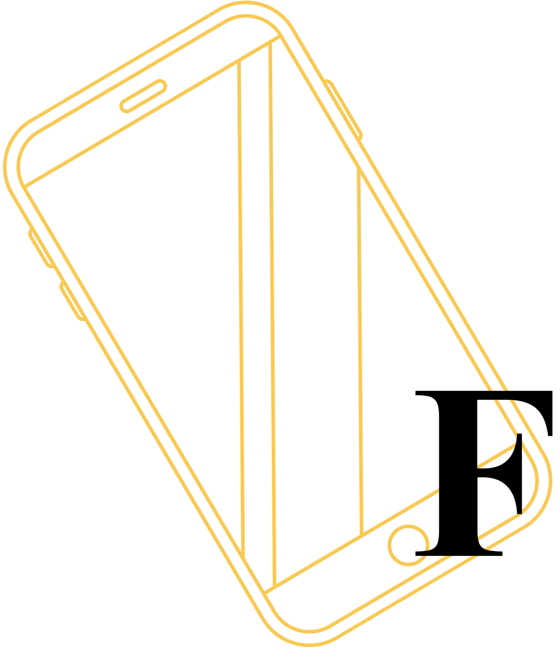
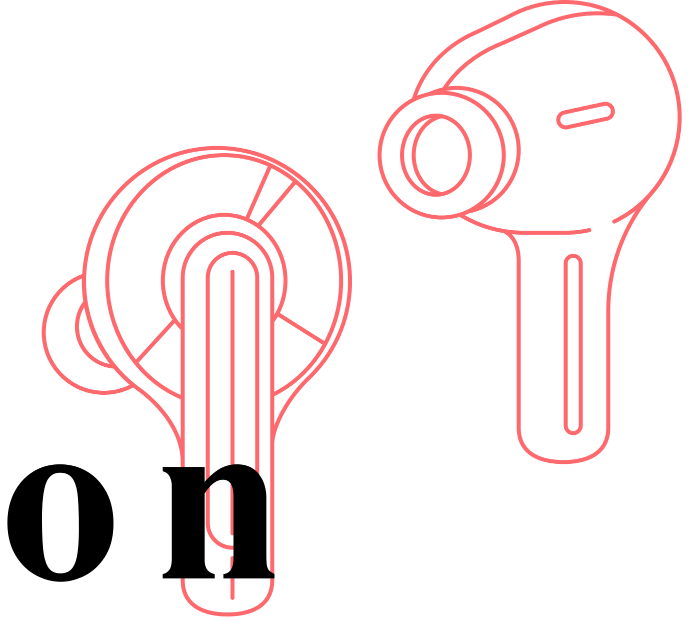
