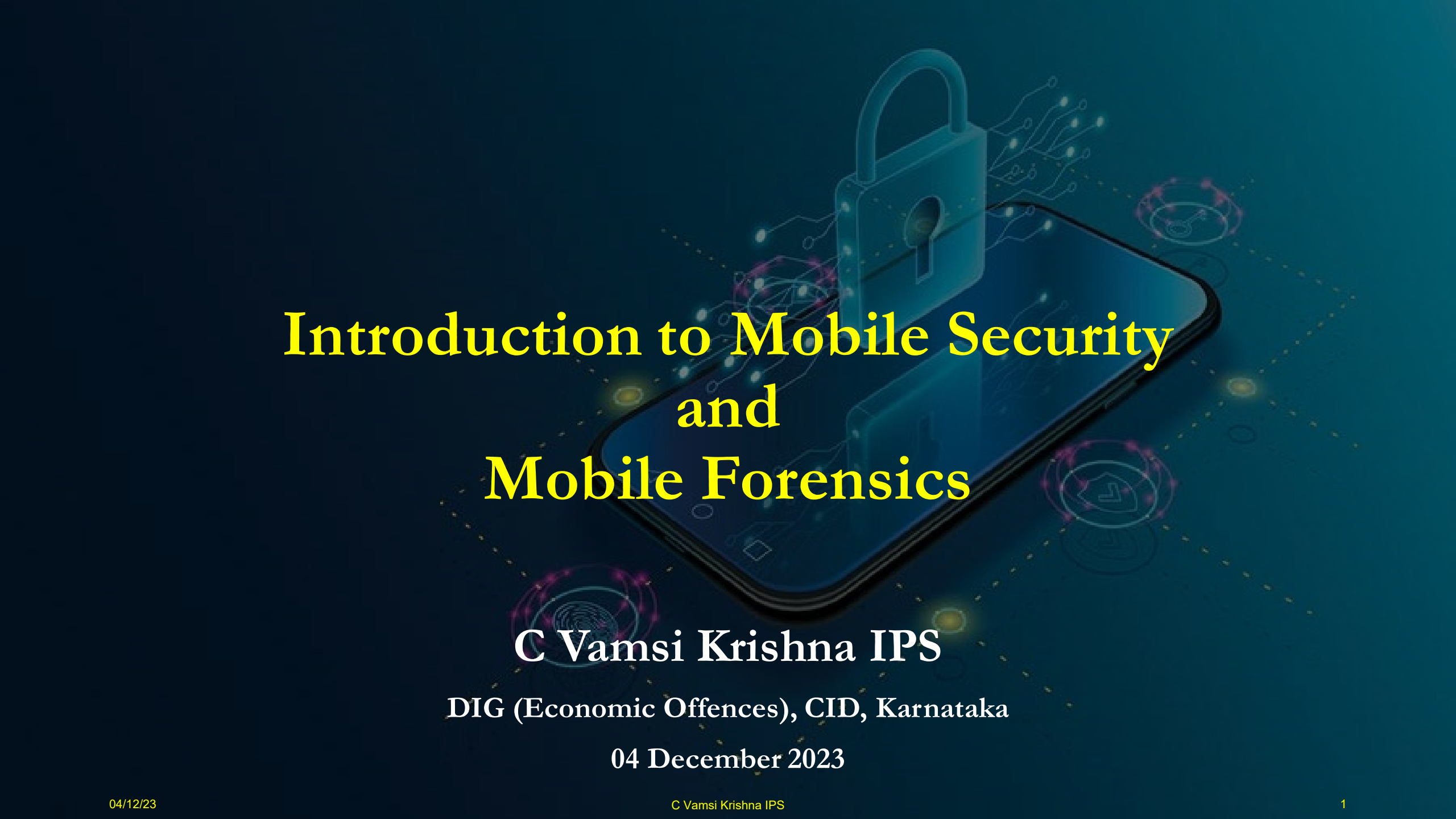


Introduction to Mobile Security and Mobile Forensics

C Vamsi Krishna IPS

DIG (Economic Offences), CID, Karnataka

04 December 2023

Agenda

- Mobile Phone Usage and Threat landscape
- Mobile Security Threats and attacks
- Introduction to Mobile technology and GSM terminologies
- SOP of Mobile Forensics

Case Study

- X is a native of Kerala, received a video call from an unknown number. Upon answering the call, he found the caller to be similar to his former colleague in Andhra Pradesh. The caller even mentioned the names of some of their common friends.
- The call went on for few min. However, a few minutes into the call, the caller requested the victim for Rs 40,000 for immediate assistance for a relative in the hospital. Wanting to help his friend, the victim agreed to help and sent the amount online.
- However, a short time later, the same person asked for another Rs 35,000. But this time, the victim became suspicious. He subsequently contacted his former colleague directly to cross-check. It was then that he realized he had been cheated and the call was not genuine.

How did the crime happen?

- **What's interesting is - How did the perpetrator get the following information:**
  - **The relationship between the victim and the colleague**
  - **The victim's phone number**
  - **The names of other common friends**

How do you prevent such a crime from happening?

Another Case...

- A person in Mehsana, Gujarat filed a FIR stating that cybercriminals have stolen Rs 37 lakh from his bank accounts within a span of 30 minutes, though he didn't share OTP or any other sensitive information with anyone.
- He claims to have received back-to-back money transaction messages on December 31 while he was working in his office.
- After receiving back-to-back unauthorized transaction notifications, he rushed to the bank and informed officials about the withdrawals and requested to freeze his account to stop further withdrawals. He also informed that he was unable to access his account through net banking and his username and password entries were shown invalid.

How did it happen?

How do you prevent such a crime from happening?

The phone is no longer a device we use.

It has become a second home we often escape to.

However, it also became a tool to defraud and exploit our vulnerabilities

Image source: Wall Street Journal

Understanding Mobile Security Threat Landscape

Evolving Mobile Usage

- **Always pushing tech boundaries.**
- Smartphone is now taking on tasks it was never designed to carry out.
- **What does this mean for security?**

