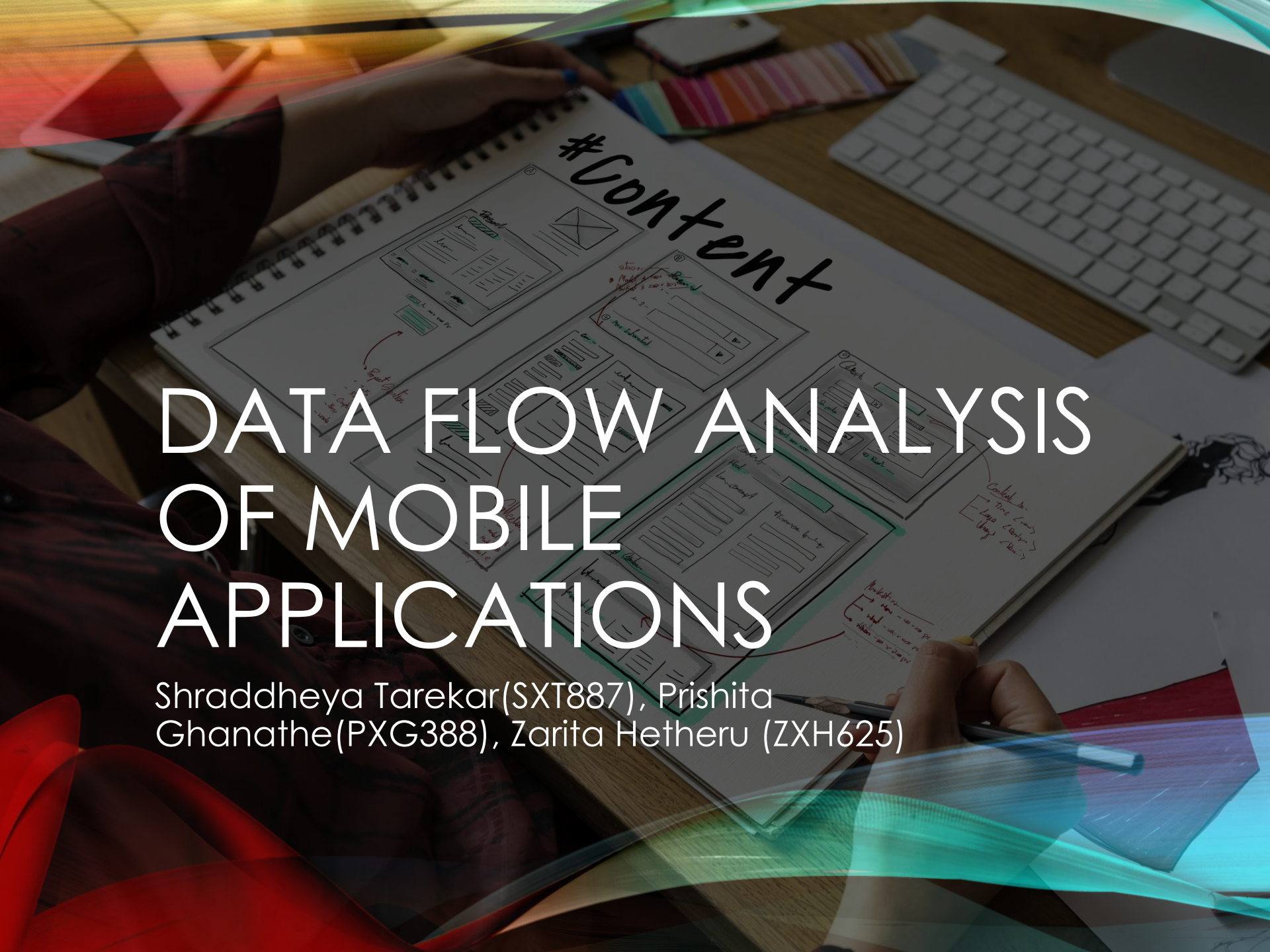


DATA FLOW ANALYSIS OF MOBILE APPLICATIONS

Shraddheya Tarekar(SXT887), Prishita Ghanathe(PXG388), Zarita Hetheru (ZXH625)

PROJECT OVERVIEW

Goal: Analyze how mobile apps handle user data (PII, geolocation), involvement of third party.

