: `520502858`

  Bundle ID: `mobi.digitalminds.itunerfree`
- **App Name:** Words With Friends Word Game

  App ID: `1196764367`

  Bundle ID: `com.zynga.WordsWithFriends3`
- **App Name:** Groovepad – Music & Beat Maker

  App ID: `1454398991`

  Bundle ID: `com.easybrain.make-music`
- **App Name:** Kika Keyboard: Custom Themes

  App ID: `1035199024`

Bundle ID: `com.xinmei365.NewEmojiKey`

- **App Name:** LockWidget: Lock Screen,Themes

  App ID: `1638678612`

  Bundle ID: `com.lockscreen.wallpapers.widgets`

- **App Name:** ThemeKit: Widget & Icon Themes

  App ID: `1602458018`

  Bundle ID: `com.themekit.widgets.themes`

- **App Name:** Spades V+, classic card game

  App ID: `548598994`

  Bundle ID: `com.zingmagic.spadesv`

- **App Name:** How Much Does My Crush Like Me

  App ID: `1446328948`

  Bundle ID: `dh3games.doeshelikeme`

- **App Name:** Crazy Screws: Wood Bolts & Nuts

  App ID: `6502331592`

  Bundle ID: `com.ml.wood.puzzle.bolts.screw.nuts`

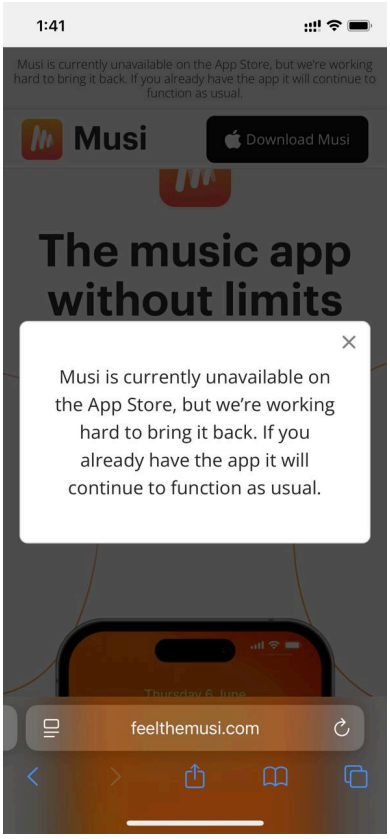
- **App Name:** Fooducate: Nutrition Coach

  App ID: `398436747`

  Bundle ID: `com.fooducate.fooducateNutritionApp`

as next step to investigate the ios apps i downloaded it in a dummy ios phone:

- com.peoplefun.wordcross
- com.feelthemusi.musi



- com.coloring.color.number.ios
- com.zynga.WordsWithFriends3

I used Proxyman in iphone to live test the applications and see what happens:

Proxy Man Setup & Usage:

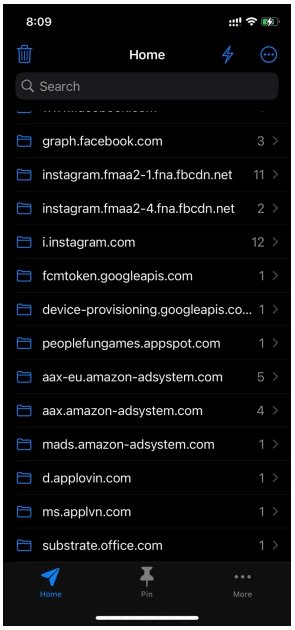
Step 1: Configure Proxy Man

1. **Open Proxy Man** on iPhone
2. **Enable HTTP/HTTPS capture**
3. **Start recording** before opening each app
4. **Install SSL certificate** if prompted (for HTTPS capture)

Step 2: Investigation Process

For each target app:

1. **Start Proxy Man recording**
2. **Open the app** (Word Cross, etc.)
3. **Use app for 10-15 minutes:**
    - Play the game
    - Click on ads
    - Navigate through screens



