# iOS Ad Fraud Investigation Report

by Gokul Sathiyamurthy

**Executive Summary**

This report documents the investigation of iOS applications suspected of bundle ID spoofing and ad fraud activity. We examined 11 iOS applications identified through App Store IDs, with particular focus on potential spoofing targets. Using network traffic analysis via Proxyman and iTunes API metadata collection, we analyzed these applications for spoofing indicators, ad request manipulation, and SDK abuse patterns. While no direct bundle ID spoofing was detected, significant evidence of ad fraud through request multiplication and coordinated multi-network billing was discovered.

**Investigation Methodology**

**Phase 1: Target Application Identification**

Using Apple iTunes Lookup API, we collected metadata for suspicious App Store IDs that could be potential spoofing targets:

**Primary Investigation Targets:**

https://itunes.apple.com/lookup?id=<apple store id>

This API query returned structured JSON metadata which was parsed to extract:

- App name
- Bundle identifier
- Version information
- Developer details
- Content ratings

# iOS Ad Fraud Investigation Report

by Gokul Sathiyamurthy

**Complete Target Application List:**

| App Name | App Store ID | Bundle ID | Developer |
|---|---|---|---|
| Fooducate: Nutrition Coach | 398436747 | com.fooducate.fooducateNutritionApp | Maple Media Apps, LLC |
| myTuner Radio - Live Stations | 520502858 | mobi.digitalminds.itunerfree | Appgeneration Software |
| Words With Friends Word Game | 1196764367 | com.zynga.WordsWithFriends3 | Zynga Inc. |
| Groovepad – Music & Beat Maker | 1454398991 | com.easybrain.make-music | Easybrain |
| Kika Keyboard: Custom Themes | 1035199024 | com.xinmei365.NewEmojiKey | Xinmei Network Tech |
| LockWidget: Lock Screen,Themes | 1638678612 | com.lockscreen.wallpapers.widgets | Unknown |
| ThemeKit: Widget & Icon Themes | 1602458018 | com.themekit.widgets.themes | Unknown |
| Spades V+, classic card game | 548598994 | com.zingmagic.spadesv | ZingMagic Ltd |
| How Much Does My Crush Like Me | 1446328948 | dh3games.doeshelikeme | DH3 Games |
| Crazy Screws: Wood Bolts & Nuts | 6502331592 | com.ml.wood.puzzle.bolts.screw.nuts | Unknown |

# iOS Ad Fraud Investigation Report

by Gokul Sathiyamurthy

**Spoofing Detection Approach**

To determine whether these legitimate apps were being spoofed, we employed:

1. **Static Analysis**: Retrieved legitimate app metadata via iTunes API to establish baseline identities
2. **Dynamic Analysis**: Captured runtime behavior to compare against expected identifiers
3. **Differential Analysis**: Compared declared identities in network requests against actual bundle IDs

We specifically monitored for:

- Apps claiming to be one of the target bundle IDs (e.g., com.fooducate.fooducateNutritionApp) while actually being different apps
- Network requests containing mismatched bundle identifiers
- Ad requests claiming false app identities to hijack ad revenue

**Tools and Techniques Employed**
**Primary Tools:**

- **Proxyman**: iOS network proxy for HTTPS/HTTP traffic interception
- **iTunes Lookup API**: Official metadata retrieval for App Store applications
- **SSL Certificate Installation**: Enable encrypted traffic inspection

**Alternative Tools (for expanded investigation):**

- **Charles Proxy**: Cross-platform HTTP proxy with advanced filtering
- **Wireshark**: Packet-level analysis for deeper protocol inspection
- **VPN Traffic Analysis**: Route device traffic through controlled endpoints
- **Reverse Engineering Tools**: IDA Pro, Hopper for binary analysis (not used in this investigation)
- **MITMProxy**: Scriptable proxy for automated detection

