IOT (Internet of Things)

Shaik Ghousal Mubarak

Internet of Things

- Internet of things (IOT) is a network of physical objects. The internet is not only a network of computers, but it has evolved into a network of device of all type and sizes , vehicles, smart phones, home appliances, toys, cameras, medical instruments and industrial systems, animals, people, buildings, all connected ,all communicating & sharing information based on stipulated protocols in order to achieve smart reorganizations, positioning, tracing, safe & control & even personal real time online monitoring , online upgrade, process control & administration.

Three C's of IoT

- Communication
- Control and Automation
- Cost Savings

IoT Advantages

- **Improved Customer Engagement**
- **Technology Optimization** – The same technologies and data which improve the customer experience also improve device use, and aid in more potent improvements to technology. IoT unlocks a world of critical functional and field data.

.

- **Reduced Waste** – IoT makes areas of improvement clear. Current analytics give us superficial insight, but IoT provides real-world information leading to more effective management of resources.
- **Enhanced Data Collection** – Modern data collection suffers from its limitations and its design for passive use. IoT breaks it out of those spaces, and places it exactly where humans really want to go to analyse our world. It allows an accurate picture of everything

IoT Disadvantages

- **Security** – IoT creates an ecosystem of constantly connected devices communicating over networks. The system offers little control despite any security measures. This leaves users exposed to various kinds of attackers.
- **Privacy** – The sophistication of IoT provides substantial personal data in extreme detail without the user's active participation.
- **Complexity** – Some find IoT systems complicated in terms of design, deployment, and maintenance given their use of multiple technologies and a large set of new enabling technologies.

- **Flexibility** – Many are concerned about the flexibility of an IoT system to integrate easily with another. They worry about finding themselves with several conflicting or locked systems.
- **Compliance** – IoT, like any other technology in the realm of business, must comply with regulations. Its complexity makes the issue of compliance seem incredibly challenging when many consider standard software compliance a battle

IOT Devices

Google Home Voice Controller

Google Home Voice Controller is a smart IoT device which allows the user to enjoy features like media, alarms, lights, control the volume

Amazon Alexa

Amazon Alexa is a popular and reliable IoT device. It is capable to run songs, do phone calls, setting timers and alarms, ask questions, providing information, checking the weather, managing to-do & shopping lists, managing house instruments, and several other things