Tools Used: Burp Suite, Android Emulator.

Tested 33 apps from weather, fitness, travel, and utility categories.

Focused on observing data transmissions and privacy policy adherence.

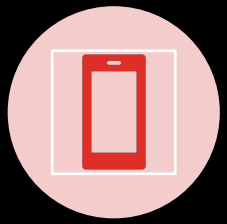
PROBLEM STATEMENT

Many apps transmit sensitive data without proper user consent.

Data sharing practices often hidden or vaguely mentioned in privacy policies.

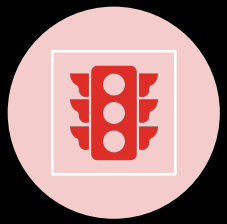
Challenges user trust and regulatory compliance (GDPR, CCPA).

TOOL DEMONSTRATION - BURP SUITE



Intercept mobile app traffic via proxy setup.

Captured sensitive data: geolocation, UUIDs, media uploads, and tokens.



Filtered traffic using endpoints, parameters (e.g., lat/lon, IDFA).

Inspected headers like x-goog-ext, authorization tokens, and data payloads.

Demo of the Burp Suite in Action

- Used Burp Suite as a proxy to intercept HTTPS traffic.
- Installed Burp Certificate for SSL decryption.

Captured sensitive transmissions using heuristics like:

- Exact GPS coordinates (e.g., WeatherBug, Transit)
- Emails and session tokens (e.g., Reddit, DeepSeek)
- WiFi SSID & UUIDs (e.g., WiFi Finder, DeepSeek)
- OAuth tokens giving access to Gmail (e.g., Calculator)
- Identified unknown trackers by analyzing domain names and payloads.

Request

Pretty Raw Hex

```
POST /v1/issuetoken HTTP/2
Host: oauthaccountmanager.googleapis.com
Accept: */*
Content-Type: application/x-www-form-urlencoded
Content-Length: 555
Accept-Language: en-US,en;q=0.9
X-Oauth-Client-Id: 278930400967-s7eptfh2d81vvi86kptt63pfa0o5usjt.apps.googleusercontent.com
User-Agent: com.google.photos/7.24.0 iSL/3.4 iPhone/18.3.2 hw/iPhone17_1 (gzip)
Authorization: Bearer
1//04eV2RKQb1hJ9CgYIARAAGAQSNwF-L9Ir8vVlZGrOecKXIxvfJBI3dUc1i6m2ZofRFi3rK9yejrS65h2bAhHBDmzr78Mr
fN3ymA8
Accept-Encoding: gzip, deflate, br

app_id=com.google.photos&client_id=
278930400967-s7eptfh2d81vvi86kptt63pfa0o5usjt.apps.googleusercontent.com&device_id=
B4E980A2-6714-4A88-99CF-FB202E80D057&hl=en-US&lib_ver=3.4&response_type=token&scope=
https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fphotos%20https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fpho
tos.native%20https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fmobileapps.native%20https%3A%2F%2Fwww.goo
gleapis.com%2Fauth%2Fnotifications%20https%3A%2F%2Fwww.googleapis.com%2Fauth%2Faccount_settings_
mobile%20https%3A%2F%2Fwww.googleapis.com%2Fauth%2Fsupportcontent
```