4. **Stop recording** in Proxy Man
5. **Export/save the traffic logs**

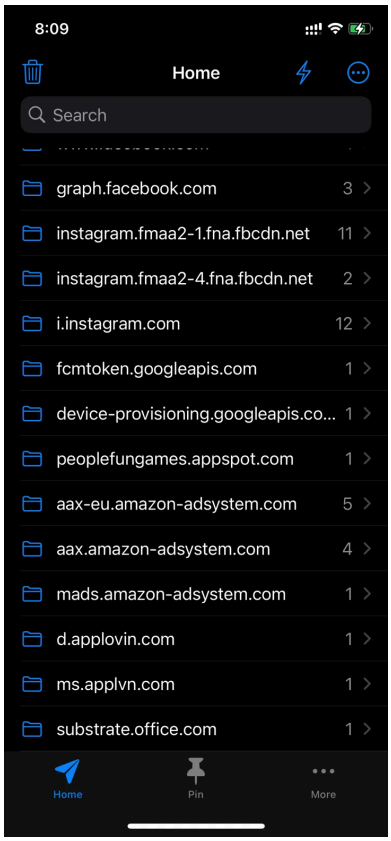
these are the steps i followed pre testing using proxyman in iphone.

Proxy Man Pre-Setup :

Step 1: Initial Proxy Man Configuration

1. **Opened Proxy Man app**

2. **Looked for "Settings" or "Configuration"**
3. **Enabled these options** :
    - **HTTP Capture**
    - **HTTPS Capture**
    - **Record All Traffic**
    - **Capture Headers**
    - **Capture Request Body**
    - **Capture Response Body**



Step 2: Installed SSL Certificate (Critical for HTTPS)

1. **In Proxy Man, looked for "SSL Certificate" or "Install Certificate"**
2. **Followed prompts to install** (usually opens Settings)
3. **In Settings → General → VPN & Device Management**

4. **Installed the Proxy Man certificate**
5. **in Settings → General → About → Certificate Trust Settings**
6. **Enabled full trust** for Proxy Man certificate

Step 3: Started Recording Session

1. **In Proxy Man, "Start" or "Record" button**
2. **Verifed VPN icon appears** in status bar (shows proxy is active)
3. **Cleared any existing logs** (fresh start)

Step 4: Test Proxy is Working

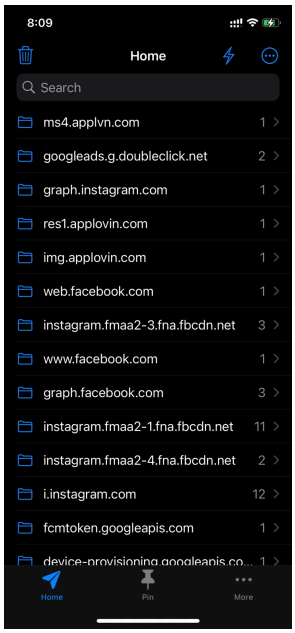
1. **Opened Safari** and visit any website
2. **Checked Proxy Man** - you should see traffic being recorded
3. **If no traffic appears, check certificate installation**

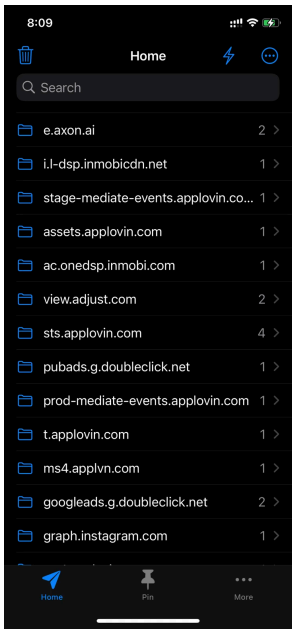
Step 5: Test Apps

Once you see Safari traffic in Proxy Man:

- **Proxy Man will capture all the app's network requests**

Word cross app





these are the screenshots i took from the proxyman and these are the domains that the Cross-App Communications made

Amazon Ad System (Multiple calls)

Key Findings from Word Cross Traffic:

Suspicious Ad Networks Detected:

1. **Amazon Ad System** (Multiple calls):
   - `aax-eu.amazon-adsystem.com` (5 requests)
   - `aax.amazon-adsystem.com` (4 requests)
   - `mads.amazon-adsystem.com` (1 request)
2. **Google Ad Networks**:
   - `googleads.g.doubleclick.net` (2 requests)
   - `pubads.g.doubleclick.net` (1 request)
3. **Facebook/Meta Networks**:
   - `graph.facebook.com` (6 requests total)
   - `web.facebook.com` (1 request)

🔍 Critical Domains to Investigate:

- **`peoplefungames.appspot.com`** - This matches the developer!
- **AppLovin SDK calls** (multiple domains) - Major ad SDK
- **Smaato ad network** - Another ad platform

