2024 - PDR - 41F-7C7 - Forensics Analysis of Oura Ring Gen 3 on Android, iOS and Cloud - hu961@purdue.edu - Xiao Hu

CERIAS

The Center for Education and Research in Information Assurance and Security

Forensics Analysis of Oura Ring Gen 3 on Android, iOS and Cloud

Xiao Hu, Akif Ozer, Miloš Stanković and Umit Karabiyik

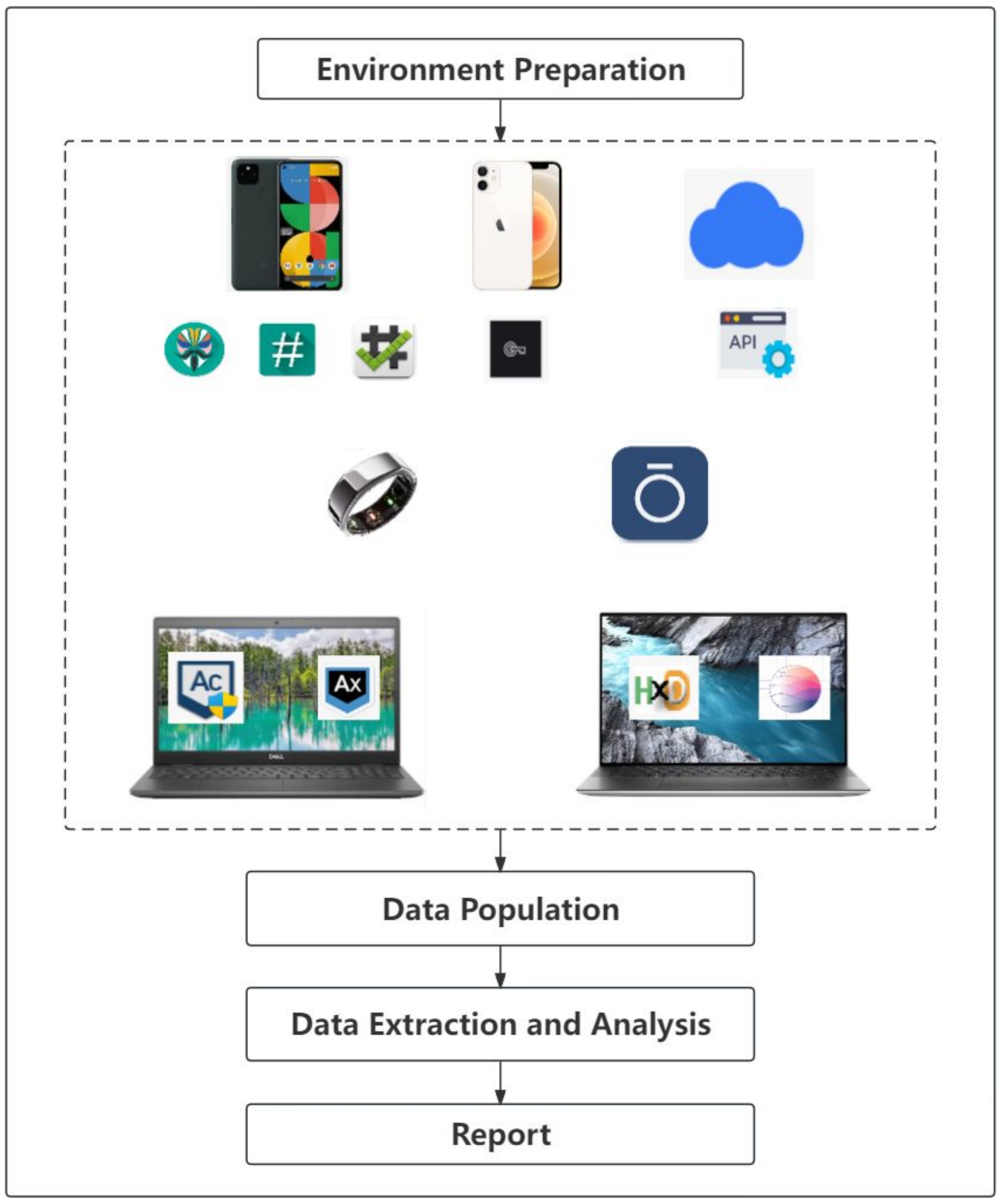
OVERVIEW

This research aims to examine smart rings, specifically the Oura Ring Generation 3 and its accompanying mobile application, from a digital forensics perspective. The study aims to identify the types of data that can be recovered from the device and address privacy and security concerns related to its use.

METHODOLOGY

For mobile devices, we used a Google Pixel 5a running Android 11 and an iPhone 12 with iOS 16.2.
Our methodology followed these phases:

- **Environment Preparation**: introduces the devices and software used, as well as preparatory steps.
- **Data Population**: consisted of three main activities: exercise, sleep, and normal operation. It was first performed on the Pixel 5a and then on the iPhone 12 at multiple day intervals.
- **Data Extraction and Analysis**: Under elevated privileges, the full image of the Pixel 5a was accomplished through Magnet ACQUIRE and AXIOM Process. The acquisition of iPhone 12 was acquired through Magnet AXIOM suite with GrayKey.


Environment Preparation

Data Population

Data Extraction and Analysis

Report

GOALS

The main goals of our project included:

1. Delivered a detailed analysis of the Ora Ring Generation 3 application called Oura on Android, iOS and Cloud

2. Created a script that is capable of gathering cloud information from Oura app across a time range

FINDINGS

- **Android:** forensically valuable information was found in the folder \data\data\com.ouraring.oura including the user's personal data, device data, and activity logs
  Key files: hke2ryGknzgNaHF86QuONBHuFuynvgUR\events.realm\timeseries.realm
- **iOS:** important data was stored under \private\var\mobile\Containers\Data\Application\98C8AAF8-673D-43B7-A899-F0E23ACDEB82 and other paths, including the user's workout information, sleep, heart rate records and so on.
  Key files: score-percentiles.csv\RMAdminStore-Local.sqlite\assa.sqlite\timeseries v2.sqlite
- **Cloud:** As long as user has active subscription OURA keeps user information in the cloud. This information can be accessed through OURA portal or with an authorization token the user information can be accessed through their API.
  Critical data found:
  - Daily Activity
  - Daily SpO2
  - Heart Rate
  - Rest Mode Periods
  - Session
  - Sleep Time
  - Workout
  - Daily Readiness
  - Daily Sleep
  - Personal Info
  - Ring Configuration
  - Sleep
  - Tags

CONCLUSION

- This research can be a great resource for future research on wearable technologies with mobile device connection and smart rings
- Future directions for this study include expanding the scope to examine interactions between the Oura app and third-party applications like Instagram, Snapchat, Amazon, and Google, as well as exploring advanced forensic techniques such as Man-in-the-Middle (MITM) attacks via Bluetooth, data recovery post-app deletion, and chip-off analysis, to further understand the privacy and security implications of wearable devices.

PURDUE UNIVERSITY

{hu961, ozer, mstankovic, umit}@purdue.edu