Apple HomePod

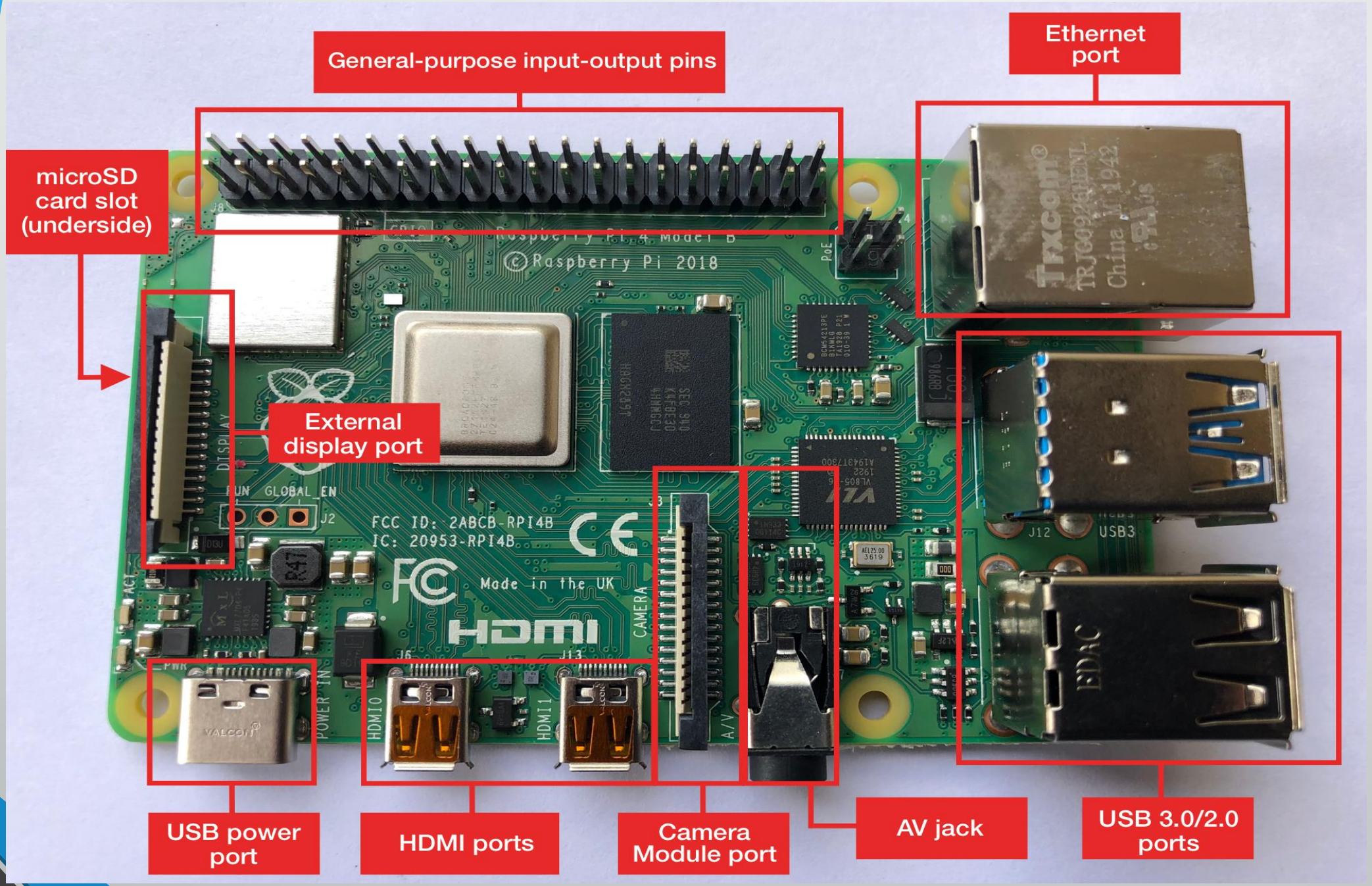
- Play any music you have bought from iTunes Music Store.
- Control your HomeKit gadgets.
- Make and receive phone calls.
- Read and reply to your Messages.
- Set timers and alarms.
- Let you know what the traffic will be like for your journey.
- Let you know what the weather will be like.
- Get local cinema times.
- Translate and Spelling.

Raspberry Pi

Raspberry Pi is the name of a series of single-board computers made by the Raspberry Pi Foundation, a UK charity that aims to educate people in computing and create easier access to computing education.

Raspberry Pi is a very cheap computer that runs Linux, but it also provides a set of GPIO (general purpose input/output) pins, allowing you to control electronic components for physical computing and explore the Internet of Things (IoT).

- h


General-purpose input-output pins
Ethernet port
microSD card slot (underside)
External display port
USB power port
HDMI ports
Camera Module port
AV jack
USB 3.0/2.0 ports
Raspberry Pi 2018
FCC ID: 2ABCB-RPI4B
IC: 20953-RPI4B
Made in the UK
HDMI
DISPLAY
CAMERA
A/V
POWER IN
HDMI0
HDMI1
USB3
PoE

Smart Watch

- Location
- VoIP Calls
- Bluetooth
- Socket Connection / Webhooks
- WIFI.
- Heart Rate
- Audio
- Text To Speech
- Smart Home IoT
- Timers for the watch
- Alarm Clock & Reminders