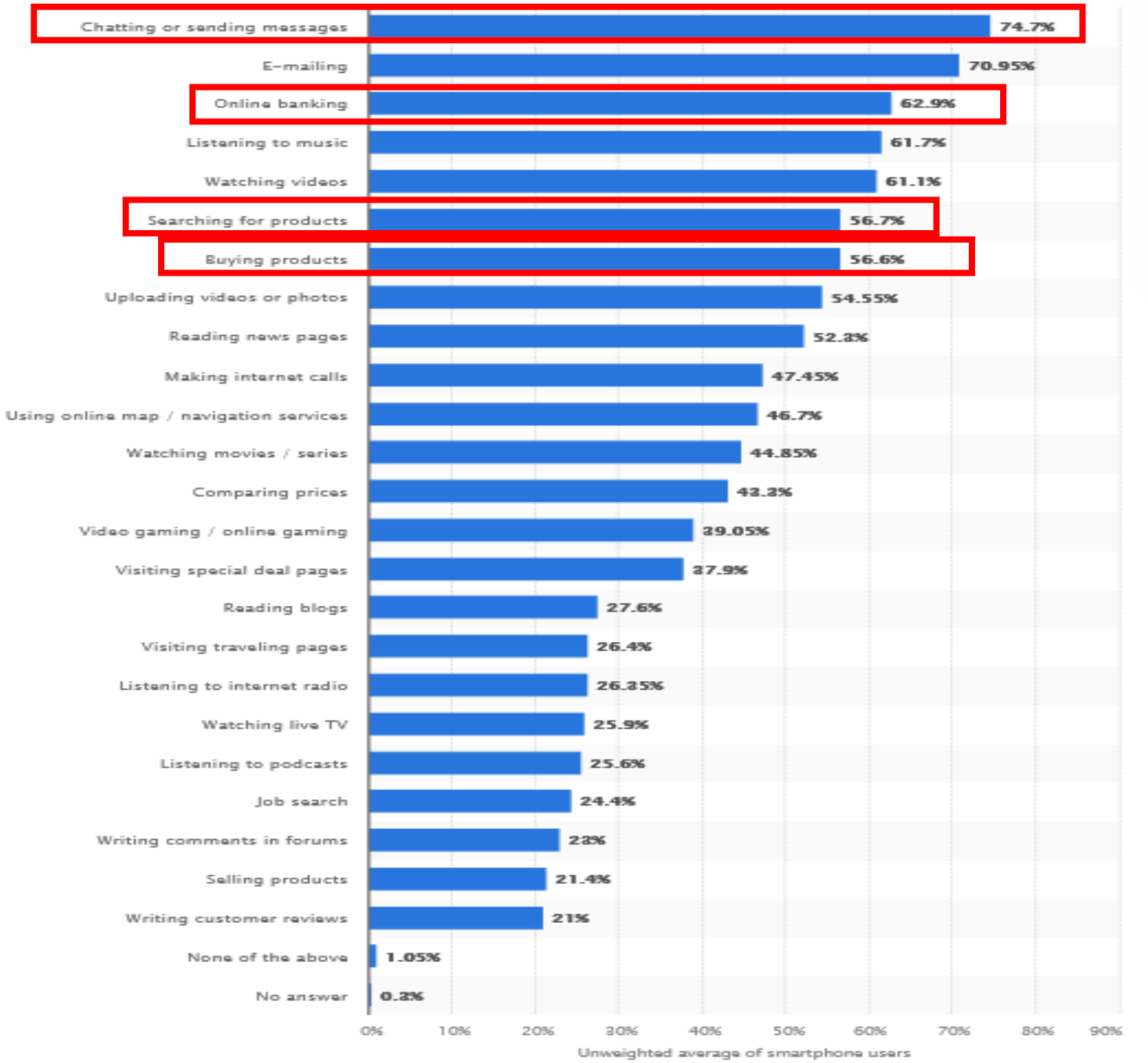
Image source: https://licelus.com

We use Mobile Phones for….

(Survey of June 2022 to July 2023)

- Communication and Interaction
- Education
- Office and Professional works
- E-Banking and Finance
- Photo and video
- Entertainment
- Navigation
- Notes and Reminders
- Shopping and Deliveries
- Health and Fitness
- IoT and Smart device Management
- Travel

List is endless….



Source: Statista

App Dependent lives…

- The average person uses **9 mobile apps per day** and has around 80 apps installed.

- Means around 62% apps don't get used per month.

Source: socialmediatoday.com

iOS and Android Operating systems

iOS

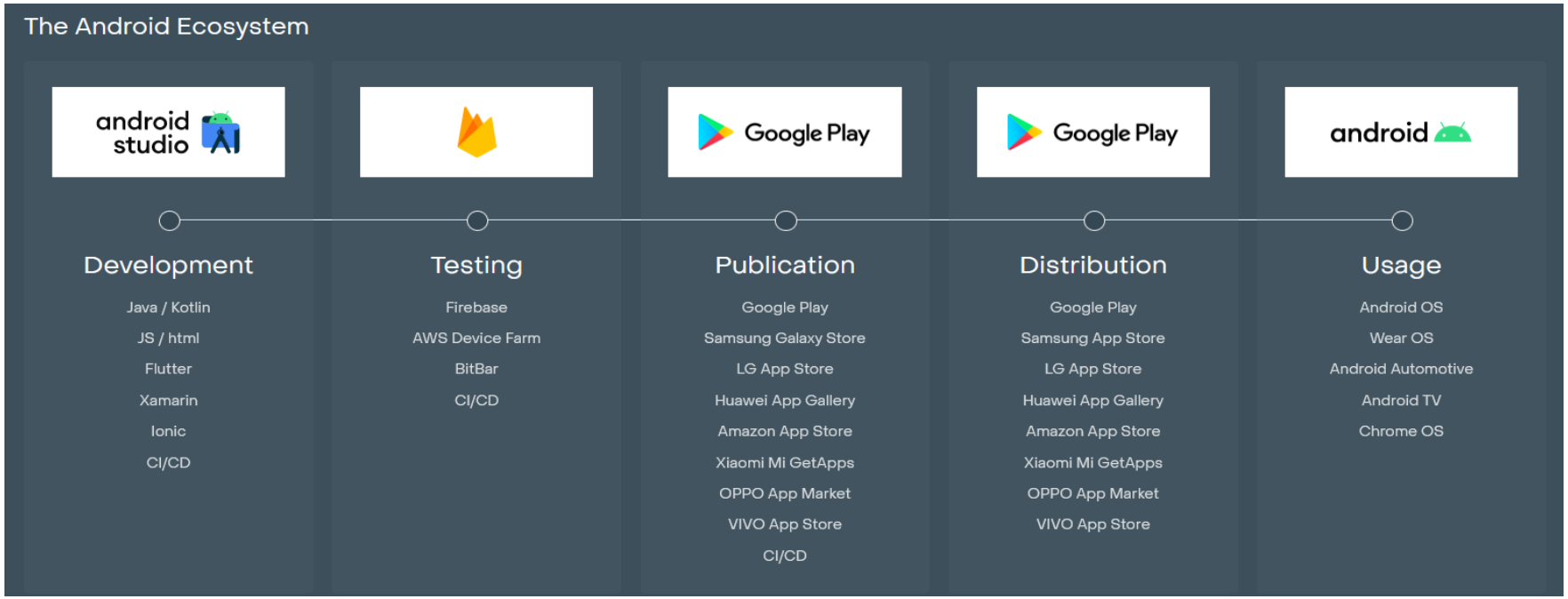
The centralized nature of Apple and its streamlined update process makes iOS a more secure platform than Android with over 1.46 billion users in 2023.

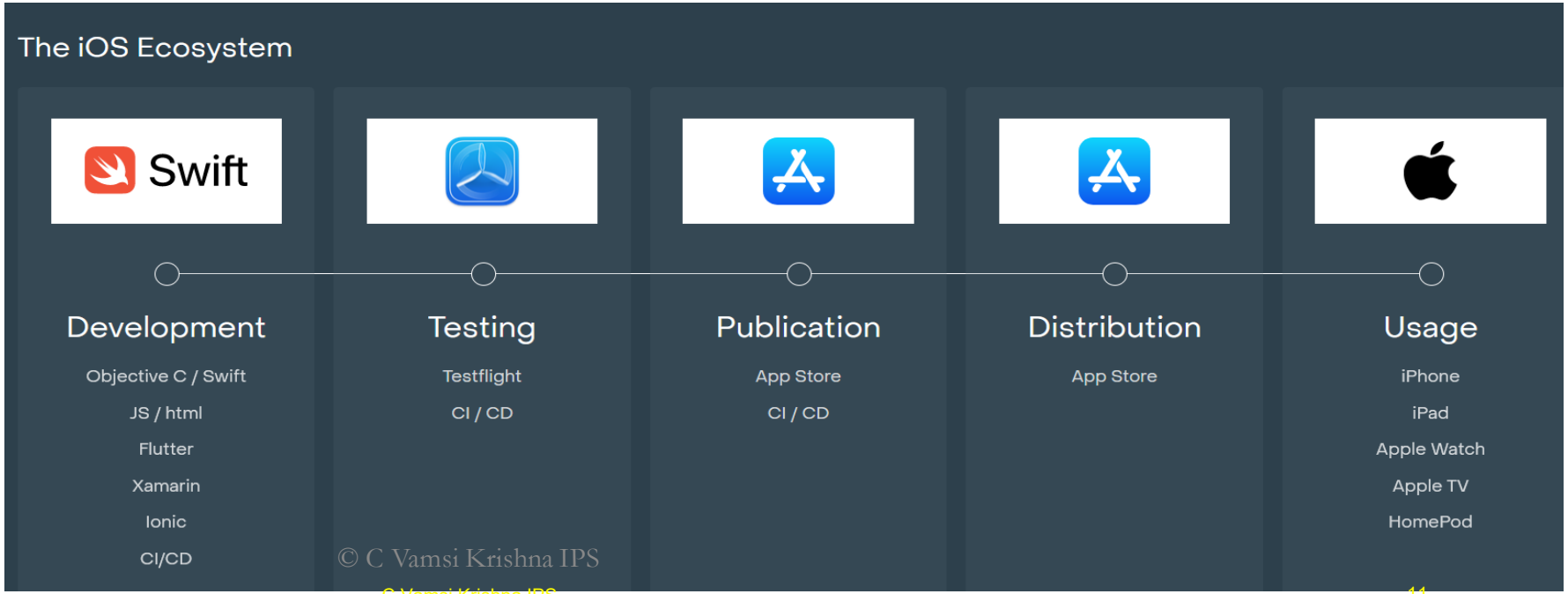
However, In 2020 alone, over 1,200 malicious apps were available in the Apple app store — and were being downloaded more than *300 million times* a month