Response

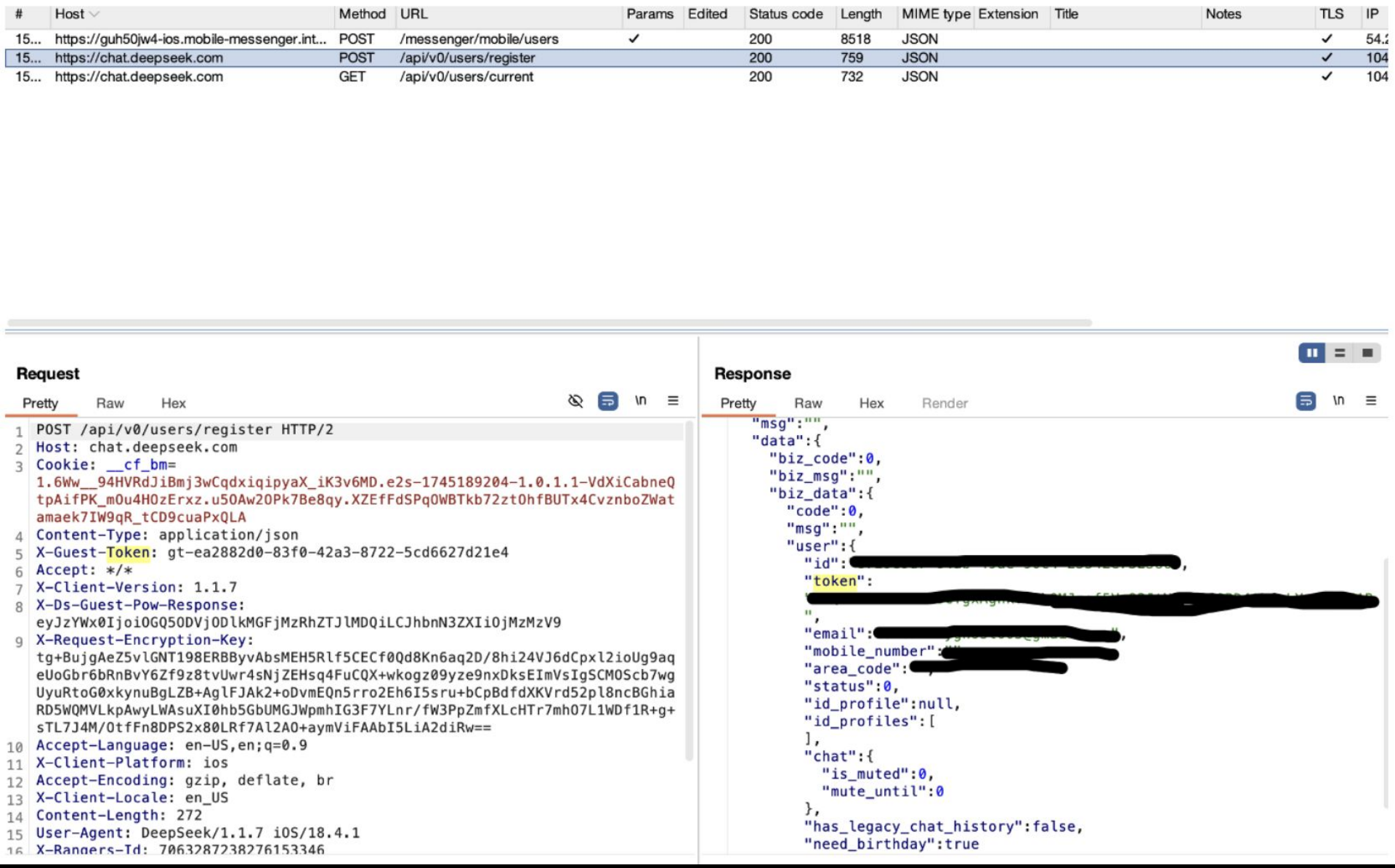
Pretty Raw Hex Render

```
HTTP/2 200 OK
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Date: Sun, 20 Apr 2025 08:20:42 GMT
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Content-Type: application/json; charset=UTF-8
Vary: Origin
Vary: X-Origin
Vary: Referer
Server: ESF
Content-Length: 764
X-Xss-Protection: 0
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

{
  "issueAdvice":"auto",
  "token":
  [redacted]
  At1Ru25tx42hw0345",
  "expiresIn":"3599",
  "grantedScopes":
  "https://www.googleapis.com/auth/photos.native https://www.googleapis.com/auth/photos https://
  www.googleapis.com/auth/mobileapps.native https://www.googleapis.com/auth/notifications https:
  //www.googleapis.com/auth/supportcontent https://www.googleapis.com/auth/account_settings_mobi
  le"
}
```

```
Ü´
thread-f:1829901097105283731º´
msg-f:1829901097105283731  ´
shraddheya8@gmail.com"teamsplunk@splunk.com*+Boost your skills with free Splunk
training2¿°Ù  Í  É  <u></u>
```

Calculator and transit app had token data leak and got access to the emails in the Gmail app.