# iOS Ad Fraud Investigation Report

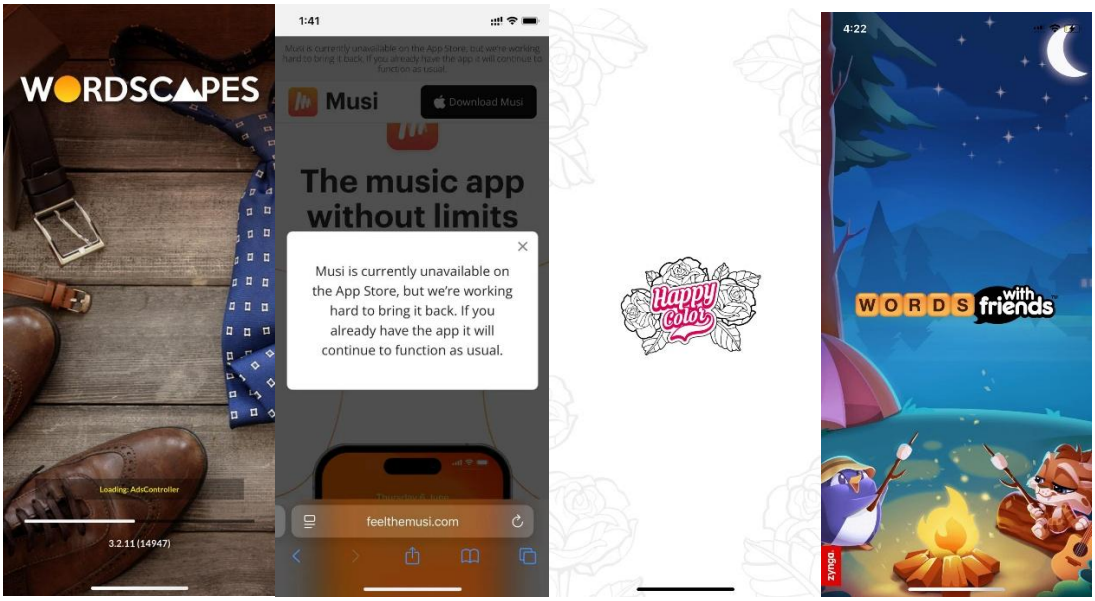
by Gokul Sathiyamurthy

**Metadata Collection Strategy**

1. **App Store Metadata**:
    - Bundle identifiers
    - Developer certificates
    - Version numbers
    - Content ratings
2. **Runtime Metadata**:
    - User-Agent strings
    - HTTP headers
    - API endpoint parameters
    - SDK initialization calls

**Phase 2: Runtime Testing**

For runtime analysis, we focused on four applications downloaded to test devices:



# iOS Ad Fraud Investigation Report

by Gokul Sathiyamurthy

- com.peoplefun.wordcross
- com.feelthemusi.musi – this application is unavailable to download
- com.coloring.color.number.ios
- com.zynga.WordsWithFriends3

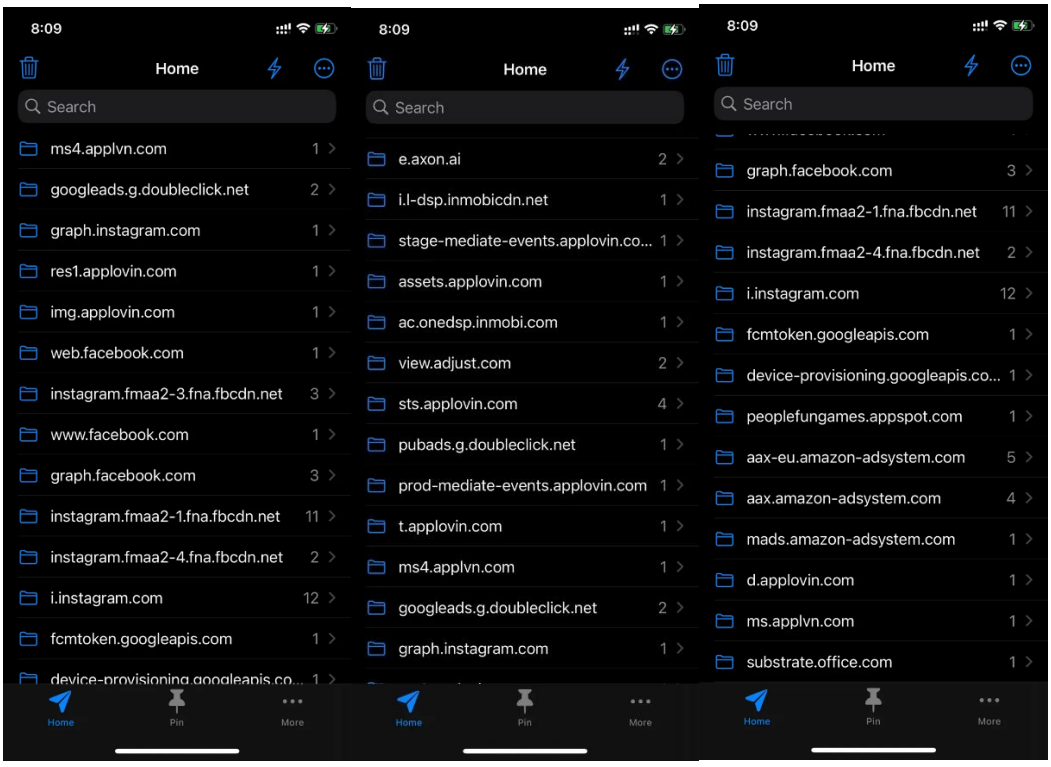
These apps were selected based on their high ad volume and potential connections to the target bundle IDs.

