

Lab 04

Cybersecurity 3

Analyse Forensique Mobile (alternative à Magnet AXIOM)

Objectifs

- Charger et analyser un backup Android ou iOS
- Identifier messages, photos, données GPS
- Extraire les métadonnées et éléments exploitables
- Générer un rapport d'investigation

Remarque sur Magnet AXIOM et Docker

Magnet AXIOM n'est pas disponible dans Docker, car :

- Il fonctionne uniquement sur Windows avec GUI.
- Il nécessite une licence (même en démo).
- Il repose sur des drivers et une interface graphique propriétaire.

Solution alternative Docker-compatible

On utilise ici :

- [MobSF](#) (Mobile Security Framework) pour l'examen de l'APK si présent
- [ALEAPP](#) (Android Logs Events And Protobuf Parser) pour l'analyse des backups Android
- [iLEAPP](#) pour iOS
- Container Docker Python avec interface CLI ou Jupyter pour explorer les fichiers

Matériel

- Android_Backup.zip (fichier de simulation, à extraire dans ./data/)
 - Contient : messages WhatsApp, GPS history, images, bases SQLite
- Docker avec ALEAPP et outils d'analyse installés

Etape 1. Préparation

a. Dossier de travail

```
mkdir -p ~/mobile-lab/data  
cp Android_Backup.zip ~/mobile-lab/  
cd ~/mobile-lab  
unzip Android_Backup.zip -d ./data
```

b. Dockerfile (ALEAPP inside)

```
# Dockerfile  
FROM python:3.10-slim  
  
RUN pip install aleapp pillow jupyterlab  
  
WORKDIR /app  
VOLUME /data  
  
CMD ["bash"]
```

c. Build et lancement

```
docker build -t aleapp-lab .  
docker run -it -v $(pwd)/data:/data aleapp-lab bash
```

Etape 2. Charger et analyser le backup avec ALEAPP

```
cd /data  
mkdir output  
aleapp -t . -o output/
```

Résultat : un rapport HTML avec les artefacts extraits :

- Messages (ex : WhatsApp.db)
- Fichiers multimédia
- Historique de localisation
- Données de navigation, comptes, etc.

Etape 3. Investigation manuelle

Utilisation de sqlite3 ou Python pour fouiller :

```
sqlite3 WhatsApp.db
```

ou

```
strings *.db | grep -Ei "password|token|session"
```

EXIF :

```
exiftool /data/DCIM/*.jpg
```

GPS :

```
grep -r "lat\|long" .
```

Etape 4. Génération de rapport

a. Rapport ALEAPP

- Format : report.html ou report.xlsx généré automatiquement dans /data/output/
- Contenu : Liste de tous les artefacts parsés

b. Rapport manuel (à compléter par l'apprenant)

- Description des éléments trouvés
- Tableaux synthétiques des messages + coordonnées GPS
- Screenshots de l'environnement ou du rapport HTML

Livrables

Rapport complet (.pdf)

- Généré via ALEAPP ou Markdown transformé en PDF
- Contenu : Messages trouvés, GPS, métadonnées, images