

# Atelier vie privée, intimité, appareil Android et les SDK

## Type de documentation

Cette page est une documentation en forme d'explication.

Vous pouvez partager vos connaissances en l'améliorant ([comment ?](#)).

**Cette page est axée sur la compréhension, explique, fournit des renseignements généraux et le contexte. Elle est comparable à un article sur l'histoire sociale de la tomate ou l'histoire sociale culinaire.**


Exemple : [Le wiki de communs](#)

Répertoire : [Les explications](#) dans ce wiki

Support : Le [portail dédié](#) à la documentation et aux codes sources

2020/11/27 15:59 · xavcc

### **Pourquoi :**

Un téléphone  [fr:Android](#) peut transmettre des informations très intimes à google et facebook.

Lors de cet atelier nous allons démontrer et donner à voir comment google et facebook peuvent connaître la situation et santé, voir l'état médicale d'une personne

## Objectifs

- Donner à voir un état des lieux
- Partager et discuter les moyens de comprendre
- Permettre d'expliquer par soi-même par la suite
- Offrir la possibilité éventuelle de reproduire par soi-même la manipulation
- Apprendre à se protéger & aider d'autre à se protéger

## Matériel nécessaire

- Un téléphone portable fonctionnant avec Android
- Un ordinateur Linux
- Un câble USB pour connecter le téléphone et l'ordinateur
- Installer [mitmproxy](#), ou plus pointu [PiRogue sur un raspberry Pi](#)
- 1 heure ou 2 heures de temps libre pour débiter

depuis Android version 7, pour regarder le comportement des requêtes https des applications (mitmproxy)

Vous aurez probablement besoin de recompiler l'apk de l'application visée avec une exception grâce à <https://github.com/levyitay/AddSecurityExceptionAndroid>

ISSUE [mitmproxy](#) est toujours en active depuis 2017  
<https://github.com/mitmproxy/mitmproxy>

## Explications

Un appareil Android contient un Android Advertising Identifier (IDFA) qui est un identifiant unique et spécifique à l'appareil que vous portez sur vous. Il est un sorte de racine de votre appareil. c'est un identifiant « pour affiner votre profil de publicité » qui est transmit dans de très nombreuses requêtes vers des serveurs qui stockent et compile, et croisent, des informations.

Ce n'est pas une question de données / de « data » qui fonde notre démarche. C'est une question de méthode, de stratégie et de conception d'une enquête.

*« Dans l'espace numérique, une donnée ne signifie rien en soi, elle traduit, elle trahit des choses.*

*Lorsque nous croisons une donnée avec une autre donnée, nous produisons un savoir qui n'est pas le savoir de la donnée elle-même. Nous déduisons, par exemple, des relations sociales, un comportement politique, alors qu'ils ne sont pas dans les données elles-mêmes. »*

*Olivier Ertzscheid, 2020, Enseignant-chercheur (Maître de Conférences) en Sciences de l'information et de la communication.*

Des software développement Kit (SDK) sont posés en dessous ou en dessus des applications Android, lors de leurs créations, installées sur l'appareil. Ces SDK sont argumentés comme étant une aide pour faciliter la création d'une application. Ils sont des serrures de développement qui collecte des données pour les envoyer sur un serveur de l'entreprise qui fournit et maintient ces SDK, qui sont bien souvent des boîtes sombres. L'une des raisons de leur utilisation est la baisse des coûts de production d'un application mobile. Il existe plus 9000 SDK Adnroid listés via github.

Les SDK sont

- Une délégation de pouvoir de la technique à des tiers
- Une opportunité de monétisation des informations collectées par les tiers
- Des moyens d'agir en « pisteurs » via des autorisations


Les autorisations que demandent des logiciels (type application pour appareil Android) pour avoir accès à des fonctionnalités de l'appareil pour ensuite les transmettre à un ou des tiers :

- Niveau de batterie
- langue utilisée
- géolocalisation
- type de connexion (Bluetooth, wifi, etc.)
- type de machine utilisées et lesquelles interagissent ensemble (votre téléphone avec tels spots de connexion dans un bar par exemple)
- réglage de la machine
- 1ère ou énième connexion à tel service ou tel site web
- le produit de soin et d'hygiène que vous avez cherché via telle appli ou telle autre
- etc...