Android

- Linux based OS with 3.6 billion users in 2023
- Android's open nature allows for plenty of freedom and customization. But a large proportion of devices are running legacy versions with security gaps attackers can exploit. **Only 37% of global Android users were using the latest version at the start of 2022**. [statcounter.com]
- In 2021, security researchers discovered that 13 popular Android apps exposed the personal data of up to 100 million users.
- According to a report released by Apple, Android devices have up to 47x more malware than iPhones

Differences in Ecosystem from development to usage





Mobile Security Threats

Digital Privacy is a myth

What we can hope is at best for proper protection of private data

Personal Data Collection

Apps may be collecting lots of data

Social Media and Messaging Apps

Scanning apps

Loan Apps etc

Dating apps (tindr, grindr)

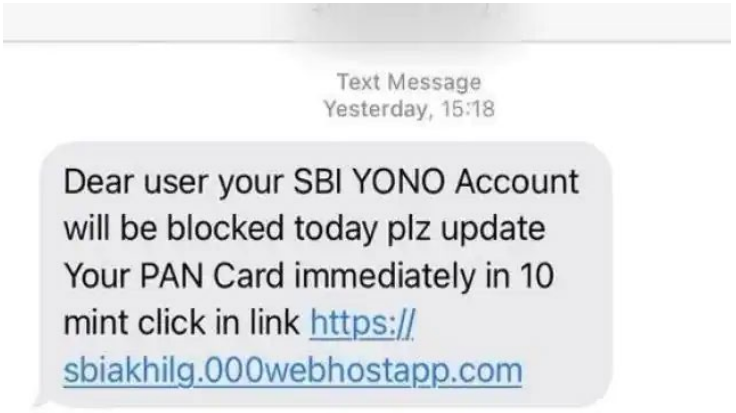
Malware Attacks

- Malware may often arrive on a user's phone via a seemingly legitimate text message.
- Malware can also be pushed without the user even clicking on any link.

- **Types of Malware**
  - Risktool – SMSreg, Dnotua, Robtes
  - Banking Trojans – 1,96,476 detected – Bray Trojan, Trojan.Fakecalls
  - Adwares – Adlo, Ewind, HiddenAd
  - Ransomware Trojans – trojan.pigetrll/lockscreen, trojan.locker/rkor

How Do Phones Get Infected with Malware commonly

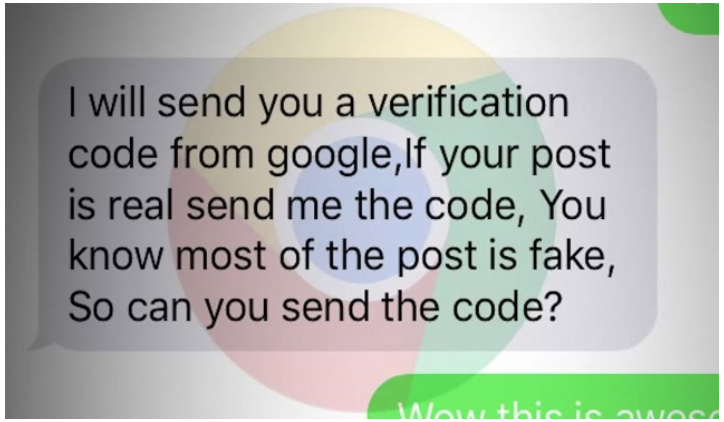
Juice jacking



Phishing attacks

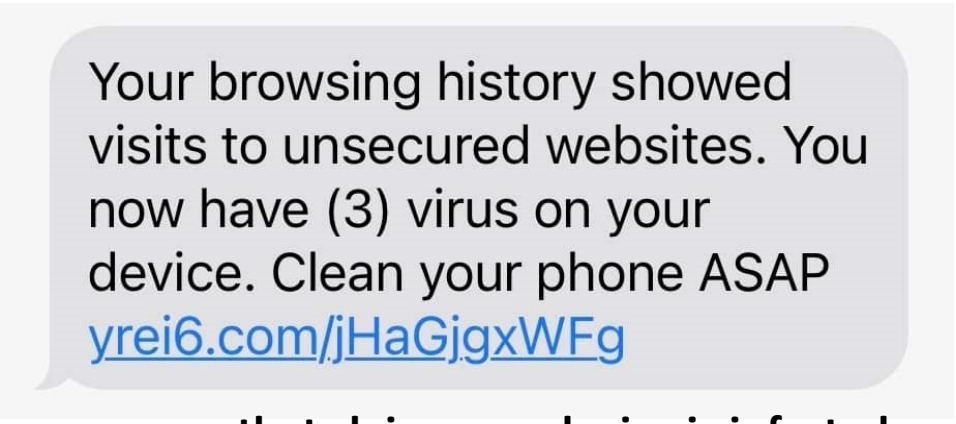
Wi-Fi and Bluetooth attacks

Interestingly mobile phishing is more successful.