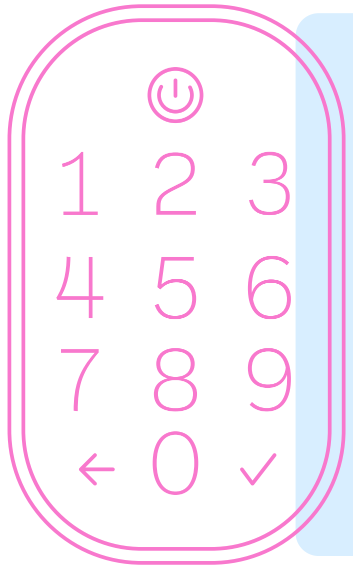
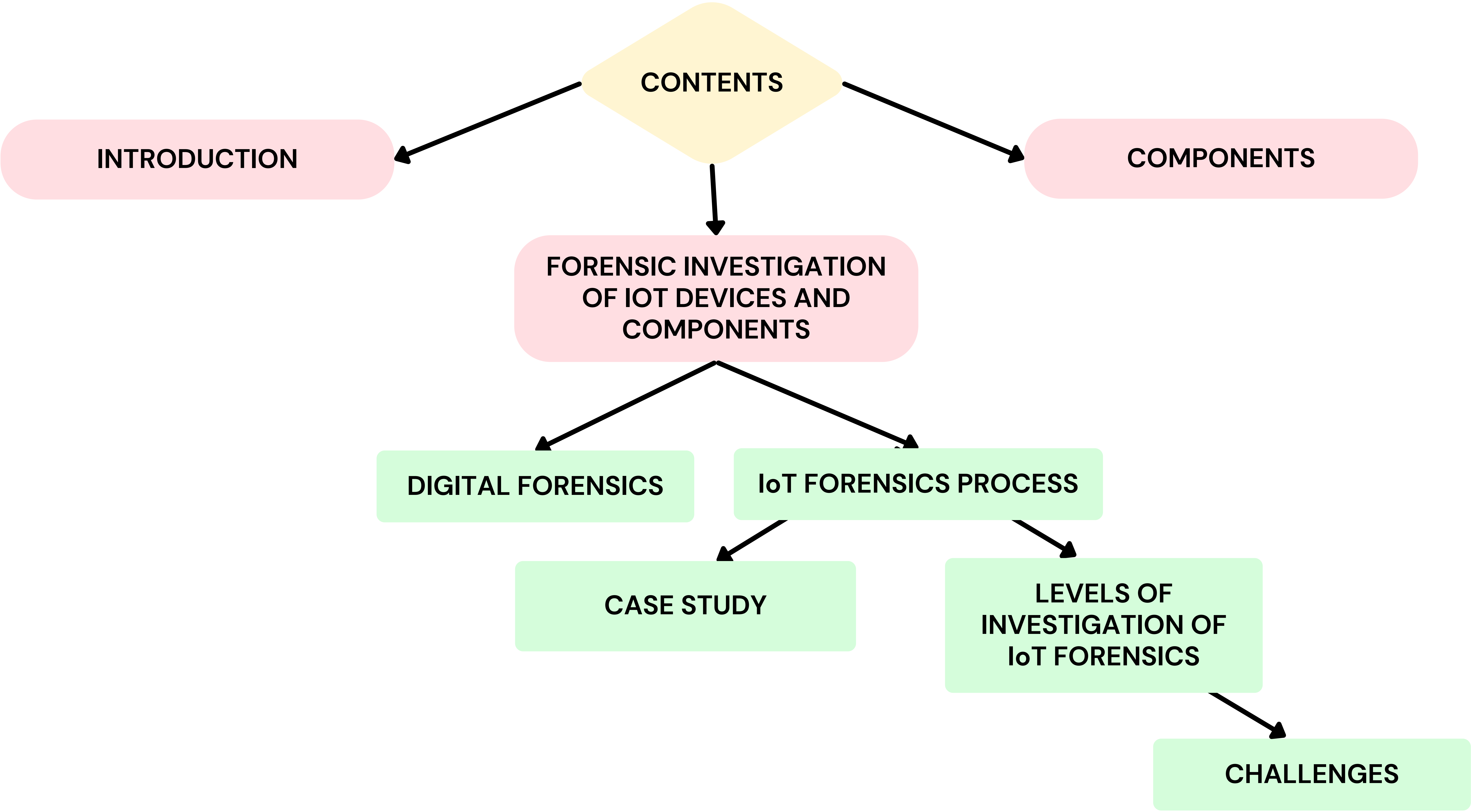