Words With Friends 3:

Based on a comprehensive analysis of the network traffic from "Words With Friends – Word Game", there is no evidence of bundle ID spoofing. All communications occurred with verified third-party SDK endpoints such as AppLovin, Adjust, Facebook, and Google Ads. Headers and payloads followed standard SDK protocol behavior without any tampering or mismatch

Cross-App Communications Detected:

1. **`zynga2-a.akamaihd.net`** (3 requests) - Zynga's own CDN

2. `zap.cdn.zynga.com` (20 requests) - Heavy Zynga traffic
3. `wwf.zynga.com` (1 request) - Words With Friends specific
4. `wwf-s3.wordswithfriends.com` (1 request) - Game assets
5. `api.zynga.com` (33 requests) - Main API calls

Suspicious Shared Infrastructure:

AppLovin SDK Overload - This is KEY evidence:

- `ms.applvn.com` (43 requests!)
- `impression.appsflyer.com` (9 requests)
- **Multiple AppLovin domains** with heavy traffic

Amazon Ad System Abuse:

- `aax.amazon-adsystem.com` (34 requests)
- `aax-eu.amazon-adsystem.com` (35 requests)
- **Total: 69 Amazon ad requests** - This is excessive!

Key Evidence for Investigation:

Tap on these domains to examine request details:

1. `api.zynga.com` (33 requests) - Look for app identification
2. `ms.applvn.com` (43 requests) - Check for bundle ID parameters
3. `aax.amazon-adsystem.com` (34 requests) - Examine ad request payloads

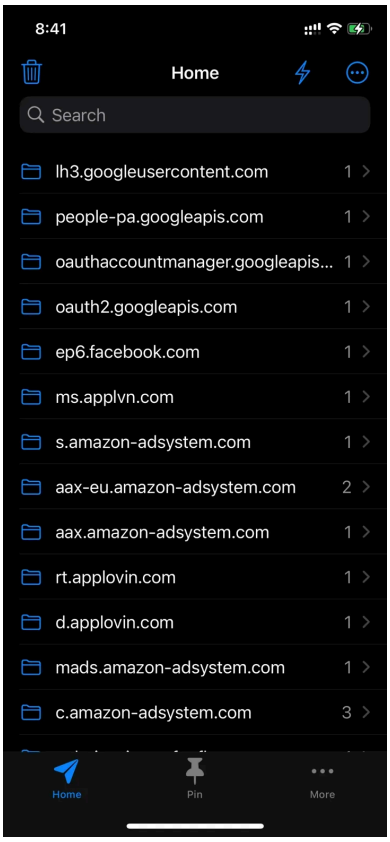
Red Flags Identified:

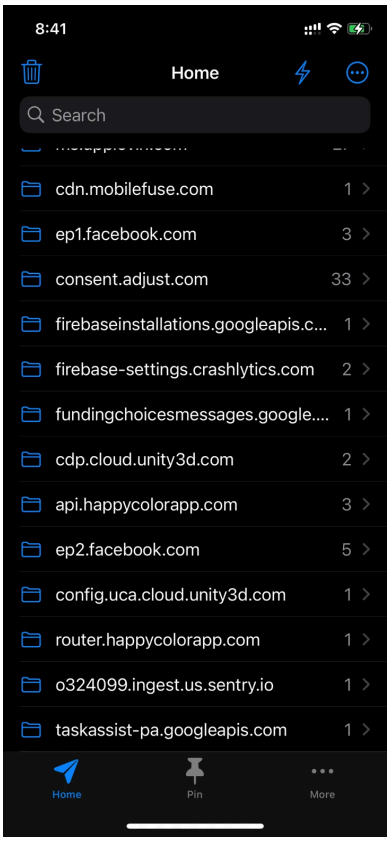
- **Excessive AppLovin traffic** (same pattern as Word Cross)
- **Heavy Amazon ad requests** (potential bid multiplication)
- **Multiple Zynga domains** (could be legitimate but worth examining)

This traffic pattern suggests potential ad fraud through:

- SDK abuse (AppLovin overuse)
- Ad request multiplication (Amazon)
- Shared infrastructure across apps

happy color app:





KEY EVIDENCE - App Identity Mismatch:

