Analysis process:

# Rip phone (Quick & FFS)

## Use one of the commercial tools

Image the device first with a quick scan and then a full file system rip.

Ensure the hardware is most up to date to have the most chance of success

Follow the tools individual set up requirements for successful processing of data

# Create iTunes Backup:

## Use ilibmobile package (Ubuntu)

The use of ilibmobiles idevicebackup2 to generate the iTunes backup is the proffered method. To do so ensure you are in the tools.venv python environment and follow the steps bellow:

1. Establish the trust between iPhone and the server by interfacing with the iPhone
2. Use the command idevice\_id to find the uuid of the device
3. Turn on encryption to make sure you get the most comprehensive backup and set password to admin

idevicebackup2 encyption on admin

1. Use the idevicebackup2 command like

idevicebackup2 -u <uuid> backup --full <dest>

1. From there, there should be a directory created with the name being the UUID of the device
2. Its good practice to turn encryption off once complete

idevicebackup2 encyption off admin

## Use iTunes for windows GUI

Sometimes versions of IOS and phone don’t comply and therefore we have alternate means with our analyst laptops to use iTunes that has been directly downloaded from apple website and not windows store

1. Start with plugging in and trusting the device
2. Sign into iTunes with the account of the device
3. You will find a little phone icon top left near the music button
4. From there if you are prompted to either “set up new iPhone” or “restore from backup” ensure to check the “set up new iPhone” options as this will register the phone to the laptop, it will not be used to wipe any data or anything.
5. Once the device is registered you will be able to access the summary section found on the left-hand side menu bar
6. Under the section “Backups” subsection “automatically back up” there will options for “this computer” and “encrypt local backup”; ensure to set password to “admin” for ease of use
7. If the backup does not automatically begin you can use the generate manual backup button in the same section
8. Backups are stored in C:\Users\[your username]\AppData\Roaming\Apple Computer\MobileSync\Backup

# Dump syslogs

## Use ilibmobile package (Ubuntu)

This method once again will be done on the server, and we need to be in the python environment tools.venv. then follow the steps bellow:

1. Use the idevicecrashreport command to dump all the logs to a directory

idevicecrashreport -u <uuid> -k <dest>

## Use MacOS

Dumping logs with macOS is easy utilising the log command. You can then use the command to analyse different parts/types of logs.

# Decrypt/check backup with mvt-ios

To decrypt backups is a two-step process and straight forward. The backups are all in UUID format upon initial creation, so they are you targets

Step 1 we need to perform a backup decrypt with the backup-decrypt command as show here

mvt-ios decrypt-backup -d <dest> </path/to/backup>

Step 2 we can check some of the data using check-backup

mvt-ios check-backup --output <dest> </path/to/backup>

# Process syslogs

Use a Mac OS Device to process the logs using the AUL\_Creator.sh script. It can output to log, json, jsonl.

Step 1 is to get your log files:

* /private/var/db/diagnostics
* /private/var/db/uuidtext
* /Library/Logs/Crashreporter/MobileDevice/<Device Name>/DiagnosticLogs/Sysdiagnose

# Ingest syslogs into SEIM

For this step it is only a matter of accessing the SIEM\_SVR through the url http://10.0.0.100:80 and load the jsonl files into the timesketch server through the web interface.

# Ingest logs into streamlit