User activity characterization using iOS forensic artifacts

Authors: Sebastien Kanj[a,b], Daniel López[a,b], Josep Pegueroles[a]
Contact: sebastien.kanj@upc.edu

(a) Incide Digital Data SL

(b) Universitat Politècnica de Catalunya

ABSTRACT

The identification of human usage hours of a mobile device plays a crucial role in certain legal cases, enabling the determination of the time of last usage or the user's activity during a specific period. This research consists of the identification of forensic artifacts within the iOS operating system related to the user's activity and discarding those that are related to background services. The result is a Python script that extracts data from an encrypted iOS backup and generates an output that is easily indexable and drawable.

INTRODUCTION

Our research aims to identify forensic artifacts within the iOS operating system to determine human usage hours of mobile devices and discard background activity, facilitating investigations in legal cases.

- Identifying relevant artifacts.
- Developing software for artifact parsing.
- Creating dynamic graphical representations for activity analysis.
- Extracting information on critical dates and anomalous activity.

ARTIFACTS

After identification [1] [2] [3], parsing, and review of iOS artifacts, the following are highlighted as useful for our investigation:

Application traces
– /Library/Logs/mobile installation helper.log.*
–/Library/com.apple.itunesstored/itunesstored2.sqlitedb
– /Library/CoreDuet/People/interactionC.db
– /Library/Databases/DataUsage.sqlite

Keyboard
– /Library/Keyboard/langlikelihood.dat

Activity throttling
–/Library/Preferences/com.apple.contextstored.plist
–/Library/Preferences/com.apple.coreduetd.plist

Disk usage
–/Library/Preferences/com.apple.Preferences.plist

Safari History
– /Library/Safari/History.db

User Created/Saved Photos
– /Media/DCIM/1*APPLE

This work has been made possible thanks to the funding from the Ministry of Science and Education with the Trusted Data Sharing (TDS) project and from the Generalitat de Catalunya with grant 2021 DI 92.

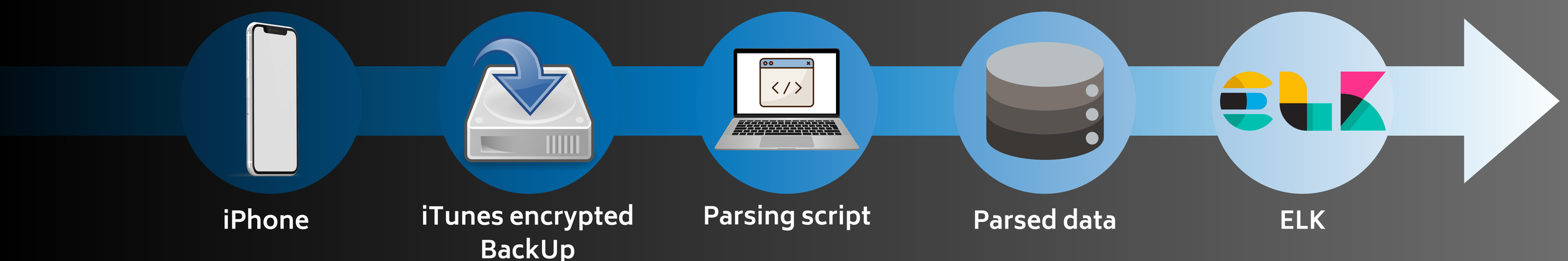
References:

[1] SANS Institute. (2023). iOS Third-Party Apps Forensics. https://sansorg.egnyte.com/dl/TeOraX38Od, [Accessed 02-03-2024]

[2] SANS Institute. (2023). DFIR Advanced Smartphone Forensics. https://www.sans.org/posters/dfir-advanced-smartphone-forensics/, [Accessed 02-03-2024]

[3] Casey, E., & Carvey, J. D. (2014). Mobile device forensics: A guide for law enforcement, second edition. Springer. [https://link.springer.com/book/10.1007/978-1-4842-8026-3]

ANALYSIS FLOW



USER DAILY ACTIVITY