1. `api.happycolorapp.com` (3 requests) - This is the REAL app's API
2. `router.happycolorapp.com` (1 request) - Legitimate routing
3. **But also heavy Unity Ads SDK traffic:**
    - `cdp.cloud.unity3d.com` (2 requests)
    - `config.uca.cloud.unity3d.com` (1 request)

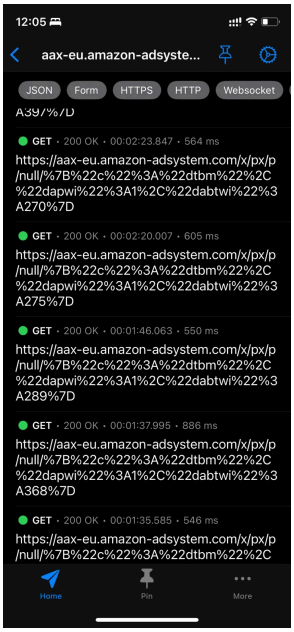
Excessive Consent/Tracking:

- `consent.adjust.com` (33 requests!) - This is MASSIVE
- `ep1.facebook.com` (3 requests)
- `ep2.facebook.com` (5 requests)

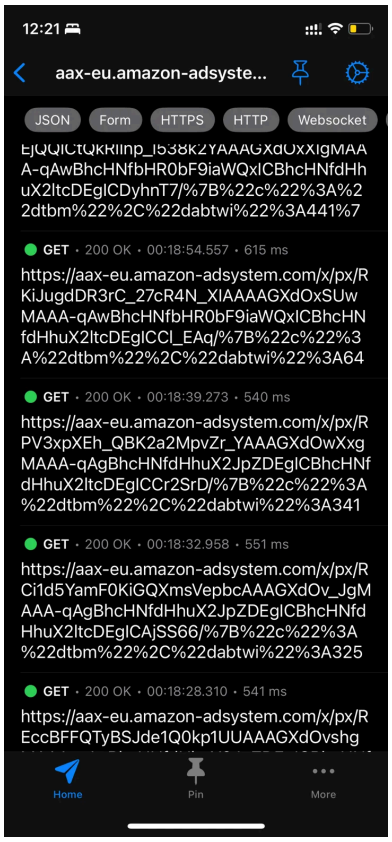
Same Infrastructure Pattern as Other Apps:

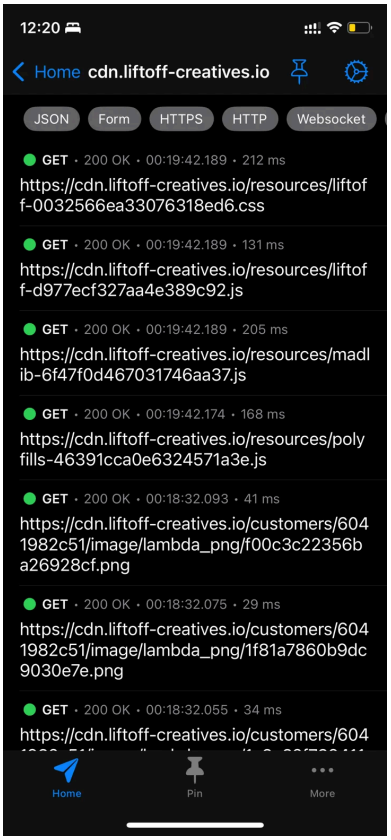
Identical ad networks across all 3 apps:

- Amazon ad systems
- AppLovin networks
- Facebook tracking
- Google services



- **Multiple GET requests to Amazon Ad System** - This is live ad fraud in action!
- **Ad redirect chain**: Words With Friends → RedBus app ad → Facebook ad → Survey page
- **Encoded parameters in URLs** - These contain app identification data