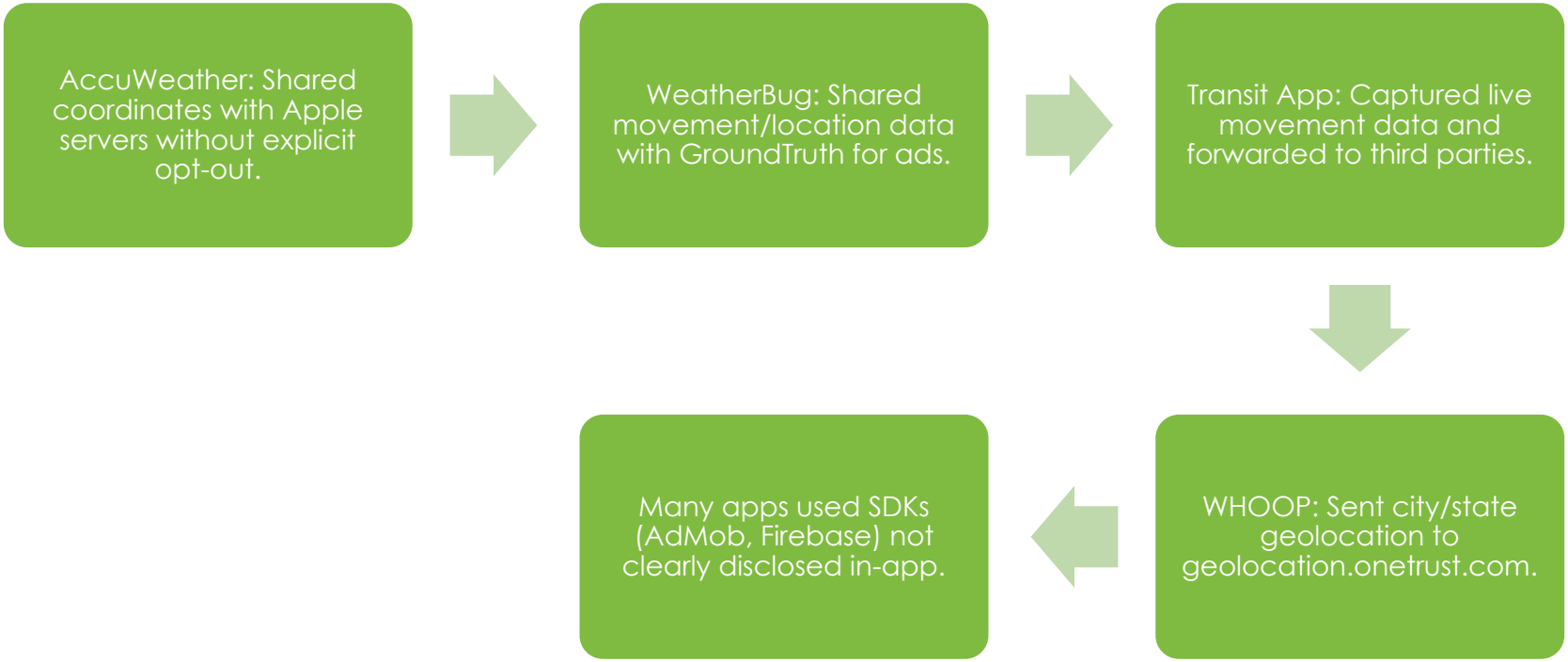
DeepSeek was tracing token,email, mobile number

```
Host: events.mapbox.com
Accept: */*
Content-Type: application/json
Content-Length: 356
Accept-Language: en-US,en;q=0.9
User-Agent: com.aws.weatherbug.pro/5.105.0/70 mapbox-maps-ios/6.3.0
X-Mapbox-Agent: WeatherBug/5.105.0 (com.aws.weatherbug.pro; v70; iOS 18.3.2; arm64e)
Mapbox/6.3.0 (com.mapbox.Mapbox; v15278) MapboxMobileEvents/0.10.5
(com.mapbox.MapboxMobileEvents; v10)
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

[
  {
    "enabled.telemetry":false,
    "sdkIdentifier":"mapbox-maps-ios",
    "event":"appUserTurnstile",
    "operatingSystem":"iOS 18.3.2",
    "userId":"[redacted]",
    "skuId":"00",
    "locationEnabled":true,
    "locationAuthorization":"whenInUse",
    "created":"2025-04-19T23:58:31.873+0000",
    "device":"iPhone17,1",
    "sdkVersion":"6.3.0",
    "accuracyAuthorization":"full"
  }
]
```

Weatherbug was sending details to the Third party without users consent.