Forensic Investigation Of IoT Devices & Components



Name- Anouska Dutta
M.Sc. Digital Forensics and Information Security
Enrollment - 032200300003014



CONTENTS

INTRODUCTION

COMPONENTS

FORENSIC INVESTIGATION OF IOT DEVICES AND COMPONENTS

DIGITAL FORENSICS

IoT FORENSICS PROCESS

CASE STUDY

LEVELS OF INVESTIGATION OF IoT FORENSICS

CHALLENGES

What is IoT?

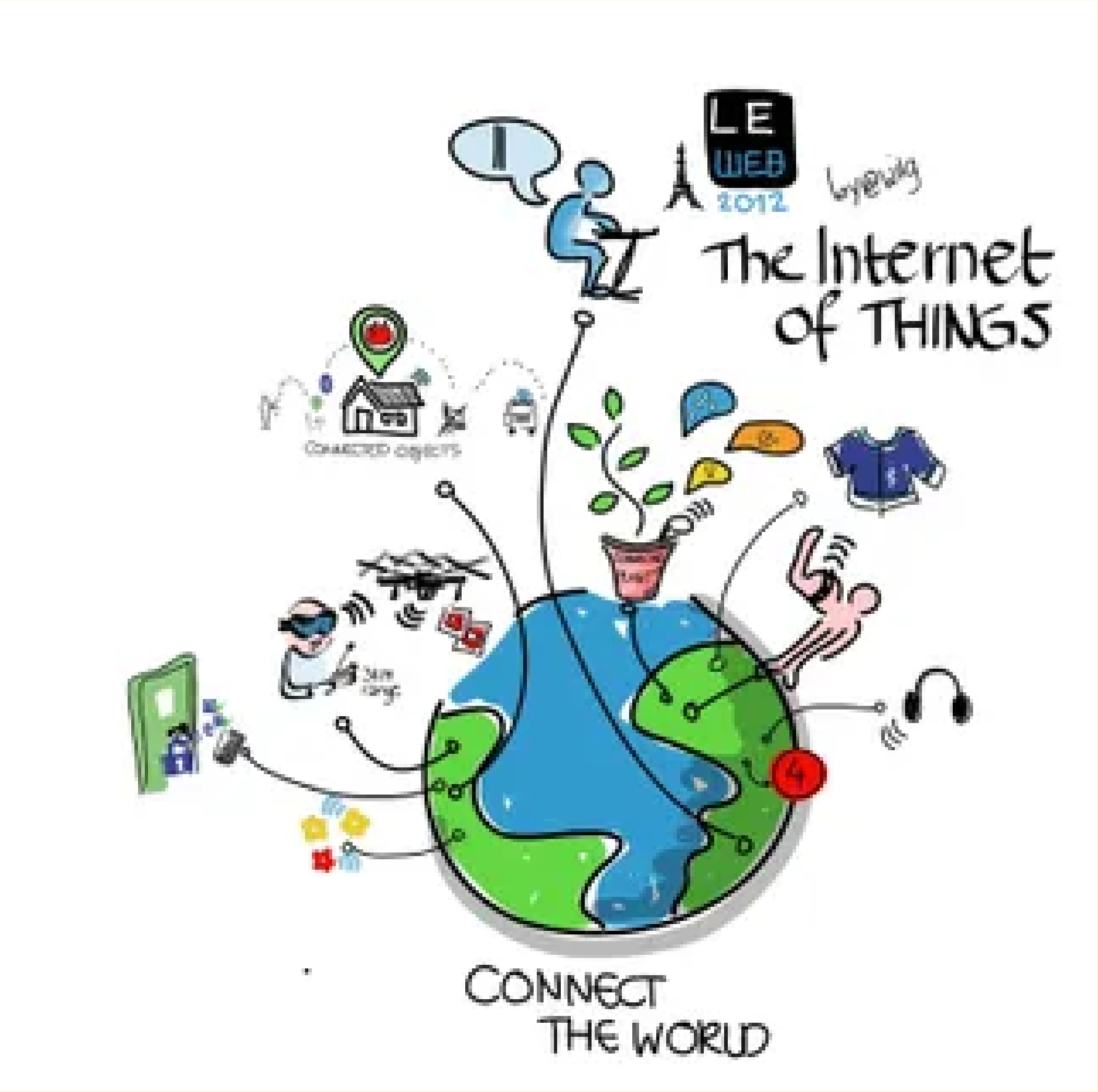
- The internet of things, or IoT, is a network of interrelated devices that connect and exchange data with other IoT devices and the cloud.
- IoT devices are typically embedded with technology such as sensors and software.
- With IoT, data is transferable over a network without requiring human-to-human or human-to-computer interactions.