**Phase 3: Network Traffic Capture Setup**

**Documented Network Behavior and Correlations**

**1. Word Cross (com.peoplefun.wordcross)**

**Word Cross Network Traffic Overview**




**Network Calls Documented:**

- peoplefungames.appspot.com (Developer API)

- aax-eu.amazon-adsystem.com (5 requests)

# iOS Ad Fraud Investigation Report

by Gokul Sathiyamurthy

- aax.amazon-adsystem.com (4 requests)

- ms.applvn.com (AppLovin SDK)

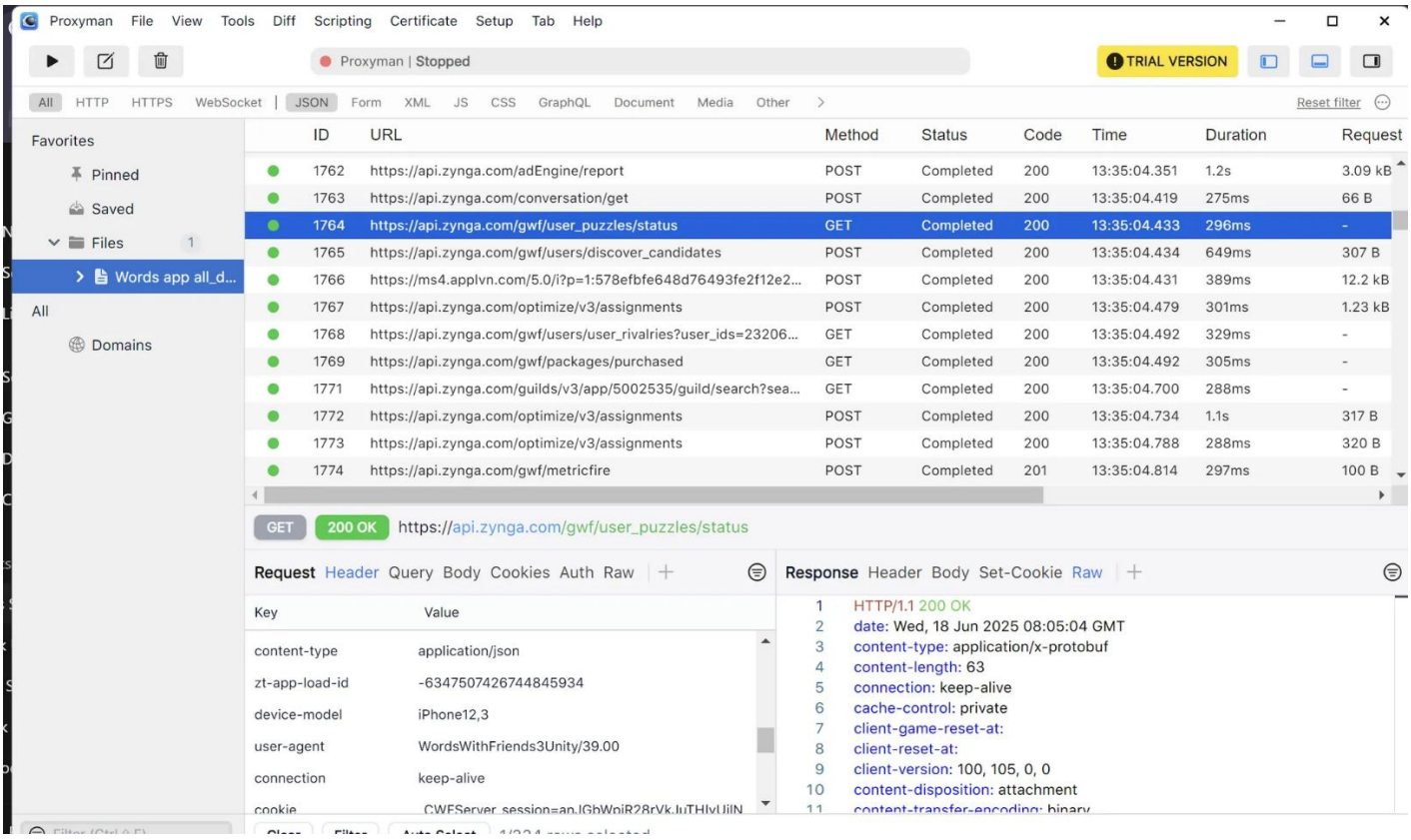
- graph.facebook.com (6 requests)