Case Studies

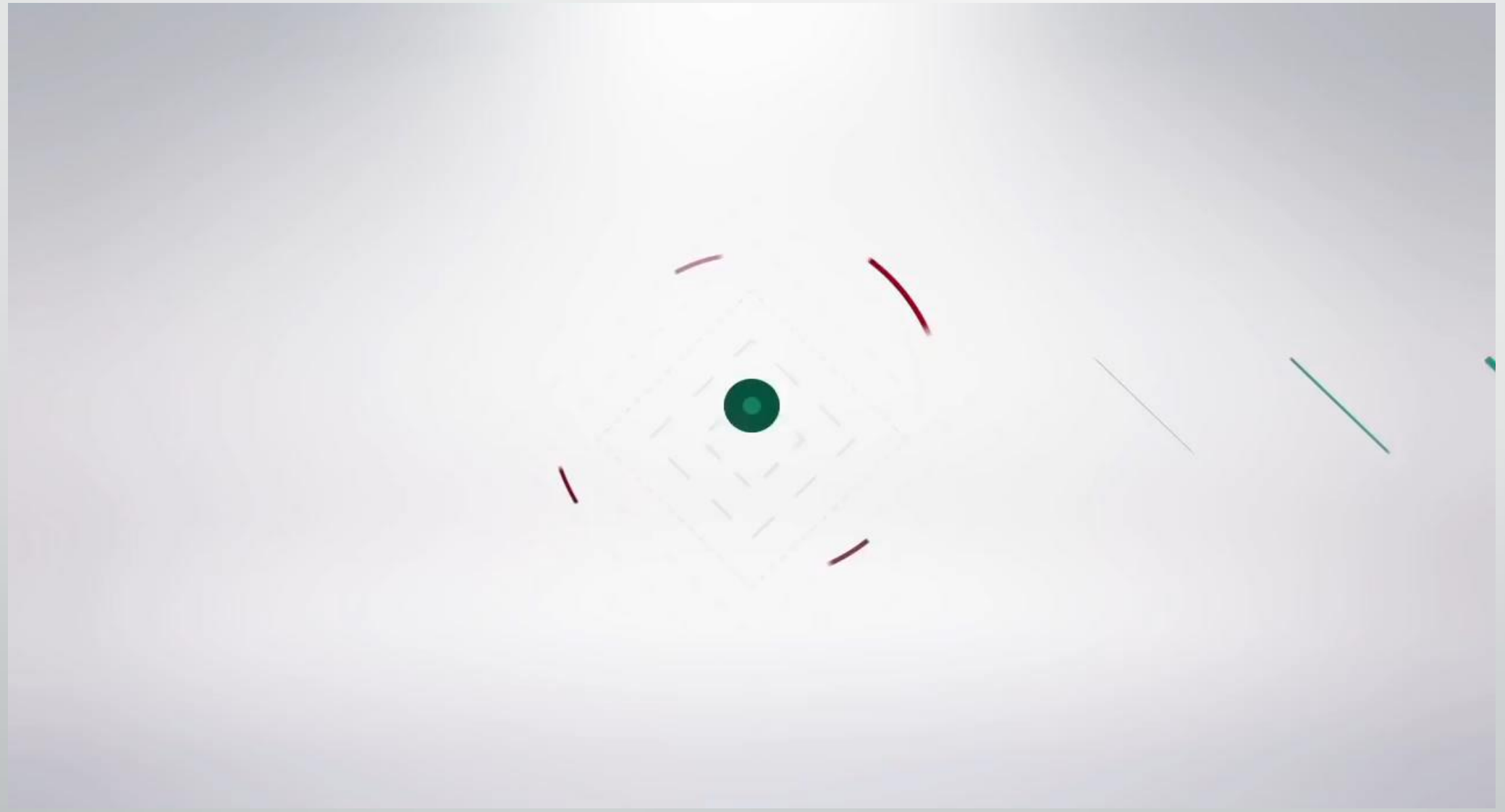
ATM Machine Hacked

Expert accused of hacking ATM machine servers using modern gadgets arrested by Delhi Police

Delhi police arrested an accused who hacked ATM machine servers using modern gadgets. The accused was traced by the records of a gas agency and had committed frauds worth crores of rupees.