Components of IoT

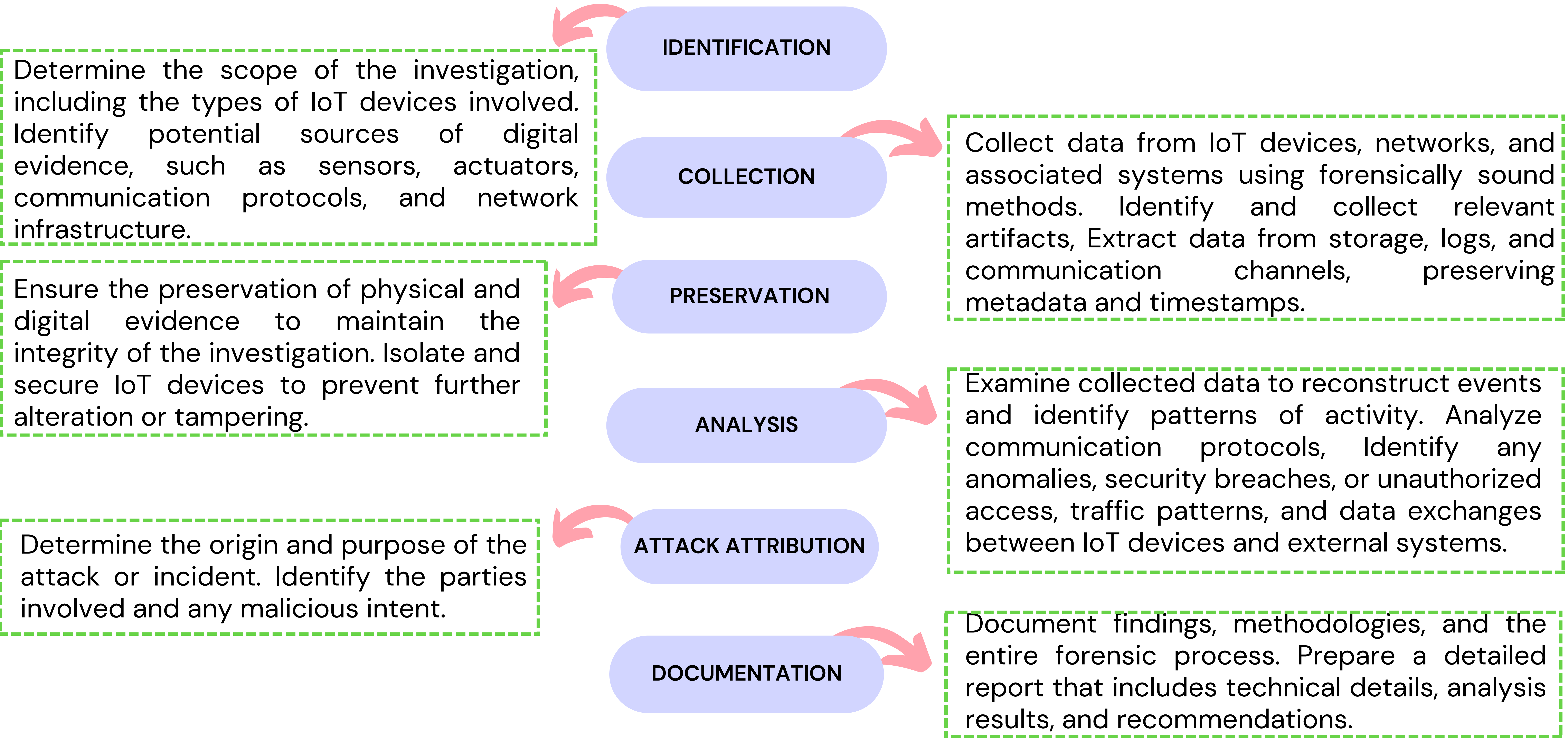
1. Thing Or Device
2. Gateway
3. Cloud
4. Analytics
5. User Interface

Digital Forensics

- Digital forensics deals with evidence in a digital form.
- Digital, or sometimes called electronic, evidence is easy to change.
- Every access to a file on a digital device (PC, smart phone, IoT device) changes the file’s last access time, and thus changes the file in a way that might constitute evidence. This is an example of a change that is neither malicious nor substantial but might be considered evidence tampering.



