

Lab 04 - Cybersecurity 3

Analyse Forensic Android

1. Mise en place

Le `docker-compose.yml` a été modifié pour répondre aux exigences du Lab04. Le fait qu'un APK soit mentionné mais non fourni indique un usage désiré de MobSF. On va déployer un lab complet des fois qu'on veuille creuser l'aspect "analyse statique d'un APK".

Le `Dockerfile` a été retravaillé également pour répondre aux besoins des étapes 3 (mentionnant sqlite3, et exiftool notamment). L'installation est légèrement plus lourde mais totalement complète.

2. Démarrage de la stack

Container CPU usage ⓘ 0.02% / 800% (8 CPUs available)					Container memory usage ⓘ 150.69MB / 15.25GB				
Q Search					Only show running containers				
☐	Name	Container ID	Image	Port(s)	CPU (%)	Memory usage/limit	Memory (%)	Disk read/write	
☐	mobile_lab	-	-	-	0.03%	150.69MB / 31.24GB	0.94%	13MB / 777MB	
☐	mobsf-analyzer	c4d4adf48547	opensecurity/mobile-securi	8000:8000 ↗	0.03%	149.5MB / 15.62GB	0.93%	13MB / 777MB	
☐	forensic-lab	86965ce71675	mobile_lab-forensic-lab	8888:8888 ↗	0%	1.19MB / 15.62GB	0.01%	0B / 0B	

Ensuite, il faut juste se connecter au conteneur `forensic-lab` pour avoir la stack installée tantôt par le `Dockerfile` :

```
(kali@GAWIN) - [/mnt/d/Users/Gawin/LiveCampus/Semaine_12/Jour_04/mobile_lab]
$ docker ps
CONTAINER ID   IMAGE                                     COMMAND                  CREATED
STATUS        PORTS          NAMES
c4d4adf48547   opensecurity/mobile-security-framework-mobsf:latest   "/home/mobsf/Mobile-..."   26 minutes ago
Up 26 minutes (healthy)   0.0.0.0:8000->8000/tcp, [::]:8000->8000/tcp   mobsf-analyzer
86965ce71675   mobile_lab-forensic-lab                  "bash"                   26 minutes ago
Up 26 minutes            0.0.0.0:8888->8888/tcp, [::]:8888->8888/tcp   forensic-lab

(kali@GAWIN) - [/mnt/d/Users/Gawin/LiveCampus/Semaine_12/Jour_04/mobile_lab]
$ docker exec -it forensic-lab bash
root@86965ce71675:/app# ls
root@86965ce71675:/app# pwd
/app
root@86965ce71675:/app# cd /data
root@86965ce71675:/data# ls
ALEAPP_Reports_2026-07-02_Thursday_162524  output
root@86965ce71675:/data#
```

3. Investigations

A. ALEAPP

Deux options s'offraient à moi : l'analyse du fichier ZIP ou du dossier inclus dedans. Le ZIP aurait été plus propre, mais le dossier plus rapide pour éviter une étape de décompression à la volée. Voici les commandes pour les deux, après que mon premier `Dockerfile` ait été amélioré pour que `aleapp` soit appelée comme une VRAIE application plutôt que comme un paquet Python secondaire :

```
# Analyse du dossier décompressé
aleapp -t fs -i /data -o /data/output

# Ou analyse directe du fichier ZIP
aleapp -t zip -i /data/L04-ALEAPP_Reports_2026-07-02_Thursday_162524.zip -o /data/output
```

Maintenant, on laisse mouliner :

```
root@711ddc40a31d:/data# aleapp -t fs -i /data -o /data/output
Mister Skinnylegs package not available, browser artifacts disabled: int() argument must be a string, a
bytes-like object or a real number, not 'auto'
Processing started. Please wait. This may take a few minutes...

-----
ALEAPP v2026.2.0: ALEAPP Logs, Events, and Protobuf Parser
Objective: Triage Android Full System Extractions.
By: Alexis Brignoni | @AlexisBrignoni | abrignoni.com
By: Yogesh Khatri | @SwiftForensics | swiftforensics.com

Building files listing...
File listing complete - 11388 files
Info: 640 modules loaded.
Artifact categories to parse: 640
File/Directory selected: /data
```