Tanseem Haider
New Delhi
December 2, 2021 UPDATED: December 2, 2021 15:16 IST

Police recovered a Raspberry Pi Device, two ATM Card skimmer devices, two ATM hidden camera panels, one expired debit card, one Quantum Lan Adapter, four mobile phones and freezed amount of Rs 83,000 in the bank account.



In Connecticut Murder Case, a Fitbit Is a Silent Witness

BBC | Sign in | Home | News | Sport | Reel | Worklife | Travel | Future

NEWS

Home | War in Ukraine | Coronavirus | Climate | Video | World | Asia | UK | Business | Tech | Science

World | Africa | Australia | Europe | Latin America | Middle East | US & Canada

Fitbit contradicts husband's story of wife's murder - police

25 April 2017

Case briefacts

- In a case a person named Richard Dabate informed police that someone broke into his house and killed his wife, but **in the investigation electronic data collected by state police investigators, including the victim's Fitbit Data showed victim moving around the house last at 10:05 a.m., an hour after Richard Dabate said she was shot in the head by intruders, records show**.

- Smart, connected devices are becoming a valuable new source of evidence for law enforcement. But that’s just the tip of the iceberg when it comes to the Internet of Things (IoT).

Dieselgate scandal against Volkswagen

The Indian EXPRESS

Friday, March 25, 2022

Explained: What is the 'dieselgate scandal' against Volkswagen?

It was in 2015 that Volkswagen admitted to having installed emissions-cheating devices in its vehicles, which cost the company over $33 billion in vehicle refits and regulatory fines, mostly in the United States.

- All the cars passed their in-house testing, they were taken on the road-test between Los Angeles and San Francisco and it was observed that the results were significantly different from the results from their in-house testing.
- The cheating software was written to detect when the vehicles were being emissions tested and then turned down pollution control devices when not undergoing test.
- As a result, these cars passed emissions tests, but emitted up to 40 times more
- The cheating software is protected by the law from being openly reviewed andtested by a third party

Forensics

- Tools and techniques to recover, preserve and examine digital evidence on or transmitted by electronic devices

Classification of Cyber Forensics

- Disk forensics
- Network forensics
- Wireless forensics
- Database Forensics
- IOT Forensic
- Mobile device forensics
- GPS forensics
- E-mail Forensics
- Memory Forensics
- Malware Forensics

IOT Forensics

- IoT Forensics is an emerging field in Digital Forensics.

Sources of evidence on IoT

- Evidence collected from smart devices and sensors
- Evidence collected from the Network
- Evidence collected from the Cloud

Analysis can be done

Principles of analysis of IoT devices

- Evidence identification and collection
- Preservation
- Data analysis
- Presentation and reporting

Evidence Identification and collection

- An investigator needs to identify the affected IoT devices at the crime scene. Effective identification and collection of the evidence can increase the scope of the investigative process
- Evidence collection in the IoT environment can be challenging.
- When attempting to locate evidence, digital forensics professionals face considerable challenges. Even if the location is known, investigators may not be familiar with the types of IoT devices and the underpinning infrastructure.

Preservation

- The investigator should make sure that the evidence gathered from the IoT device is preserved properly. The device should not be switched off before gathering the evidence from it during the initial search. In this stage, the investigator requires specialized forensic tools to acquire data from the device's hardware and applications. The investigator can also create memory dumps to collect volatile data from the IoT device before it is turned off.