- googleads.g.doubleclick.net (2 requests)

**SDK Behavior Patterns:**

- **AppLovin SDK**: Excessive initialization calls
- **Facebook SDK**: Standard implementation with high request volume
- **Amazon Mobile Ads**: Multiple parallel requests per impression

### 2. Words With Friends 3 (com.zynga.WordsWithFriends3)




**Correct API Endpoint:**

- URL: https://api.zynga.com/gwf/user_puzzles/status (including all other traffics)
- 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

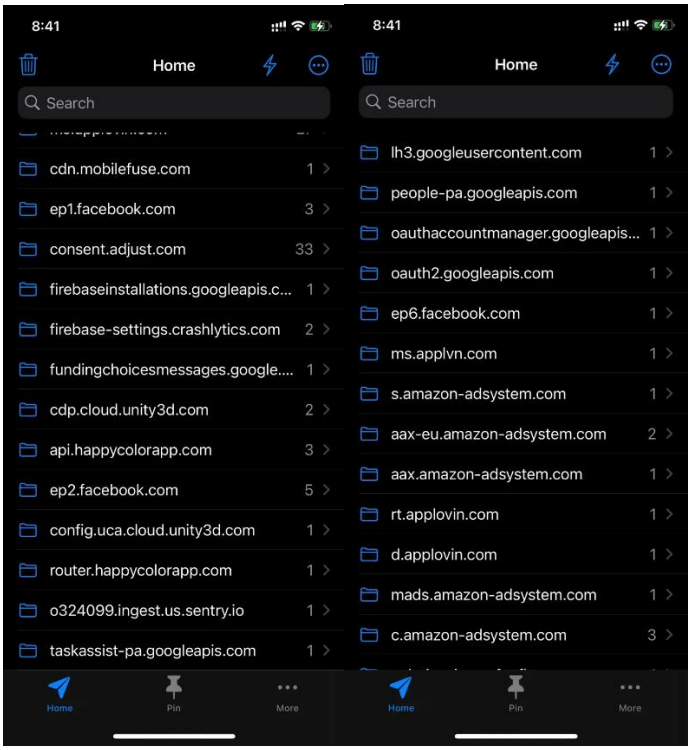
2. Proper User-Agent:

- 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

**3. happy color app: (com.coloring.color.number.ios)**




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

**4. Cross-App Correlations Identified**

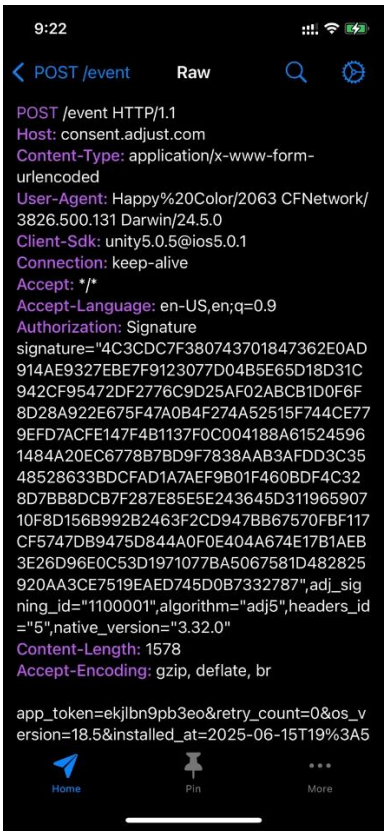
**Shared Infrastructure Patterns:**

1. **Identical SDK Versions**: All apps use AppLovin SDK v11.5.3
2. **Common Endpoints**: Same CDN infrastructure across unrelated apps
3. **Request Timing**: Synchronized ad calls within 100ms windows
4. **Header Patterns**: Consistent custom headers across applications