INTERESTING FINDINGS



HOW WE FOUND ISSUES USING BURP SUITE

- We used Burp Suite to intercept and analyze network traffic from 33 Android applications.
- Here's how we identified the issues:

1. Installed the app on a test device with Burp Suite set as the proxy.
2. Monitored HTTP/S requests and responses.
3. Looked for transmission of sensitive information like:
   - Location coordinates (latitude/longitude)
   - Unique identifiers (GUID, Android ID)
   - Personally Identifiable Information (PII)
4. Noted any suspicious or unauthorized transmissions to third-party servers.
5. Matched findings with the app’s privacy policy to assess policy compliance.
6. Identified third-party analytics and advertising SDKs not mentioned explicitly.

Challenges & Solutions

Challenges:

1. Connectivity issues to Burp Suite using Android devices and emulators.
2. WiFi stability issues
3. Finding apps that were not pinning CA

Solutions:

1. BurpSuite needed to be altered to work properly with Android. Then the CA was able to connect.
2. WiFi could be reconnected but must first be “forgotten.”
3. Broadened our search criteria for apps while remaining within the scope.

RISK ASSESSMENT

High Risk: Apps transmitting exact geolocation or PII without consent.

Moderate Risk: Usage of advertising identifiers and analytics SDKs.

Low Risk: Apps with transparent policy and proper opt-in/opt-out controls.

Opaque privacy policies increase user exposure to data misuse.

TEAM CONTRIBUTIONS

- Shraddheya, Zarita, and Prishita each tested 10 mobile applications using Burp Suite.
- Each member identified potential privacy issues, third-party data sharing, and tracking behaviors in their respective apps.
- Findings were documented and validated against app privacy policies.
- Collaboration included comparative analysis and cross-verification of results.
- Final report and presentation prepared jointly, integrating individual findings.

ADDITIONAL FINDINGS BY TEAM MEMBERS

Zarita's Findings:

- Identified multiple apps transmitting PII such as email addresses and phone numbers to third-party domains.
- Discovered that some apps retained device identifiers (like IMEI) even after permissions were revoked.
- Noted the lack of encryption during transmission of sensitive analytics data in certain fitness tracking apps.

ADDITIONAL FINDINGS BY TEAM MEMBERS

Prishita's Findings:

- Observed apps requesting location access even when not essential for app functionality.
- Captured WiFi SSID and device UUIDs being transmitted silently in apps like DeepSeek and WiFi Finder.
- Noted privacy policies were vague or failed to mention third-party services, making it hard for users to understand data flow.

ADDITIONAL FINDINGS

Shraddheya's Findings:

- Apps sending coordinates to third-party services without clear disclosure.
- Apps were using the google OAuth token and getting access to the email under the Gmail app.
- Media files being accessed and uploaded to cloud services like Google Photos without explicit user consent.
- GUIDs and device-level identifiers being shared in traffic without clear permissions from users.