IoT Forensics Process



IDENTIFICATION

Determine the scope of the investigation, including the types of IoT devices involved. Identify potential sources of digital evidence, such as sensors, actuators, communication protocols, and network infrastructure.

COLLECTION

Collect data from IoT devices, networks, and associated systems using forensically sound methods. Identify and collect relevant artifacts, Extract data from storage, logs, and communication channels, preserving metadata and timestamps.

PRESERVATION

Ensure the preservation of physical and digital evidence to maintain the integrity of the investigation. Isolate and secure IoT devices to prevent further alteration or tampering.

ANALYSIS

Examine collected data to reconstruct events and identify patterns of activity. Analyze communication protocols, Identify any anomalies, security breaches, or unauthorized access, traffic patterns, and data exchanges between IoT devices and external systems.

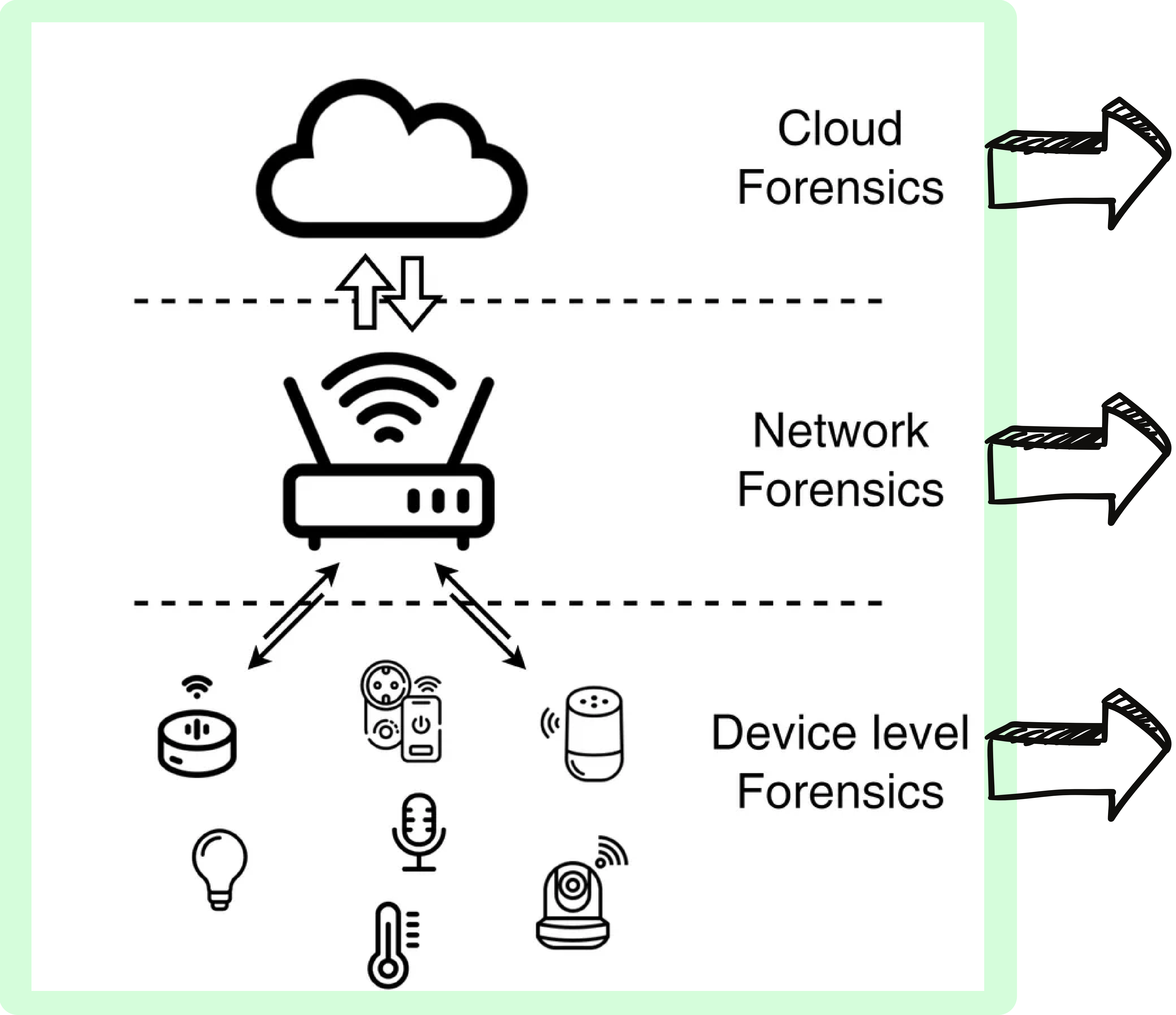
ATTACK ATTRIBUTION

Determine the origin and purpose of the attack or incident. Identify the parties involved and any malicious intent.

DOCUMENTATION

Document findings, methodologies, and the entire forensic process. Prepare a detailed report that includes technical details, analysis results, and recommendations.

Levels of Investigation in IoT Forensics



Cloud Forensics

Process of extrapolating information in the cloud used by the devices. Since IoT devices are usually limited in memory, most of the information is stored in proprietary cloud applications that may contain a massive amount of potential evidences. This includes analyzing logs, access records, and configurations stored in the cloud.

Network Forensics

Process of identifying and extracting evidence from network log, devices traffic traces and communication patterns. Analyzing the network traffic between IoT devices and other entities to identify communication patterns and anomalies. Capturing and analyzing the packets exchanged between devices to understand the nature of communication and identify any malicious activities.

Device level Forensics

Collecting data from the IoT devices involved in the incident. This includes extracting logs, configurations, and any relevant data stored on the devices.