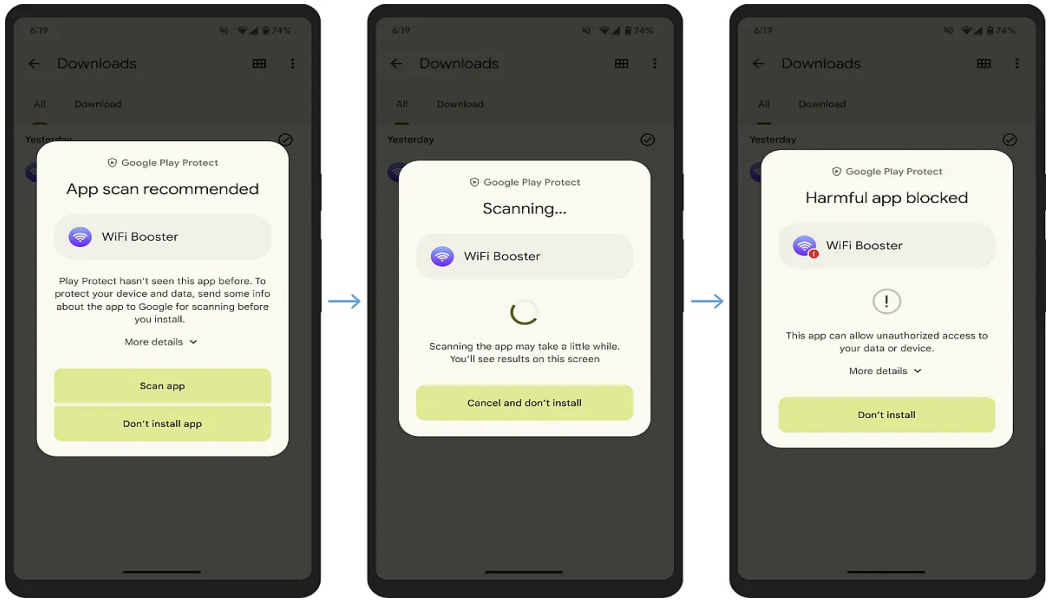
Verification code scams

Malicious Apps



pop-ups that claim your device is infected

Malicious and Cloned Apps

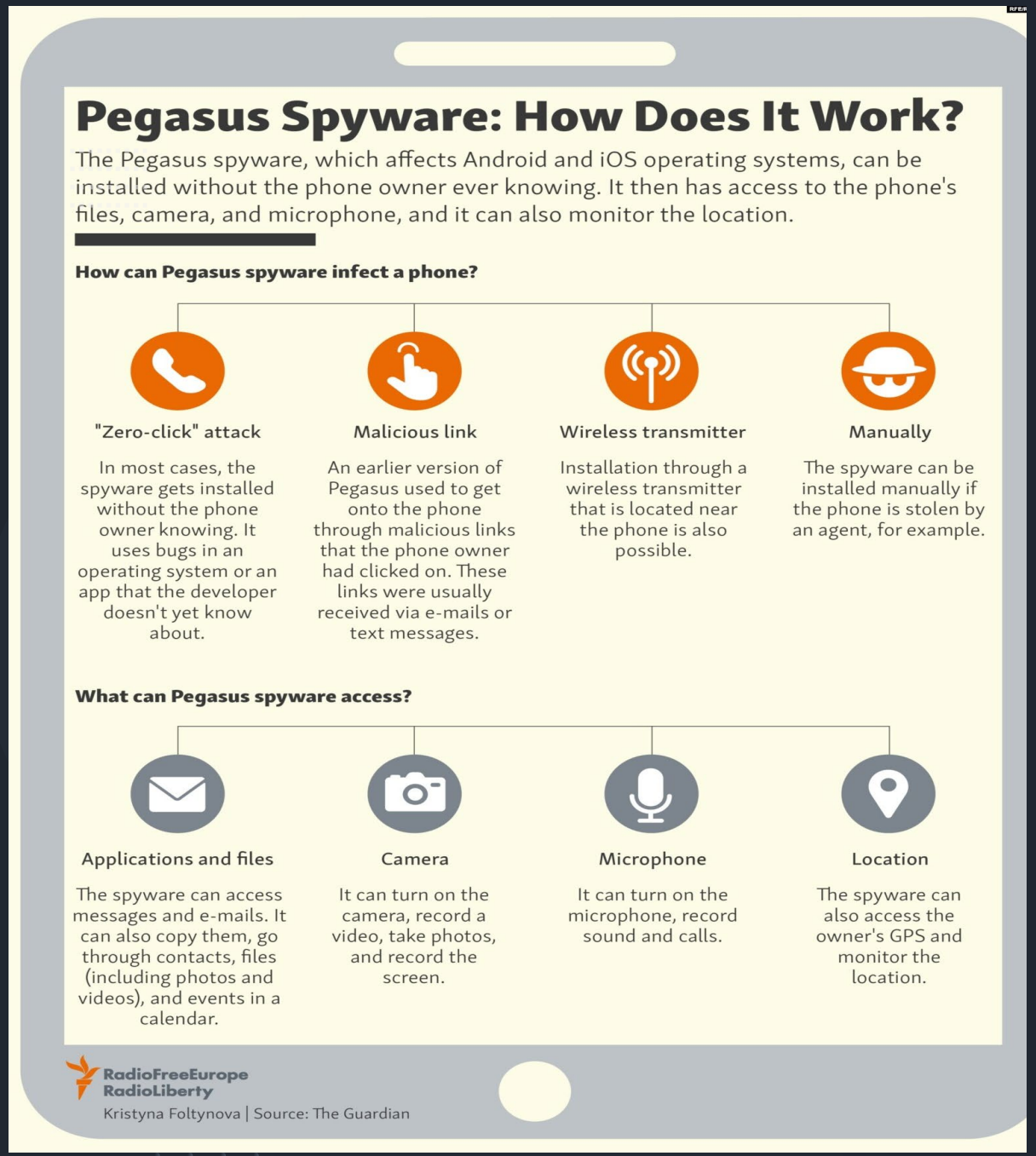


Malicious Apps:

- Kaspersky has claimed that Android users downloaded malware from Google's Play Store over 600 million times in 2023
- **Ex: Sharkbot banking Trojan downloader is disguised as a fake antivirus and was downloaded** more than 15000 times before it was taken down.

Cloned Apps:

- Its quite simple to decompile a genuine app and release a fake version and the end user may be misled to download the fake version
- Once the cloned, bogus application is downloaded, any information a user shares - login details, passwords, or financial data - can be harvested by the attacker.



"Pegasus"

Works on both Apple and Android

Pegasus has extensive capabilities.

Can even infect without user's intervention

Used across 46 countries on thousands of users

Mobile Numbers

What happens if they fall in wrong hands ?

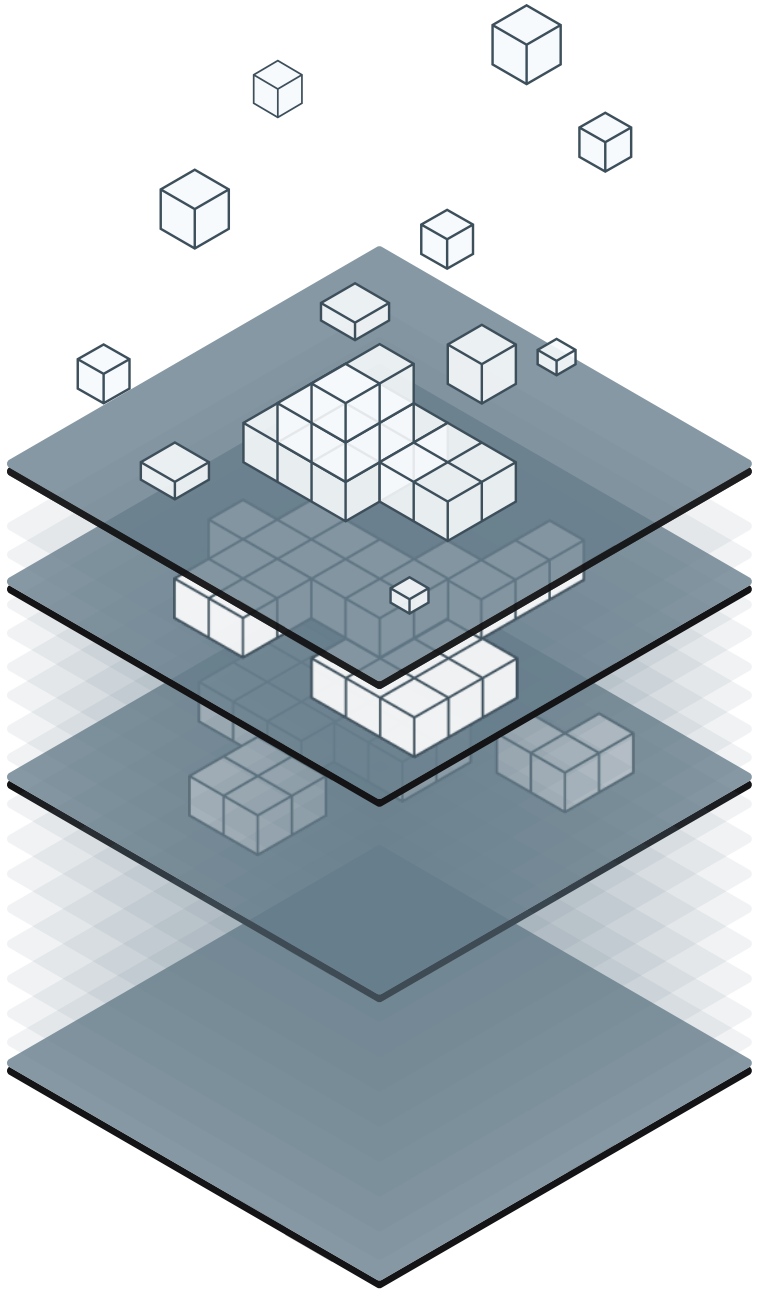
Sources for Phone Numbers

- Yellow pages and Directories
- Social media
- Phishing scams
- Data leaks
- Selling of data
- The Dark Web – almost 1/4th of leaked data contains phone numbers
- Shoulder surfing and Dumpster Diving

What can threat actors do with phone numbers:

1. **Phishing, Vishing and Smishing**
2. **Marketing and Bombarding with Adware**
3. **Exploiting vulnerabilities in websites and apps connected to you and steal personal data.**
4. **Sim Swapping**
5. **Doxxing leading to harassment and fraud**
6. **Blackmailing and Sextortion**
7. **Spoof calls to your friends and scam them**