Je vois ce qu'il est en train de faire :

```
[159/641] get_fitbit_wearos_azm [fitbit] artifact started
No file found
get_fitbit_wearos_azm [fitbit] artifact completed

[160/641] get_fitbit_wearos_splits [fitbit] artifact started
No file found
get_fitbit_wearos_splits [fitbit] artifact completed

[161/641] get_fitbit_wearos_opaque_hr [fitbit] artifact started
No file found
get_fitbit_wearos_opaque_hr [fitbit] artifact completed

[162/641] get_smyfiles_OpHistory [smyfilesOpHistory] artifact started
No file found
get_smyfiles_OpHistory [smyfilesOpHistory] artifact completed

[163/641] get_googlemapaudio [googlemapaudio] artifact started
```

L'opération dure pas mal de temps (une vingtaine de minutes) :

```
[641/641] accounts_ce_authtokens [accounts_ce] artifact started
Found 126 records for Authentication tokens
accounts_ce_authtokens [accounts_ce] artifact completed

Processes completed.
Processing time = 00:02:25
Processing time (wall)= 00:21:57

Report generation started.
Report generation Completed.

Report location: /data/output/ALEAPP_Output_2026-08-06_Thursday_090704
root@711ddc40a31d:/data#
```

Rapport généré

Le rapport peut bien être lancé avec `index.html` généré dans le dossier `/data/output/`

ALEAPP 2026.2.0

Dark Switch

SAVED REPORTS

Report Home

ACCOUNTS

- Accounts ce
- Accounts de
- Authentication tokens

ANDROID BATTERY STATISTICS

- Android Battery Stats Daily

APP ROLES

- roles

APP SEMANTIC LOCATIONS

- ULR User Prefs

BLUETOOTH CONNECTIONS

- Bluetooth Adapter Information
- Bluetooth Connections

ALEAPP

Android Logs Events And Protobuf Parser

ALEAPP is an open source project that aims to parse every known Android artifact for the purpose of forensic analysis.

Case Information

Details | Device details | Script run log | Processed files list

Extraction location	/data
Extraction type	fs
Report directory	/data/output/ALEAPP_Output_2026-08-06_Thursday_090704
Processing time	00:21:57 (Total 1317.9423943499996 seconds)

All dates and times are in UTC unless noted otherwise!

[EXEMPLES] Comptes "ce"

Account Type	Account Name	Password
com.enflick.android.TextNow.account	TextNow	
com.facebook.messenger	Messenger	
com.garmin.di	GARMIN	1601603418327
com.google	thisisdfr@gmail.com	aas_et/AKppINbL_eEHMUv6Ghv5Jho1d35KM4nphq[...]
com.google.android.apps.tachyon	Duo	

Account Type	Account Name	Password
com.imo.android.imoous	imo HD	
com.opera.browser.ping	com.opera.browser	
com.reddit.account	Reddit for Android	
com.reddit.account	This_Is_DFIR	
com.silentcircle.account	thisisdfr	dummyPassword
com.skype.raider	Skype	
com.twitter.android.auth.login	TDfir	
com.viber.voip	+19195794674	143dc6b3879c80c88454776db7e2b33608c4634f
com.whatsapp	WhatsApp	
com.zhiliaapp.musically	TikTok	
org.telegram.messenger	858233690	
org.thoughtcrime.securesms	Signal	

Egalement, des "Comptes de", des jetons d'authentification, des statistiques d'appels, de connexion Bluetooth, de roles, de navigateurs, etc.

Total number of entries: 10

WhatsApp - Messages located at: ALEAPP_Reports_2026-07-02_Thursday_162524/com.whatsappbases/msgstore.db

Show entries Search:

Message Timestamp	Received Timestamp	Message ID	Recipients	Direction	Message	Group Sender
2020-09-23 14:09:03+00:00	2020-09-23 14:09:03+00:00	19198887386@s.whatsapp.net	19198887386@s.whatsapp.net	Outgoing		19198887386@s.whatsapp.net
2020-09-23 14:09:03+00:00	2020-09-23 14:09:03+00:00	19198887386@s.whatsapp.net	19198887386@s.whatsapp.net	Outgoing	On WhatsApp now.	19198887386@s.whatsapp.net
2020-09-23 14:10:04+00:00	2020-09-23 14:10:04+00:00	19198887386@s.whatsapp.net	19198887386@s.whatsapp.net	Incoming	I'm here, too.	19198887386@s.whatsapp.net
2020-09-23 14:17:11+00:00	2020-09-23 14:17:11+00:00	19198887386@s.whatsapp.net	19198887386@s.whatsapp.net	Outgoing		19198887386@s.whatsapp.net
2020-09-23 14:18:17+00:00	2020-09-23 14:18:18+00:00	19198887386@s.whatsapp.net	19198887386@s.whatsapp.net	Incoming		19198887386@s.whatsapp.net

Files By Google - Files Master report

Parses the master files list from the Files by Google application

Total number of entries: 4

Files By Google - Files Master located at: See source file(s) below

Show

15

entries

Search:

Date Modified	Root Path	Root Relative Path	File Name	Size	Mime Type	Media Type
2020-09-11 23:09:46+00:00	/storage/emulated/0	Download/magisk_patched.img	magisk_patched.img	32665600	application/octet-stream	App/Data
2020-09-11 23:09:46+00:00	/storage/emulated/0	Download/magisk_patched.img	magisk_patched.img	32665600	application/octet-stream	App/Data
2020-09-13 01:38:17+00:00	/storage/emulated/0	Notifications/viber_message.mp3	viber_message.mp3	40174	audio/mpeg	Audio
2020-09-13 01:38:17+00:00	/storage/emulated/0	Notifications/viber_message.mp3	viber_message.mp3	40174	audio/mpeg	Audio
Date Modified	Root Path	Root Relative Path	File Name	Size	Mime Type	Media Type

Google Maps Directions report

Parse Google Maps GMM directions (gmm_storage.db)

Total number of entries: 4

Google Maps Directions located at: ALEAPP_Reports_2026-07-02_Thursday_162524/user/0/com.google.android.apps.mapsbases/gmm_storage.db

Show

15

entries

Search:

Directions URL

https://google.com/maps/dir/35.6538337z,-78.824423/35.6607118,-78.8791983/data=!4m8!4m7!1m1!4e1!1m0!2m2!6e0!7e2!3e0;

https://google.com/maps/dir/35.6538337z,-78.824423/35.6607118,-78.8791983/data=!4m8!4m7!1m1!4e1!1m0!2m2!6e0!7e2!3e0;

https://google.com/maps/dir/35.660723z,-78.8790275/The+Club+at+12+Oaks,+2004+Green+Oaks+Pkwy,+Holly+Springs,+NC+27540/data=!4m13!4m12!78.8766247!2d35.671686799999996!2m2!6e0!7e

https://google.com/maps/dir/35.660723z,-78.8790275/The+Club+at+12+Oaks,+2004+Green+Oaks+Pkwy,+Holly+Springs,+NC+27540/data=!4m13!4m12!78.8766247!2d35.671686799999996!2m2!6e0!7e

Directions URL

B. MANUEL avec SQLite3

Je lance une investigation avec SQLite3, en retrouvant la bonne archive .db selon le contenu de _lava_data.lava qui donne bien le détail.

```
cd output/ALEAPP_Output_2026-08-06_Thursday_090704/data/

sqlite3 ALEAPP_Reports_2026-07-02_Thursday_162524/com.whatsappbases/msgstore.db
```

```
root@711ddc40a31d:/data# cd output/ALEAPP_Output_2026-08-06_Thursday_090704/data/
root@711ddc40a31d:/data/output/ALEAPP_Output_2026-08-06_Thursday_090704/data# sqlite3 ALEAPP_Reports_2026-07-02_Thursday_162524/com.whatsappbases/msgstore.db
SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite>
```

Je demande un formatage préalable :

```
.headers on
.mode column
```

Et je commence les extractions :

Les messages

```
sqlite> SELECT
  _id,
  from_me,
  text_data AS message,
  datetime(timestamp / 1000, 'unixepoch') AS date_heure
FROM available_message_view
WHERE text_data IS NOT NULL
ORDER BY timestamp DESC
LIMIT 20;
```