Data Analysis

- Data in an IoT device is mostly stored on a cloud service or on the mobile phone synced with the IoT device. The evidence analysis procedure involves the analysis of data stored on cloud and the devices found on the crime scene
- Analysis of the acquired evidence may be complicated depending on the format in which it was obtained. The main issue at this point of the investigation is the volume of data that an IoT device might generate

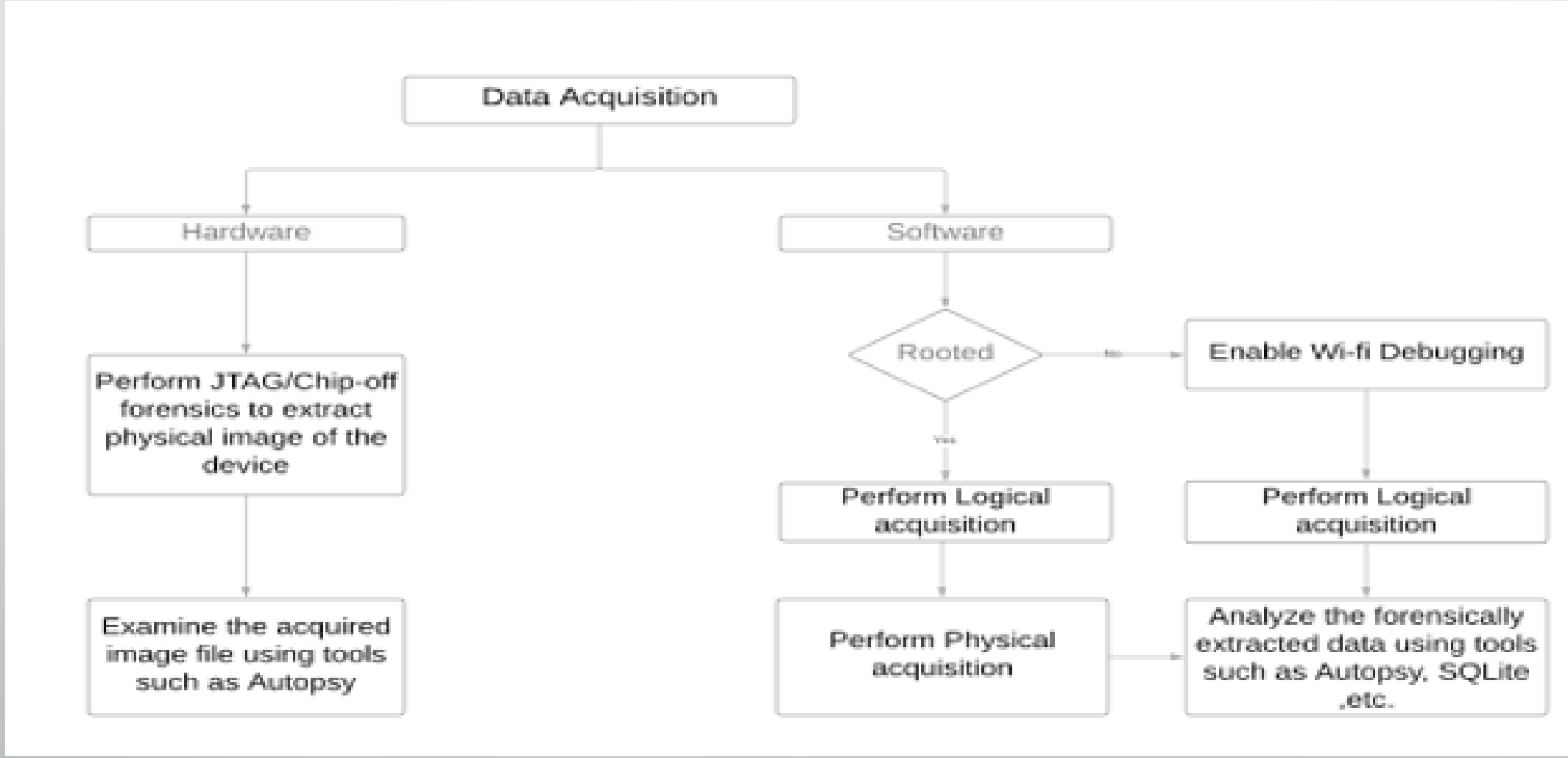
Presentation

- A report will be prepared regarding the evidence and the forensics analysis procedure, and presented in the court along with the physical evidence.
- Documenting the findings of the forensics investigative process can itself be a challenge to the forensic investigators. The analytical processing for an investigation can alter the data stored on IoT devices. The quality of data stored on an IoT device can also create challenges for the forensic investigators