Measures to take for effective Mobile Security



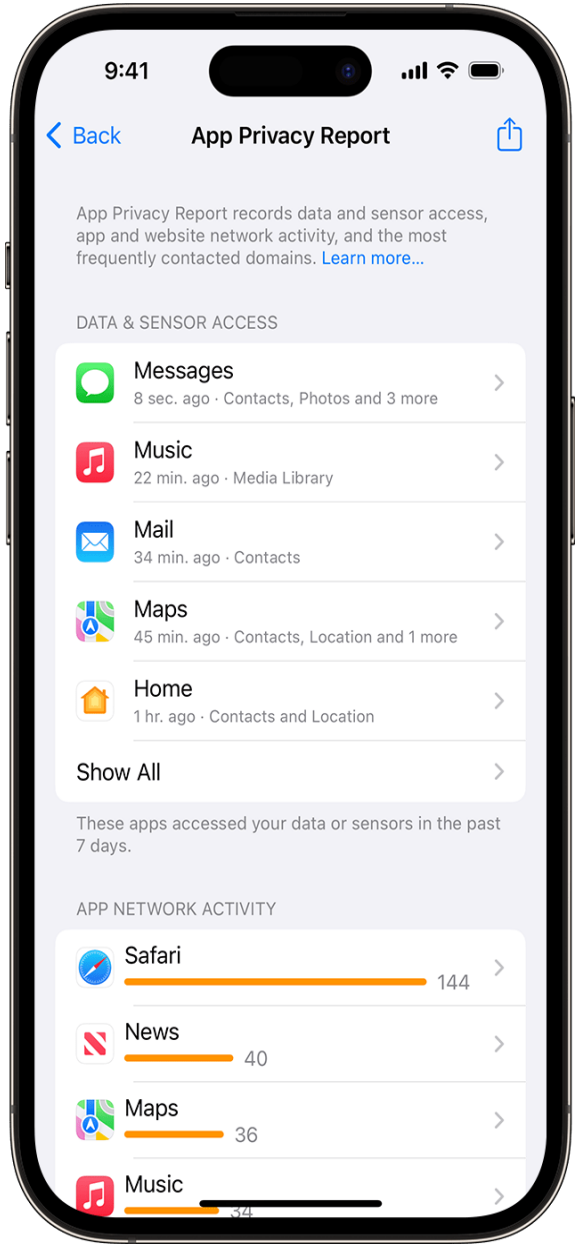
Layered approach to Security is the Need of the Hour

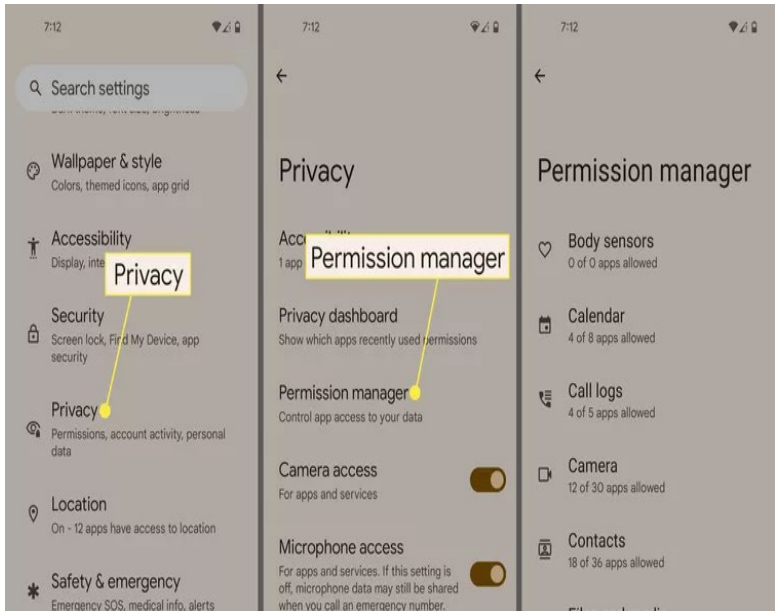
Android and iOS

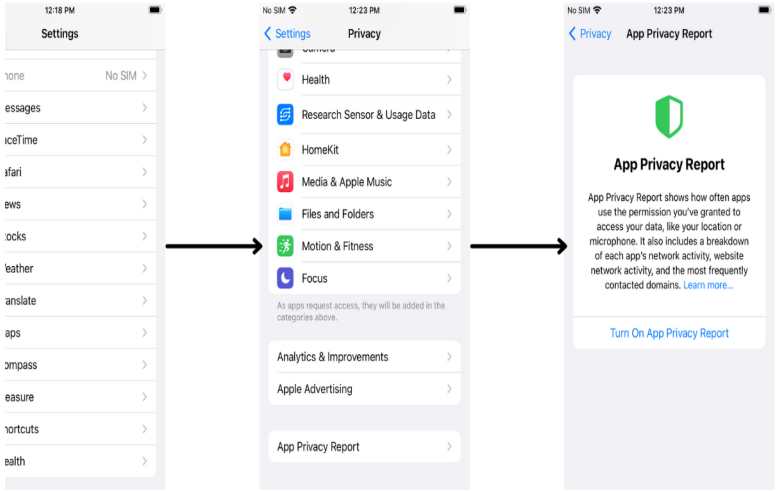
Multiple layers of security are needed to stop modern, sophisticated cyber threats. You can't rely on Apple and Google alone.

Review Permissions

- **Apple**
  - App **privacy report** updates you on how often apps use the permissions that you've granted to access your data.
- **Android**
  - Settings -> Privacy -> Permission Manager







Settings | Privacy menu | Apple Privacy mode

Upgrading to latest version of apps, OS and to latest devices

- **Upgrading versions of apps and OS** to latest version provides improved protection from malware, viruses, and hackers

- **Upgrading to latest devices/hardware**
  - Its impossible for the major platforms to protect all of their legacy devices from cyber threats.
  - Ideally once in every 2 to 3 years

Identification of Malware on Phone

YOUR PHONE'S BATTERY LOSES CHARGE FASTER THAN USUAL.

INCREASED DATA USAGE

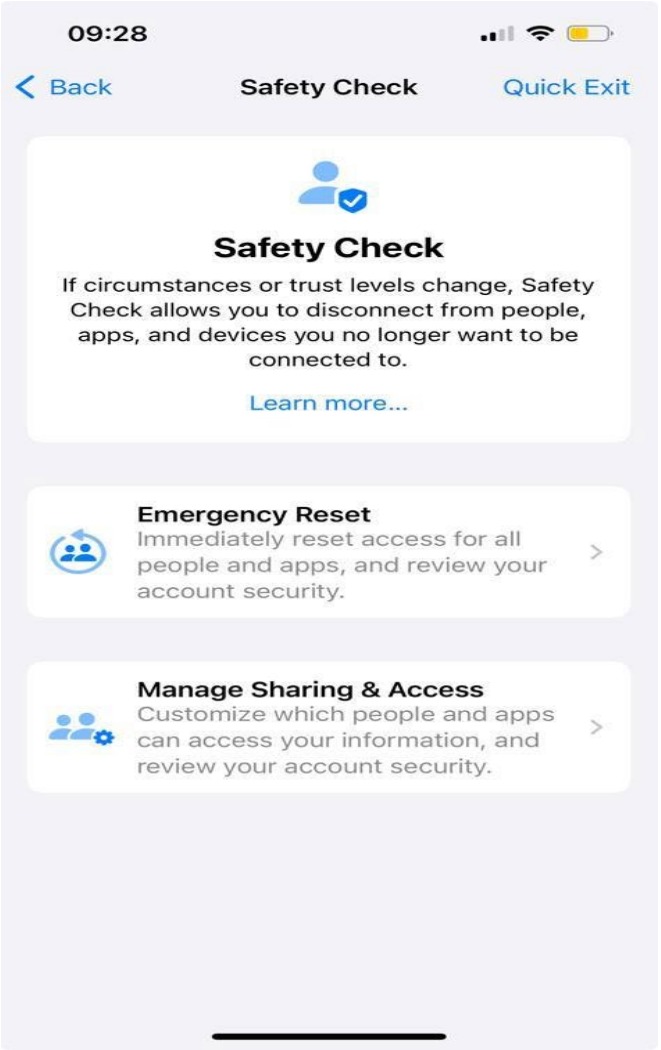
YOUR DEVICE IS ACTING STRANGELY - WORKING SLOWLY, HANGING FREQUENTLY, HEATING UP

NEW APPS SEEN WHICH HAVE NOT BEEN INSTALLED BY YOU.

YOU'RE LOCKED OUT OF YOUR APPLE ID OR GOOGLE ACCOUNT AND UNABLE TO LOGIN INTO ONLINE ACCOUNTS.