Forensic Challenges

Distributed Data

The data could reside on a device or mobile phone, in the cloud or at a thirdparty's site. Therefore, the identification of the locations where evidence resides is a major challenge.

Digital Media Lifespan

Due to device storage limitations, the lifespans of data in Internet of Things devices are short; data items are overwritten easily and often.

Cloud Service Requirements

Cloud accounts are often associated with anonymous users because service providers do not require users to provide accurate information when signing up. This can make it impossible to identify criminal entities.

Lack of Security Mechanisms

Evidence in Internet of Things devices can be changed or deleted due to the lack of security mechanisms this could negatively affect the quality of evidence and even render it inadmissible in court.

Device Types

During the identification phase of forensics, an investigator needs to identify and acquire evidence at a digital crime scene.

Data Formats

The formats of data generated by Internet of Things devices do not match the formats of data saved in the cloud.

Smartwatch Forensics Case Study

Ref: Chapter 3 INTERNET OF THINGS FORENSICS – CHALLENGES AND A CASE STUDY Saad Alabdulsalam, Kevin Schaefer, Tahar Kechadi and Nhien-An LeKha

This section presents a case study involving an Internet of Things device, specifically an Apple smartwatch. A smartwatch is a digital wristwatch and a wearable computing device. A smartwatch is used like a smartphone and has similar functions. It shows the date and time, counts steps and provides various types of information, including news, weather reports, flight information, traffic updates. It can be used to send and receive text messages, email, social media messages, tweets, etc. Smartwatch connectivity plays an imporrole in the retrieval of information from the Internet. A full-featured smartwatch must have good connectivity to enable it to communicate with other devices (e.g., a smartphone) and it should also be able to work independently. The Apple Watch Series 2 used in the case study has the following technical specifications:

- Network-accessible smartwatch with no cellular connectivity.
- Dual-core Apple S2 chip.
- Non-removable, built-in rechargeable lithium-ion battery.
- WatchOS 2.3, WatchOS 3.0, upgradable to WatchOS 3.2.
- Wi-Fi 802.11 b/g/n 2.4 GHz, Bluetooth 4.0, built-in GPS, NFC chip, service port.
- AMOLED capacitive touchscreen, Force Touch, 272 × 340 pixels (38 mm), 312×390 pixels (42 mm), sapphire crystal or Ion-X glass.
- Sensors: Accelerometer, gyroscope, heartrate sensor, ambient light sensor.
- Messaging: iMessage, SMS (tethered), email.
- Sound: Vibration, ringtones, loudspeaker

Logical Acquisition

The following results related to the Apple Watch were obtained from the iPhone after multiple logical extractions were performed in order to clarify the attempts and changes. The database contained the UUID, name, address, resolved address, Last Seen Time and Last Connection Time. In the case Study, the Apple Watch was used with five applications: (i) Health app; (ii) Nike+ GPS app; (iii) Heartbeat app; (iv) Messages app; and (v)Maps app.

Manual Acquisition

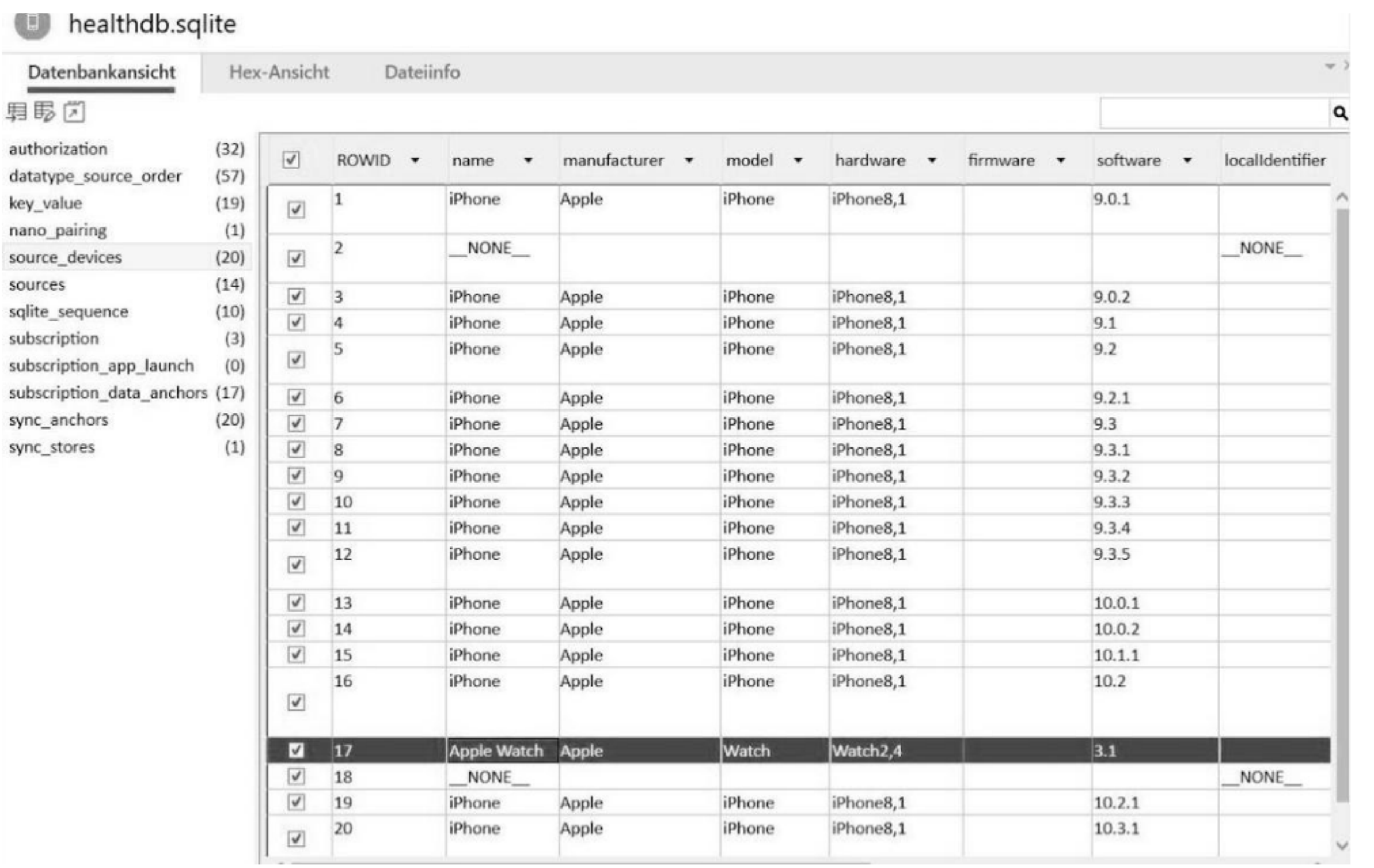
The manual acquisition involved swiping the Apple Watch to view and record the data displayed on the device screen. This method was used because no physical access to the Apple Watch was possible. The acquisition was intended to prove that the Apple Watch generated and stored data, and that it could be used as an independent device. Artifacts like i. Messages