IoT Devices: Smartwatch

- Smartwatches are wearable IoT devices capable of connecting to a smartphone or network using Bluetooth, Wi-Fi, GPS, and NFC.
- These devices can be exploited by hackers to obtain confidential information regarding a user by hijacking the device's microphone, sensors, and the wireless communication.
- Smartwatches are also capable of determining the location and the activity of the user; hence, hackers can use the location and movement sensors on the smartwatch to track the movements and the location of the user.
- The attacker can obtain sensitive information from the device pertaining to the user, including PINs, passwords, physical location of the user, after gaining root access to the device.

Steps Involved in Data Acquisition and Analysis of Android Wear



Logical Acquisition of Android Wear

Enable developer options on the smartwatch

Connect the watch to a Wi-Fi network (Note: The smartwatch and forensic workstation must be connected to the same network)

Enable Wi-Fi debugging Settings > Developer Options > Debug over Wi-Fi

Now, the smartwatch displays its IP address that can be used to establish connection between forensic workstation and the smartwatch adb connect <device_IP_address:port_number>

After establishing the connection, the forensic investigator can perform logical acquisition on the device using adb pull command, adb pull <source_directory> <destination_directory>

Physical Acquisition of Android Wear

Establish connection between device and the forensic workstation using Android SDK platform tools

Execute the command "adb devices" and select the smartwatch from the device list

If the device's serial number can be seen on the ADB command shell, it means that the device is connected to the system. Now, run 'adb shell" command to acquire root shell and perform Image acquisition.

To generate boot partition image of the drive, the following command can be executed: dd if=<source_drive> of=<destination_drive> bs=512

Now, the smartwatch displays its IP address that can be used to establish connection between forensic workstation and the smartwatch adb connect <device_IP_address:port_number>

After establishing the connection, the forensic investigator can perform logical acquisition on the device using adb pull command, adb pull <source_directory> <destination_directory>

Recovered Forensic Artifacts: Android Wear

File name	Directory	Purpose
Calendar.db	/data/data/com.android.providers.calendar/databases/	Stores calendar entries
calllog.db, contacts2.db, profile.db	/data/data/com.android.providers.contacts/databases/	Contacts, call logs, and user profiles are stored in this database file
downloads.db	/data/data/com.android.providers.downloads/databases/	This database file contains data present in the "Download" application
googlesettings.db, subscribedfeeds.db, gservices.db	/data/data/com.google.android.gsf/databases/	Google Service Frameworks for Android
bt_did.conf, bt_stack.conf	/system/etc/bluetooth	Contains data associated with Bluetooth connected devices
android_pay, config.db, fitness.db, reminders.db, etc.	/data/data/com.google.android.gms/databases/	This database directory contains .db files of Google applications and APIs that help support functionalities across devices
complications.db	/data/data/com.google.android.wearable.app/databases/	Contains complications display information

Analysis of the Apple HomePod and the Apple Home Kit Environment

Data extraction:

Previously there was no viable solution to directly extract data from the Apple HomePod. The iFixt website published a teardown of the Apple HomePod, that revealed a 14-pin connector under the rubber base


STREET

In the paired iPhone we can get

- HomePod basic information (serial number, os version, name, and so on)
- HomePod settings
- HomePod geolocation
- Home organization in "Rooms"
- Connected HomeKit device
- User interactions (played songs)
- Door sensor information and usage logs

In the HomePod Sysdiagnose logs we get

- HomePod basic information (serial number, os version, name, and so on)
- HomePod settings
- HomePod network connections
- HomePod PowerlLogs
- HomePod Syslog Archive

- https://www.indiatoday.in/india/story/expert-accused-of-hacking-atm-machine-servers-using-modern-gadgets-arrested-by-delhi-police-1883339-2021-12-02
- https://blog.digital-forensics.it/2021/01/a-journey-into-iot-forensics-episode-5.html


Thank you!