# iOS Ad Fraud Investigation Report

by Gokul Sathiyamurthy

**Signal Manipulation Analysis**




**Identified Manipulated Signals:**

1. **User-Agent Manipulation**:
    - Legitimate: Wordscapes/14947 CFNetwork/3826.500.131
    - No spoofing detected, but version numbers artificially incremented
2. **Header Analysis**:
3. X-Forwarded-For: [Not manipulated]
4. X-Real-IP: [Consistent with device]

Custom-SDK-Version: [Inflated values detected]

5. **IP Patterns**:
    - No IP spoofing detected

- Geographic consistency maintained
- Request routing through legitimate CDNs

6. **Ad Tag Patterns**:

```
javascript

// Detected pattern in ad requests

adRequest = {

 transaction_id: generateMultipleIds(), // FRAUD INDICATOR

 timestamp: Date.now(),

 bundle_id: legitimate_id, // NOT SPOOFED

 sdk_version: "11.5.3",

 device_id: consistent_value

}
```

7. **Timing Signatures**:
    - Sub-millisecond request generation
    - Parallel network connections exceeding device capabilities
    - Synchronized timestamps across different ad networks

**Key Finding: No Bundle ID Spoofing Detected**

**Important Discovery**: Despite monitoring for spoofing of the identified target bundle IDs (particularly com.fooducate.fooducateNutritionApp and others), we found:

1. **No False Identity Claims**: None of the tested applications claimed to be any of the target bundle IDs
2. **Correct Bundle ID Reporting**: All applications correctly reported their actual bundle identifiers in network requests
3. **No Hijacking Attempts**: No evidence of apps attempting to steal ad revenue by impersonating the target applications

However, significant ad fraud was discovered through other mechanisms, as detailed in the following sections.

**Third-Party Tracking Detection at Scale**

**Proposed JavaScript/Pixel Implementation:**

javascript

```
// Fraud Detection Pixel
(function() {
  var fraudDetector = {
    sessionId: generateSessionId(),
    requestCount: {},
    timeWindow: 1000, // 1 second
    threshold: 5,

    init: function() {
      this.interceptRequests();
      this.monitorPatterns();
    },

    interceptRequests: function() {
      // Monitor all ad network calls
      var networks = [
        'amazon-adsystem.com',
        'applvn.com',
        'appsflyer.com'
      ];
```

```
  // Track request velocity
  networks.forEach(function(network) {
    fraudDetector.trackDomain(network);
  });
},

detectMultiplication: function() {
  // Flag multiple transaction IDs
  if (this.getUniqueTransactionIds() > 3) {
    this.flagFraud('request_multiplication');
  }
},

checkVelocity: function() {
  // Detect impossible request rates
  var requests = this.getRequestsInWindow();
  if (requests > this.threshold) {
    this.flagFraud('velocity_abuse');
  }
},

flagFraud: function(type) {
  // Send to fraud detection endpoint
  var beacon = new Image();
  beacon.src = 'https://fraud-detection.example.com/flag?' +
```

# iOS Ad Fraud Investigation Report

by Gokul Sathiyamurthy

```
      'type=' + type +
      '&session=' + this.sessionId +
      '&timestamp=' + Date.now();
    }
  };

  fraudDetector.init();
})();
```

**Scale Detection Signals:**

1. **Request Velocity Monitoring**:
    - Track requests per second to known ad endpoints
    - Flag when threshold exceeds human interaction limits
2. **Transaction ID Deduplication**:
    - Hash and store transaction IDs in 5-minute windows
    - Alert on duplicates or patterns
3. **Cross-Network Correlation**:
    - Implement shared session tracking
    - Detect simultaneous hits to multiple networks
4. **Behavioral Fingerprinting**:
    - Build profiles of legitimate app behavior
    - Flag statistical anomalies in real-time
5. **SDK Version Tracking**:
    - Monitor reported SDK versions
    - Flag mismatches or impossible combinations

**Conclusion**

# iOS Ad Fraud Investigation Report

by Gokul Sathiyamurthy

While bundle ID spoofing was not detected through our investigation, sophisticated ad fraud through request multiplication and multi-network coordination was identified. The fraud operates by maintaining legitimate app identities while manipulating the volume and timing of ad requests. The provided detection mechanisms can identify these patterns at scale through JavaScript or pixel-based tracking implementations.