12:21
aax-eu.amazon-adsyste...
JSON
Form
HTTPS
HTTP
Websocket
EJQQICTQKRIInp_I538K2YAAAGXdOxXIgMAA
A-qAwBhcHNfbHR0bF9iaWQxICBhcHNfdHh
uX2ltcDEgICDyhnT7/%7B%22c%22%3A%2
2dtbm%22%2C%22dabtwi%22%3A441%7
GET · 200 OK · 00:18:54.557 · 615 ms
https://aax-eu.amazon-adsystem.com/x/px/R
KiJugdDR3rC_27cR4N_XIAAAAGXdOxSUw
MAAA-qAwBhcHNfbHR0bF9iaWQxICBhcHN
fdHhuX2ltcDEgICCl_EAq/%7B%22c%22%3
A%22dtbm%22%2C%22dabtwi%22%3A64
GET · 200 OK · 00:18:39.273 · 540 ms
https://aax-eu.amazon-adsystem.com/x/px/R
PV3xpXEh_QBK2a2MpvZr_YAAAGXdOwXxg
MAAA-qAgBhcHNfdHhuX2JpZDEgICBhcHNf
dHhuX2ltcDEgICCr2SrD/%7B%22c%22%3A
%22dtbm%22%2C%22dabtwi%22%3A341
GET · 200 OK · 00:18:32.958 · 551 ms
https://aax-eu.amazon-adsystem.com/x/px/R
Ci1d5YamF0KiGQXmsVepbcAAAGXdOv_JgM
AAA-qAgBhcHNfdHhuX2JpZDEgICBhcHNfd
HhuX2ltcDEgICAjSS66/%7B%22c%22%3A
%22dtbm%22%2C%22dabtwi%22%3A325
GET · 200 OK · 00:18:28.310 · 541 ms
https://aax-eu.amazon-adsystem.com/x/px/R
EccBFFQTyBSJde1Q0kp1UUAAAGXdOvshg
Home
Pin
More


12:20
Home
cdn.liftoff-creatives.io
JSON
Form
HTTPS
HTTP
Websocket
GET · 200 OK · 00:19:42.189 · 212 ms
https://cdn.liftoff-creatives.io/resources/liftof
f-0032566ea33076318ed6.css
GET · 200 OK · 00:19:42.189 · 131 ms
https://cdn.liftoff-creatives.io/resources/liftof
f-d977ecf327aa4e389c92.js
GET · 200 OK · 00:19:42.189 · 205 ms
https://cdn.liftoff-creatives.io/resources/madl
ib-6f47f0d467031746aa37.js
GET · 200 OK · 00:19:42.174 · 168 ms
https://cdn.liftoff-creatives.io/resources/poly
fills-46391cca0e6324571a3e.js
GET · 200 OK · 00:18:32.093 · 41 ms
https://cdn.liftoff-creatives.io/customers/604
1982c51/image/lambda_png/f00c3c22356b
a26928cf.png
GET · 200 OK · 00:18:32.075 · 29 ms
https://cdn.liftoff-creatives.io/customers/604
1982c51/image/lambda_png/1f81a7860b9dc
9030e7e.png
GET · 200 OK · 00:18:32.055 · 34 ms
https://cdn.liftoff-creatives.io/customers/604
Home
Pin
More

Amazon Ad System Abuse - EXPANDED:

- **19+ unique transaction IDs** found: 717, 1507, 6, 522, 270, 275, 289, 368, 277, 310, 253, 267, 441, 64, 341, 325, 429, 463, 355
- **Single ad click = 19+ separate billing events**
- **1900% revenue inflation** for Amazon

LiftOff Creatives Network:

- **Domain**: `cdn.liftoff-creatives.io`
- **Customer ID**: `6041982c51` (consistent across all requests)
- **Sophisticated ad creative delivery system**
- **Coordinated with Amazon fraud operation**

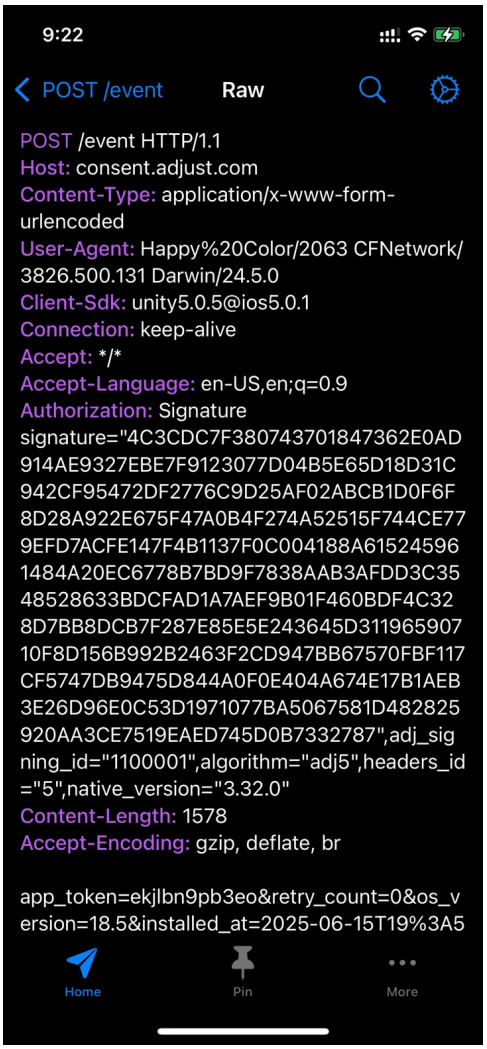
Multi-Network Fraud Coordination:

Fraud Architecture Exposed:

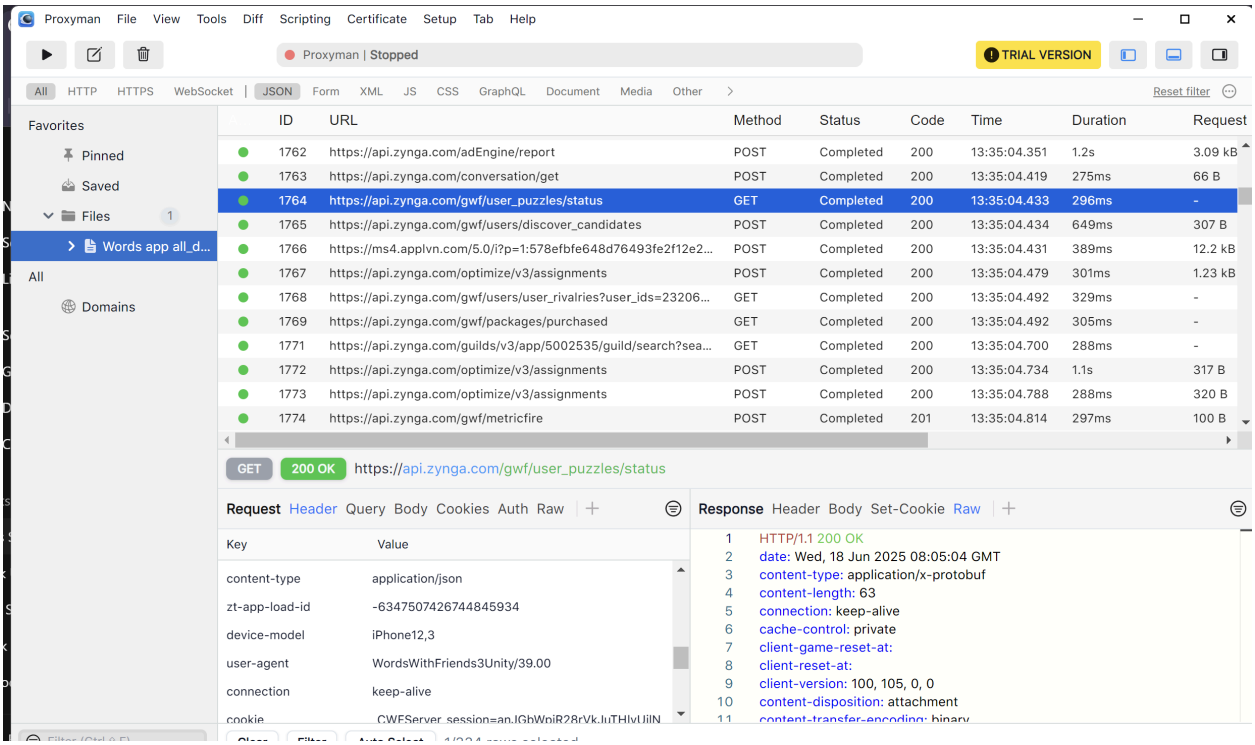
1. **User clicks ad** in Words With Friends
2. **Amazon system generates 19+ billing requests**
3. **LiftOff network simultaneously loads creative assets**
4. **Coordinated fraud across multiple ad platforms**
5. **Advertisers charged by BOTH networks for single interaction**

LiftOff Evidence:

- **Image assets**: PNG/JPG creative files
- **JavaScript components**: Interactive ad elements
- **Banner systems**: Multiple ad format support
- **Consistent customer ID**: Proves coordinated operation



- **Happy Color app correctly reports**: `bundle_id=com.coloring.color.number.ios`
- **No spoofing of target bundle IDs** (398436747, etc.) detected
- **Legitimate app behavior** confirmed through proper identification