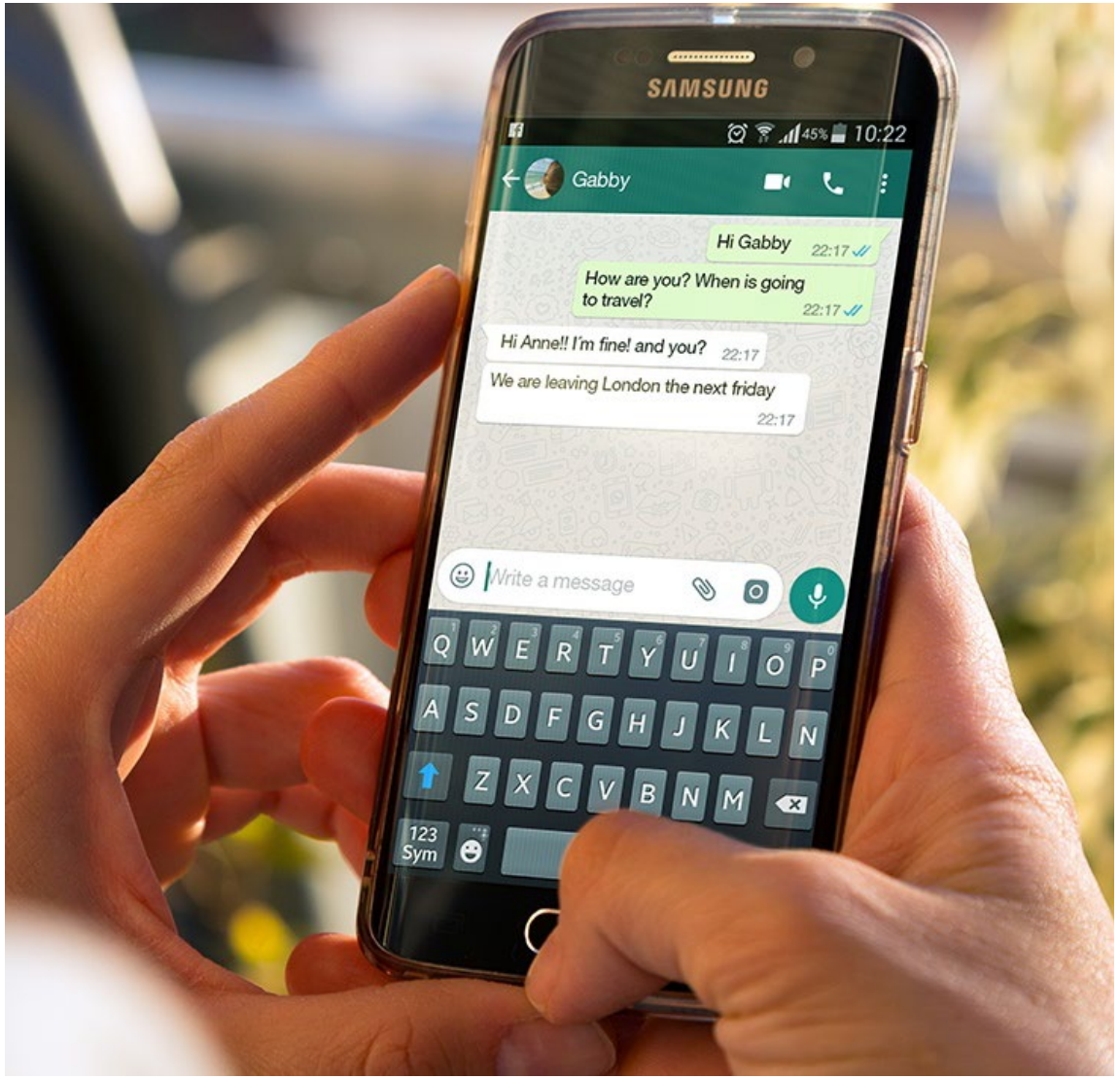
YOU RECEIVE 2FA CODES YOU DIDN'T REQUEST.

YOUR CAMERA OR MICROPHONE INDICATOR LIGHT TURNS ON.



WhatsApp Safety

- **Use only genuine App from store**
- **Two-step verification –** for registering on a new device (PIN)
- **Privacy**
  - **Privacy Checkup feature of WhatsApp**
  - **Screen Lock**
  - **Protect IP address in calls**
  - **Profile Photo privacy**
  - **Add to groups**
- **Chat Backup (encrypted and non-encrypted) and Export Chat**



What the user can do to protect their data and phone….

- Use multifactor authentication especially authenticator aps
- Make sure you're using the latest version of the Apps and OS
- Be wary of untrusted networks
- Know the data that you're sharing
- Don't install mobile apps from untrusted places
- Don't root or jailbreak your phone
- Use strong passwords and biometric data
- Use an anti-malware solution
- Don’t store personal information and autosave passwords in phones

Lost the Phone?

Don’t Panic

When you lose your Phone

What can the thief do….

- Make unauthorized purchases using your linked credit cards and Apple or Google Pay.
- Access your passwords and login information for various accounts. (As many as 99% of people reuse passwords across business and personal accounts. So, if scammers gain access to your phone, they can potentially get into your other accounts.)
- Access your bank accounts or investing apps and wire out your savings.
- Mine enough personal data to steal your identity.
- Hack your Google or Apple ID and bypass two-factor authentication (2FA) on your other apps.
- Run phishing scams targeting your friends and family.
- Use sensitive photos to blackmail you (i.e., sextortion).
- Find out what places you visit and get details about your economic status.
- Open credit cards and loans in your name.

If the Phone is lost and not stolen…

1. **Locate your phone using the "Find my device" function** - uses internet, network and also GPS to locate phones
2. **Put your device into "Lock mode"** and set a custom message on the screen displaying your contact details.
4. **Report the loss – CEIR portal** https://www.ceir.gov.in

Add a custom message with your phone number.

Is your mobile lost/stolen? Report at the local Police Station and use this web portal to block the IMEI. You can also visit your telecom service provider outlet or State Police to get the IMEI blocked.

क्या आपका मोबाइल खो गया है / चोरी हो गया है? स्थानीय पुलिस स्टेशन पर रिपोर्ट करें और आईएमईआई को अवरुद्ध करने के लिए इस वेब पोर्टल का उपयोग करें। आईएमईआई को अवरुद्ध करने के लिए आप अपने दूरसंचार सेवा प्रदाता आउटलेट या राज्य पुलिस से भी संपर्क कर सकते हैं।

How to block the phone's IMEI

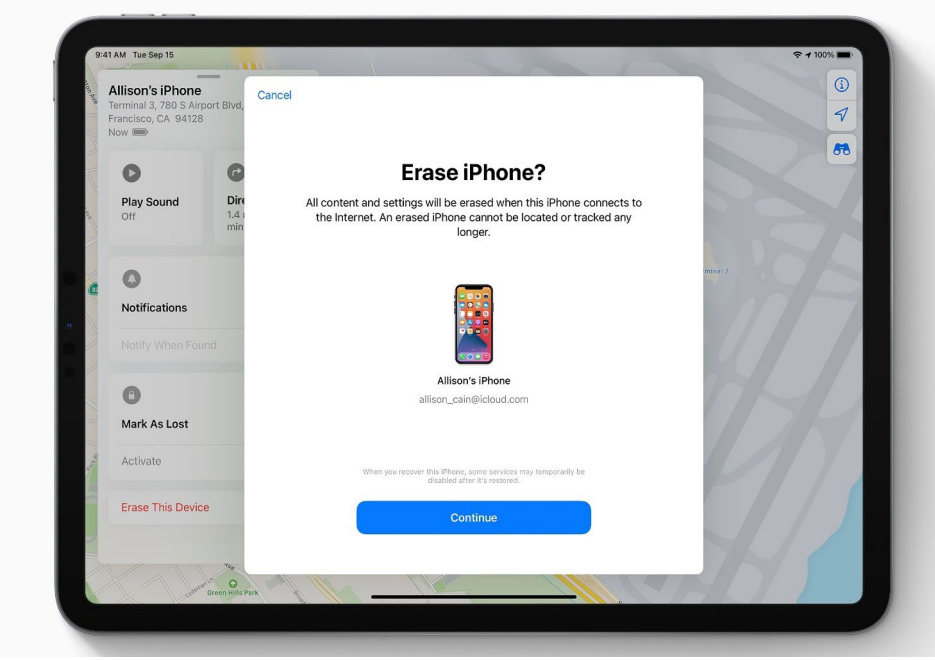
- **Through State Police**.
- The **user** can block the phone's IMEI by **any one** of the following means: Through a form submitted on this website.
- The procedure to do it is as follows: -
  - **File a report with the police, and keep a copy of the report.**
  - **Get a duplicate SIM Card for the lost number. OTP will be sent on this number** while submitting the request for blocking your IMEI.
  - **Get your documents ready - a copy of police report and an Identity Proof must be provided.**.
  - Fill out the request registration form for blocking the IMEI of lost/stolen phone, and attach the required documents.
  - After submitting the form, you will be given a Request ID.

