• Les informations générées dynamiquement ne peuvent être récupérée parune analyse statique
• Certaines méthodes d'obfuscation sont difficiles à déchiffrer.Cependant, étant donné qu'au sein de l'application, ces valeurs vont êtredéchiffrées, on peut essayer de la récupérer à ce moment
• Certaines requêtes ne peuvent être déciffrée par un MITM,on peut alors essayer de lire les données de la requête au moment de l'envoieou de la réception de la requête

Emulateur : plus de facilité pour le rooter ainsi qu'installer Xposed

Root, Xposed :
Inspeckage :Démarrer des activités non déclarées, Désactiver le SSL, remplacer des paramètres d'application...**Android Device Monitor :** Outil intégré à Android Studiooffrant des fonctions de débug et d'analyse d'application

Débugger : Permet de faire mettre des breakpointsCependant, étant donné qu'on a pas accès au code source,il est nécessaire de décompiler l'application en smali,reconstruire le projet et recompiler l'application
Mémoire : Permet de récupérer certaines valeurs

L'analyse dynamique

Intérêt :

- Obtenir des informations générées dynamiquement par l'application
- Difficulté de déchiffre des strings lourdement obfusqués
- Requêtes qui ne peuvent pas être interprétées par un MITM

Environnemnt utilisé :

- Émulateur : Genymotion
- Root, Xposed
- Inspeckage
- Android Device Monitor

Utilisation :

- Utilisation d'un débugger
- Analyse de la mémoire utilisée par l'application

centralelille
ÉCOLE CENTRALE DE LILLE

Principe :• On décompile l'APK, mais on reste au stade du smali
• On importe les fichiers dans Android Studio pour y générer un nouveau projet• On place les points d'arrêts• On lance l'application• On analyse l'état de la mémoire de l'application aux points d'arrêtsEnfin, si on souhaite produire une version modifiée de l'application, il est possible de recompilerle smali pour produire un nouveau APK

L'analyse dynamique : Debugger

Principe

1. Décompilation de l'application
2. Import du projet dans Android Studio
3. Mise en place des points d'arrêts
4. Lancement du mode debug
5. Analyse de l'état de l'application aux points d'arrêts

- Il est par la suite possible de recompiler l'application avec les modifications apportés au smali