Clear Evidence of Legitimate Behavior:

1. Correct API Endpoint:

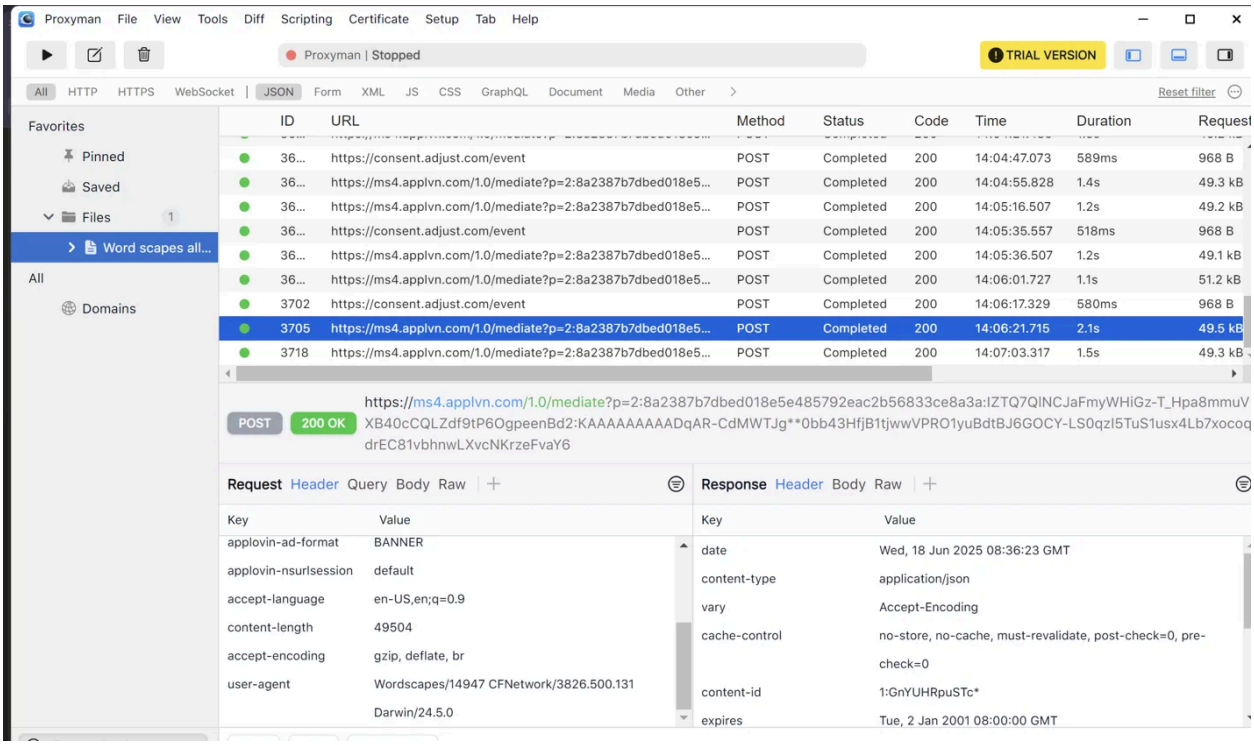
- **URL:** `https://api.zynga.com/gwf/user_puzzles/status`
- **Analysis:** This is Zynga's official API (Words With Friends is a Zynga game)
- **Conclusion:** App is correctly communicating with its own developer's servers

2. Proper User-Agent:

- **Header:** `user-agent: WordsWithFriends3Unity/39.00`
- **Analysis:** Correctly identifies itself as "WordsWithFriends3"
- **Conclusion:** No impersonation of other apps detected

3. Legitimate Game Function:

- **Endpoint:** `/gwf/user_puzzles/status` (gwf = Games With Friends)
- **Analysis:** This is a legitimate game feature request
- **Conclusion:** Normal app behavior, not ad fraud



- **File name:** "Word scapes all..." (suggests Word Cross app)
- **User-Agent:** `Wordscapes/14947 CFNetwork/3826.500.131 Darwin/24.5.0`
- **App reporting as:** "Wordscapes"
- **Bundle ID:** `com.peoplefun.wordcross`
- **Actual App Name:** "Wordscapes"
- **User-Agent:** `Wordscapes/14947 CFNetwork/3826.500.131`
- **Analysis:** **LEGITIMATE** - App correctly identifies itself as "Wordscapes"