How to unblock the phone’s IMEI

- **To unblock a lost/stolen phone's IMEI, the user has to report to local Police that it is found.**
- **After that user can unblock the phone through a form submitted on this website.**
- **The procedure to do it is as follows: -**
  - Fill out the request registration form for unblocking the IMEI of found phone.
  - After submitting the form, the IMEI will be unblocked**.**

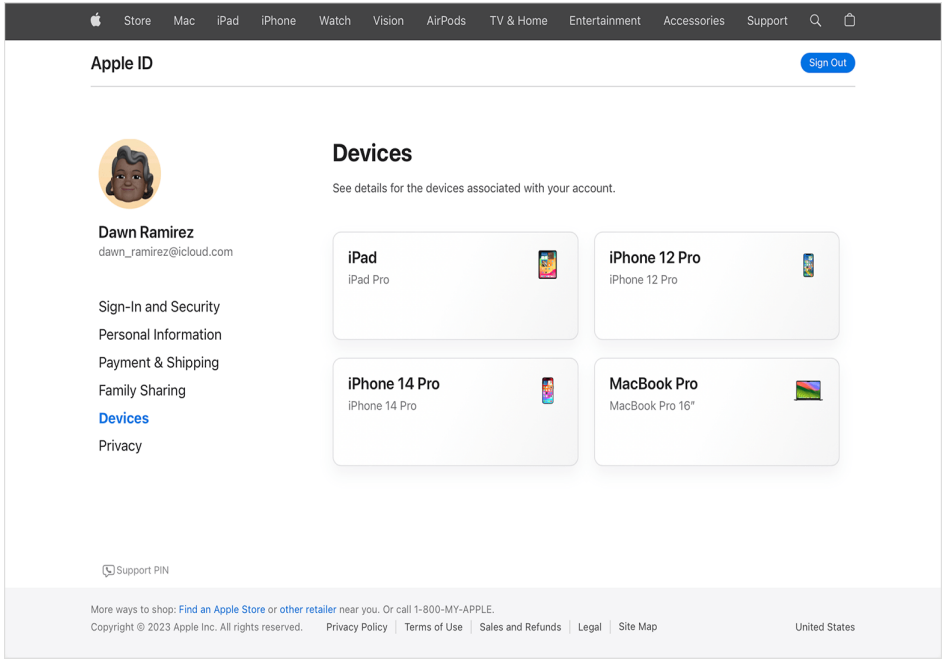
If the Phone is Stolen

- **Report the theft to your provider – CIER and Police**
- **Cancel any credit cards that were linked to Apple or Google Pay**
- **Warn friends and family about phishing scams**
- **Remotely erase your phone's data**
- **Contact your phone insurance provider**
- **Remove the device from your account**
- **Lock your phone remotely**



Change your main passwords, and enable 2FA using Authenticator App and not SMS

- **Account passwords you should change:**
  - Email — both your primary account and any backup accounts you use.
  - Social media accounts.
  - Mobile banking and investment apps.
  - Shopping apps like Amazon.
  - Streaming apps like Netflix or Prime.
  - Your password manager



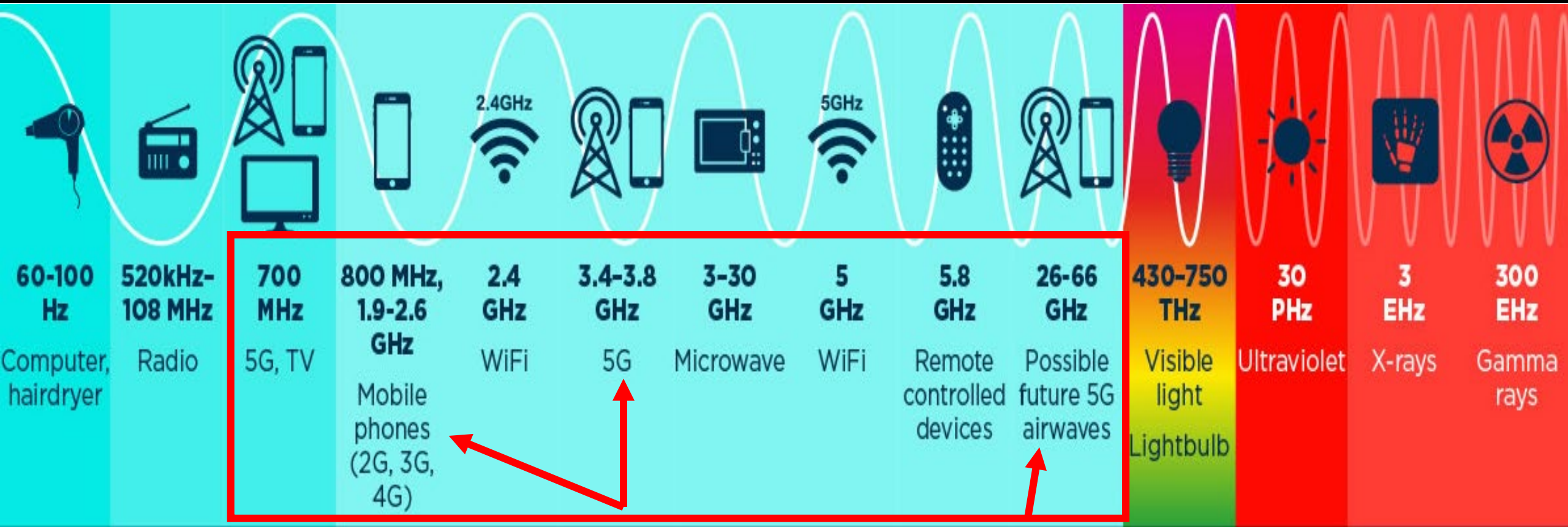
Understanding Mobile Technology

A Prerequisite for Mobile Forensics

Do you know...

1. Is mobile technology completely wireless???
2. Is the communication secured/encrypted???
3. How does the network know where you are to connect the call??
4. How is the connection established to the other end when you dial a number???
5. Why is the call not dropped when you are moving???

EMR Frequency Spectrum



From left to right, what happens to

- Frequency
- Wavelength
- Energy
- Data Carrying Capacities
- Antenna Size

G TECHNOLOGY EVOLUTION

1G	2G	3G	4G	5G
speed in kilobit per second 2.4 Kbps	speed in kilobit per second 64 Kbps	speed in kilobit per second 2,000 Kbps	speed in kilobit per second 100,000 Kbps	speed in kilobit per second 1Gbps
Analog Voice	Digital Voice + Simple Data	Mobile Broadband	Faster and Better	Real World Applications