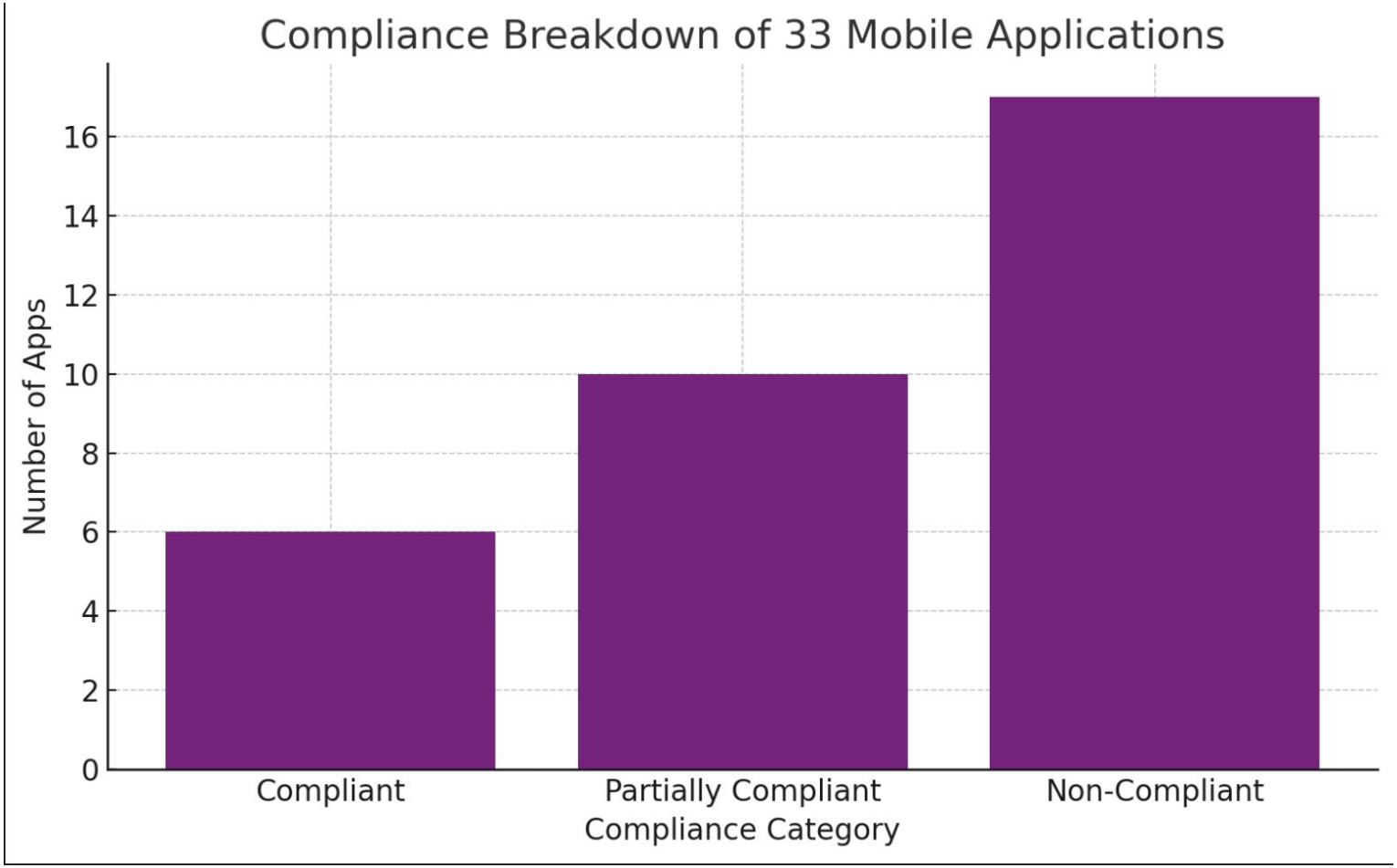
OUTCOME AND KEY LEARNINGS

- Identified gaps between stated privacy policies and actual behavior.
- Developed a repeatable method to analyze app traffic behavior.
- Recommendations for better transparency and consent handling.
- Raised user awareness about hidden data collection practices.

Top Non-Compliant Apps: What They Leaked

App	Data Leaked	Risk Level	Why it's critical
DeepSeek	Email, Token, SSID, IP	Very High	Enables tracking, session hijack
Turing Machine	Google auth token	Very High	Can compromise identity
Calculator	Gmail token, media access	High	No user consent
Reddit	Email, session ID	High	No opt-out control
TokenTransit	Phone, Location, Email, name	High	No separate opt-in

Compliance Breakdown: 33 Apps



CONCLUSION

- Sensitive data is often shared without adequate user knowledge.
- Burp Suite and proxy tools can effectively uncover such flows.
- Transparency and compliance are critical for data security.
- This methodology can be used for further research or audits.

THANK YOU