De nombreux SDK profitent de ces autorisations pour collecter des informations et aident à établir des profils et des comportements des individus en transmettant ces informations contenant votre IFDA au passage.

Sur un téléphone sans application Facebook, il y a possibilité de « shadow profiling », constitution de profil sur des personnes qui n'ont pas compte Facebook à partir des données collectées depuis les SDK dépendants de Facebook.

On peut montrer ici et maintenant que cette collecte contient nom, prénom, âge, genre, statut sérologique, grossesse ou pas, nom de l'enfant, information de santé et médicale de l'enfant.

Une analyse de ce que collecte ces bouts de codes, de comment cela se lie avec votre Android Advertising Identifier (IFDA identifiant unique), pour comprendre la collecte de données plus ou moins intrusives et plus ou moins légitime, que nous ferons ensuite avec l'aide du logiciel mitmproxy nous fournira la base de discussion sur des enjeux de biopouvoir et de  [biopolitique](#).

« Il n'y a pas de données, il n'y a que des obtenues » Bruno Latour

## Mettre en place votre installation d'investigation

### MITMPROXY

cette possibilité <3 d'enregistrer les sessions mitmproxy, par exemple sur des applis mobiles,

```
# mitmproxy -w session_apptruc-YY-MM-DD.out
```

Puis de lire ensuite tranquillement quand tu veux

```
# mitmproxy -r session_appruc-YY-MM-DD.out
```

# Ressources externes

## Outils de travail

- [exodus CLI client for local APK static analysis.](#)
- [Apkcli](#) Command line tool gathering information on APKs based on androguard.
- [ApkTool](#)
- [APKID](#)

## Biblioweb

- Améliorer son hygiène numérique  
<https://blog.dreads-unlock.fr/ameliorer-son-hygiene-numerique-sur-android/>
- Comment installer et utiliser ADB + sauvegarde d'appareil  
<https://blog.dreads-unlock.fr/installer-adb/>
- Désinstaller les appli système  
<https://blog.dreads-unlock.fr/ameliorer-hygiene-numerique-android-desinstaller-applications-sys teme/>
- Et si besoin d'automatiser car plusieurs appareils à gérer, (merci Bristow\_69)c'est ici  
<https://www.frayssinet.org/2019/08/27/nettoyer-android-avec-adb/>
- Guide : Identifier des signes de la présence d'un logiciel espion sur Android  
<https://echap.eu.org/ressources/guides/guide-identifier-des-signes-de-la-presence-dun-logiciel-e spion-sur-android/>
- Nettoyer Android sans être root <https://www.dadall.info/article657/nettoyer-android>
- Quitter Android (produit google) pour LineageOS sur un téléphone Motorola  
<https://no-google.frama.wiki/libre:installer-lineage-motorola>
- POURQUOI SÉCURISER ET MAÎTRISER LES COLLECTES DE DATAS SUR MOBILE - Esther ONFROY Vidéo de conférence (2018) <https://invidious.kavin.rocks/watch?v=o55Ap9EW8XA>
- EntréeLibre, Metal\_Pou : [Exodus Privacy, analyseur d'applications smartphone](#)
- QCSuper: a tool for capturing your 2G/3G/4G air traffic using rooted Qualcomm-based Android phone. and produce a PCAP analyzable using Wireshark and more.  
<https://labs.p1sec.com/2019/07/09/pres>
- ufluns: Easy to use APK/IPA Mobile App Inspector (experimental)  
<https://github.com/wargio/fufluns>

[Vie privée](#), [numérique](#), [InfoSec](#), [Ateliers](#)

From:

<https://wiki.kaouenn-noz.fr/> - **Kaouenn-noz**

Permanent link:

[https://wiki.kaouenn-noz.fr/ateliers:android\\_sdk\\_vie\\_privée](https://wiki.kaouenn-noz.fr/ateliers:android_sdk_vie_privée)

Last update: **2021/05/28 13:35**