_id	from_me	message	date_heure
11	0		2020-10-03 22:48:37
10	1		2020-10-03 22:45:17
9	1		2020-10-03 22:44:32
8	1		2020-10-03 22:43:57
7	0		2020-10-03 22:42:40
6	0		2020-09-23 14:18:17
5	1		2020-09-23 14:17:11
4	0		2020-09-23 14:10:04
2	1		2020-09-23 14:09:03
3	1		2020-09-23 14:09:03

Les appels

```
sqlite> SELECT
  cl._id,
  j.raw_string AS contact,
  cl.from_me AS appel_emission,
  cl.video_call AS appel_video,
  cl.duration AS duree_secondes,
```

```

datetime(cl.timestamp / 1000, 'unixepoch') AS date_heure
FROM call_log cl
LEFT JOIN jid j ON cl.jid_row_id = j._id
ORDER BY cl.timestamp DESC;

```

_id	contact	appel_emission	appel_video	duree_secondes	date_heure
4	19198887386@s.whatsapp.net	0	1	122	2020-09-23 14:27:02
3	19198887386@s.whatsapp.net	1	1	92	2020-09-23 14:24:11
2	19198887386@s.whatsapp.net	0	0	91	2020-09-23 14:22:10
1	19198887386@s.whatsapp.net	1	0	107	2020-09-23 14:19:29

Les géolocalisations

```

sqlite> SELECT
    ml.message_row_id,
    j.raw_string AS contact,
    ml.latitude,
    ml.longitude,
    datetime(m.timestamp / 1000, 'unixepoch') AS date_heure
FROM message_location ml
JOIN message m ON ml.message_row_id = m._id
JOIN chat c ON m.chat_row_id = c._id
JOIN jid j ON c.jid_row_id = j._id;

```

Les contacts

```

sqlite> SELECT
    _id,
    user,
    server,
    raw_string
FROM jid
WHERE server = 's.whatsapp.net' OR server = 'g.us'
LIMIT 30;

```

_id	user	server	raw_string
2	19198887386	s.whatsapp.net	19198887386@s.whatsapp.net
3	19198887386	s.whatsapp.net	19198887386.0:0@s.whatsapp.net

C. MANUEL avec Exiftool

Je me mets dans le dossier racine `output/` pour itérer un exiftool, qui contient déjà une option pour le GPS. Pour aller "plus vite" et surtout faire quelque chose de récursif avec une sortie exploitable proprement, je travaille un peu ma commande :

```
# Pour une extraction générale
exiftool -r -ext jpg -csv /data > /data/output/exif_resultats.csv

# Pour répondre à des critères Forensics un peu plus avancés, en inscrivant
# les données GPS en degrés à 6 décimales, ce qui est requis en Forensic
# à la place des traditionnels Degrés-Minutes-Secondes
exiftool -r -ext jpg -csv -c "%.6f" \
  -FileName -Directory -CreateDate -ModifyDate -Make -Model -GPSLatitude -GPSLongitude -
GPSAltitude \
  /data > /data/output/exif_gps_filtre.csv
```

Le rapport généré est... grand.

```
^Croot@711ddc40a31d:/data/output# exiftool -r -ext jpg -csv -c "%.6f" \
  -FileName -Directory -CreateDate -ModifyDate -Make -Model -GPSLatitude -GPSLongitude -GPSAltitude \
  /data > /data/output/exif_gps_filtre.csv
1261 directories scanned
6100 image files read
root@711ddc40a31d:/data/output#
```

Je peux user de la CLI, mais je décide de charger le CSV dans un tableur classique et d'afficher uniquement des lignes non-vides :

	D	E	F	G	H	I	J	K	L	M
	CreateDate	ModifyDate	Make	Model	GPSLatitude	GPSLongitude	GPSAltitude			
1										
2										
3	2020:03:22 09:31:03	2020:03:22 09:31:03								
4	2020:08:20 21:22:09	2020:08:20 21:22:09	samsung	SM-A305G						
5										
6	2020:03:22 09:40:14	2020:03:22 09:40:14								
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										