ii. Pictures

iii. Apps

iv. Emails

v. Contacts and Phone



authorization	(32)
datatype_source_order	(57)
key_value	(19)
nano_pairing	(1)
source_devices	(20)
sources	(14)
sqlite_sequence	(10)
subscription	(3)
subscription_app_launch	(0)
subscription_data_anchors	(17)
sync_anchors	(20)
sync_stores	(1)

☑	ROWID	name	manufacturer	model	hardware	firmware	software	localIdentifier
☑	1	iPhone	Apple	iPhone	iPhone8,1		9.0.1	
☑	2	__NONE__						__NONE__
☑	3	iPhone	Apple	iPhone	iPhone8,1		9.0.2	
☑	4	iPhone	Apple	iPhone	iPhone8,1		9.1	
☑	5	iPhone	Apple	iPhone	iPhone8,1		9.2	
☑	6	iPhone	Apple	iPhone	iPhone8,1		9.2.1	
☑	7	iPhone	Apple	iPhone	iPhone8,1		9.3	
☑	8	iPhone	Apple	iPhone	iPhone8,1		9.3.1	
☑	9	iPhone	Apple	iPhone	iPhone8,1		9.3.2	
☑	10	iPhone	Apple	iPhone	iPhone8,1		9.3.3	
☑	11	iPhone	Apple	iPhone	iPhone8,1		9.3.4	
☑	12	iPhone	Apple	iPhone	iPhone8,1		9.3.5	
☑	13	iPhone	Apple	iPhone	iPhone8,1		10.0.1	
☑	14	iPhone	Apple	iPhone	iPhone8,1		10.0.2	
☑	15	iPhone	Apple	iPhone	iPhone8,1		10.1.1	
☑	16	iPhone	Apple	iPhone	iPhone8,1		10.2	
☑	17	Apple Watch	Apple	Watch	Watch2,4		3.1	
☑	18	__NONE__						__NONE__
☑	19	iPhone	Apple	iPhone	iPhone8,1		10.2.1	
☑	20	iPhone	Apple	iPhone	iPhone8,1		10.3.1	

Figure 1. Screenshot of the `healthdb.sqlite` database.

Since physical access to the Apple Watch was not possible,
a manual acquisition by swiping the screen is currently the only method for determining the artifacts stored on the Apple Watch.
However, logical and manual acquisitions can be performed only when the Apple Watch is not pin-locked.

Thank you!