FileName	Directory	CreateDate	ModifyDate	Make	Model	GPSLatitude	GPSLongitude	GPSAltitude
2110668f5161f4ce2a964ea2ee8c15299bfa18.jpg	/data/ALEAPP_Reports_2026-07-02_Thursday_162524/media	2017-11-02 20:42:35	2018-09-13 15:09:72	Apple	iPhone X	34,025817 N	118,401567 W	33.9 m Above Sea Level
be65795becb78385e80a3de2f5ba70d6677452a8.jpg	/data/ALEAPP_Reports_2026-07-02_Thursday_162524/media	2020-10-01 00:26:08	2020-10-01 00:26:08	Apple	iPhone 11 Pro Max	28,508631 N	80,604408 W	2 m Above Sea Level
2110668f5161f4ce2a964ea2ee8c15299bfa18.jpg	/data/ALEAPP_Reports_2026-07-02_Thursday_162524/HTML/media	2017-11-02 20:42:35	2018-09-13 15:09:72	Apple	iPhone X	34,025817 N	118,401567 W	33.9 m Above Sea Level
be65795becb78385e80a3de2f5ba70d6677452a8.jpg	/data/ALEAPP_Reports_2026-07-02_Thursday_162524/HTML/media	2020-10-01 00:26:08	2020-10-01 00:26:08	Apple	iPhone 11 Pro Max	28,508631 N	80,604408 W	2 m Above Sea Level
2110668f5161f4ce2a964ea2ee8c15299bfa18.jpg	/data/output/ALEAPP_Output_2026-08-06_Thursday_090704/data/ALEAPP_Reports_2026-07-02_Thursday_162524/media	2017-11-02 20:42:35	2018-09-13 15:09:72	Apple	iPhone X	34,025817 N	118,401567 W	33.9 m Above Sea Level
be65795becb78385e80a3de2f5ba70d6677452a8.jpg	/data/output/ALEAPP_Output_2026-08-06_Thursday_090704/data/ALEAPP_Reports_2026-07-02_Thursday_162524/media	2020-10-01 00:26:08	2020-10-01 00:26:08	Apple	iPhone 11 Pro Max	28,508631 N	80,604408 W	2 m Above Sea Level
2110668f5161f4ce2a964ea2ee8c15299bfa18.jpg	/data/output/ALEAPP_Output_2026-08-06_Thursday_090704/data/ALEAPP_Reports_2026-07-02_Thursday_162524/HTML/media	2017-11-02 20:42:35	2018-09-13 15:09:72	Apple	iPhone X	34,025817 N	118,401567 W	33.9 m Above Sea Level
be65795becb78385e80a3de2f5ba70d6677452a8.jpg	/data/output/ALEAPP_Output_2026-08-06_Thursday_090704/data/ALEAPP_Reports_2026-07-02_Thursday_162524/HTML/media	2020-10-01 00:26:08	2020-10-01 00:26:08	Apple	iPhone 11 Pro Max	28,508631 N	80,604408 W	2 m Above Sea Level
53f8b36052ca9f65fd1b56a964e39b4f362e8a6.jpg	/data/output/ALEAPP_Output_2026-08-06_Thursday_090704/media	2017-11-02 20:42:35	2018-09-13 15:09:72	Apple	iPhone X	34,025817 N	118,401567 W	33.9 m Above Sea Level
82cf0863ecc0d0f1cc83261165f4b77016b8056.jpg	/data/output/ALEAPP_Output_2026-08-06_Thursday_090704/media	2020-10-01 00:26:08	2020-10-01 00:26:08	Apple	iPhone 11 Pro Max	28,508631 N	80,604408 W	2 m Above Sea Level
53f8b36052ca9f65fd1b56a964e39b4f362e8a6.jpg	/data/output/ALEAPP_Output_2026-08-06_Thursday_090704/HTML/media	2017-11-02 20:42:35	2018-09-13 15:09:72	Apple	iPhone X	34,025817 N	118,401567 W	33.9 m Above Sea Level
82cf0863ecc0d0f1cc83261165f4b77016b8056.jpg	/data/output/ALEAPP_Output_2026-08-06_Thursday_090704/HTML/media	2020-10-01 00:26:08	2020-10-01 00:26:08	Apple	iPhone 11 Pro Max	28,508631 N	80,604408 W	2 m Above Sea Level