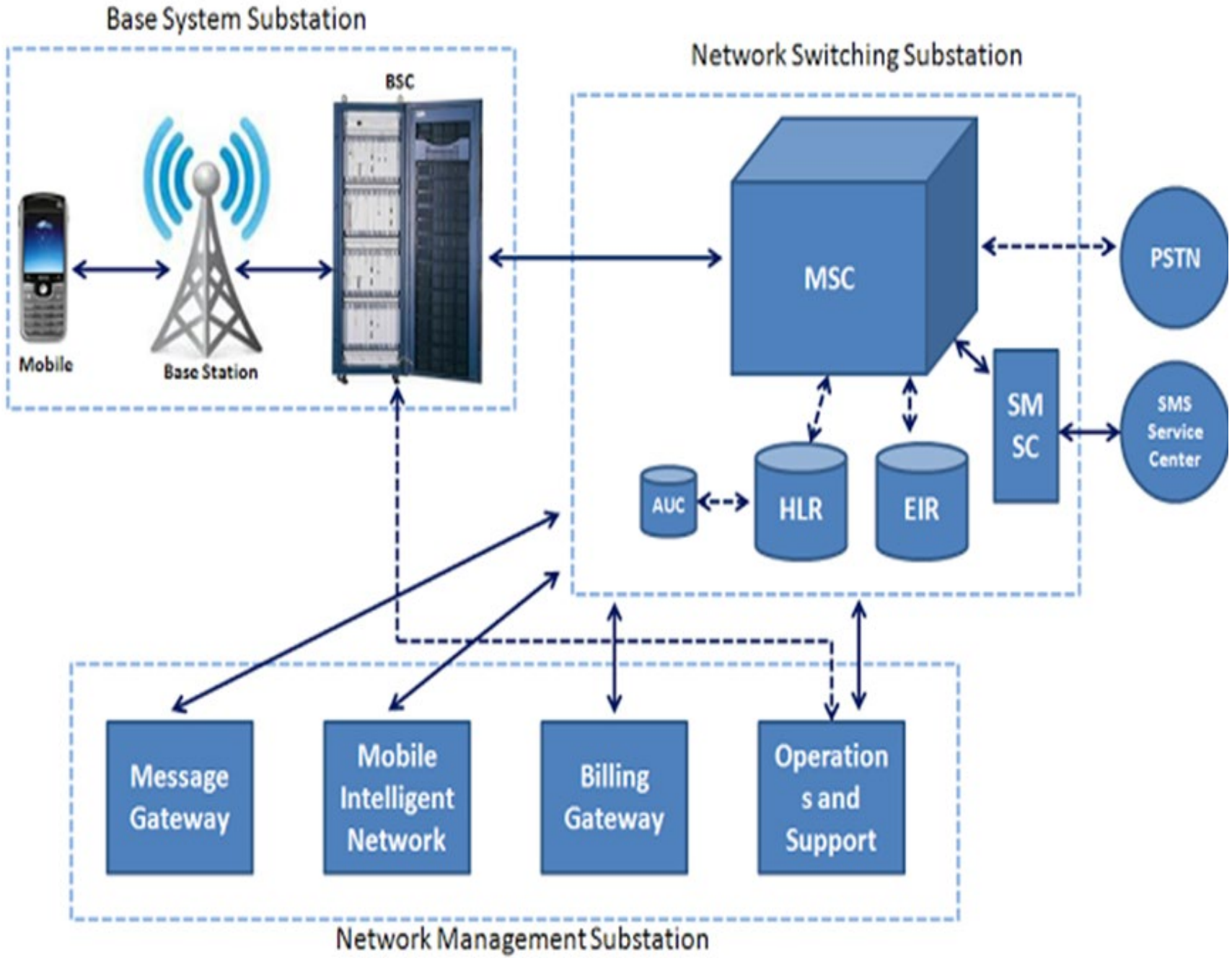
Richer Content (Video)

More Connections

Cellular Network

- Mobile phones communicate with cell towers that are placed to give coverage across a telephone service area which is divided up into 'cells'.
- Approximated to hexagonal shapes.
- Each cell uses a different set of frequencies
- The cells are therefore sized depending on the expected usage density

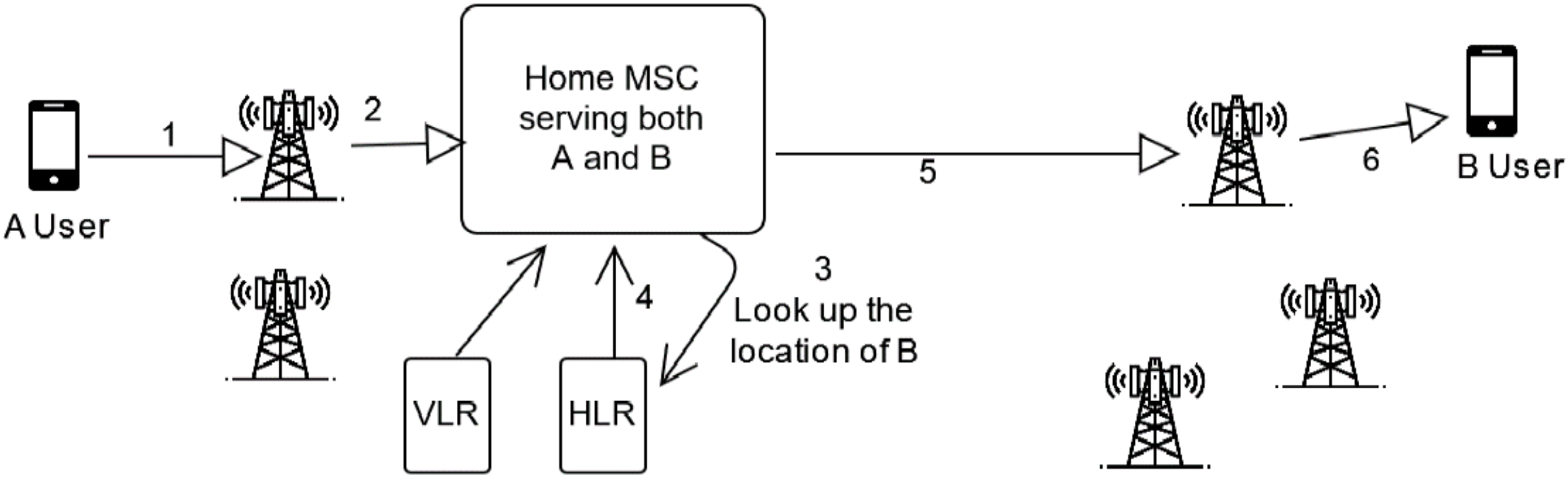
GSM Network Architecture



Mobile Services Switching Center (MSC)	Switching of calls between the mobile and other fixed or mobile network users, registration, authentication, location updating, handovers, and call routing to a roaming subscriber. Every MSC is identified by a unique ID.
Home Location Register (HLR)	The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status.
Visitor Location Register (VLR)	The VLR is a database that contains temporary information about subscribers to service visiting subscribers. During roaming, the VLR connected to that MSC will request data about the mobile station from the HLR.
Authentication Center (AUC)	The Authentication Center is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering of the radio channel.
Equipment Identity Register (EIR)	The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where its International Mobile Equipment Identity (IMEI) identifies each MS.

Mobile Call Routing

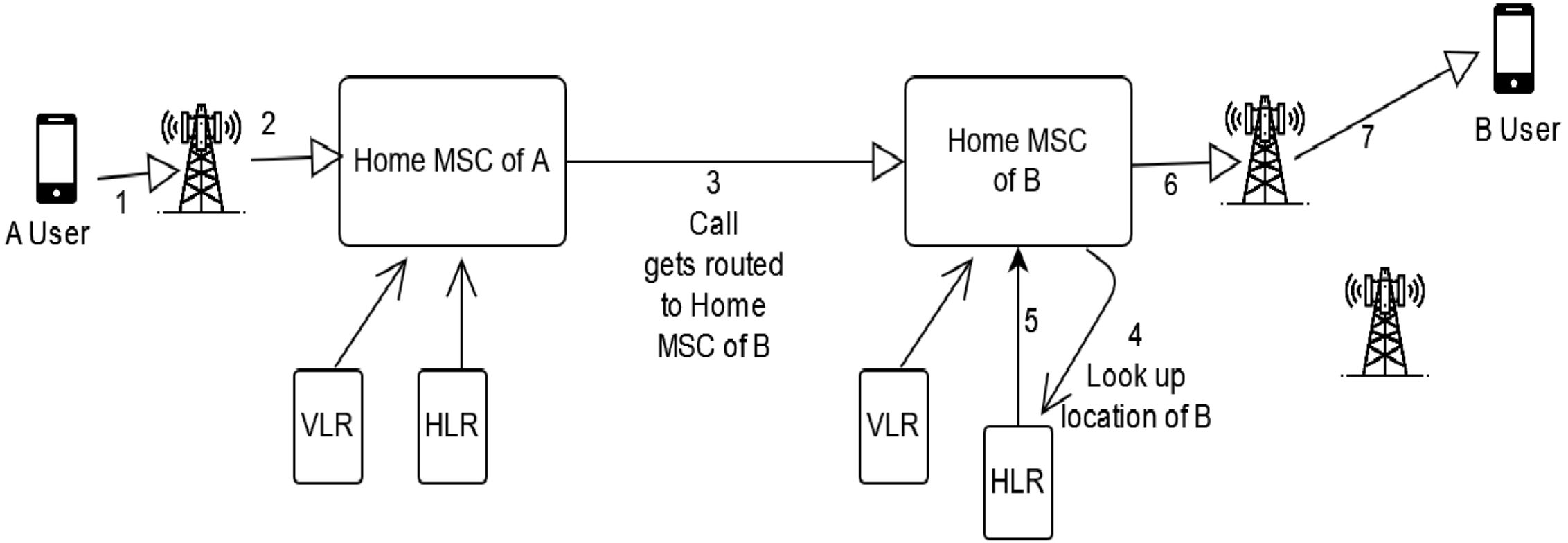
Scenario 1: Users A and B present in the same circle and use same service provider



Call gets routed to the destination tower to which B is connected based on the location returned by Home Location Register (HLR)

Mobile Call Routing

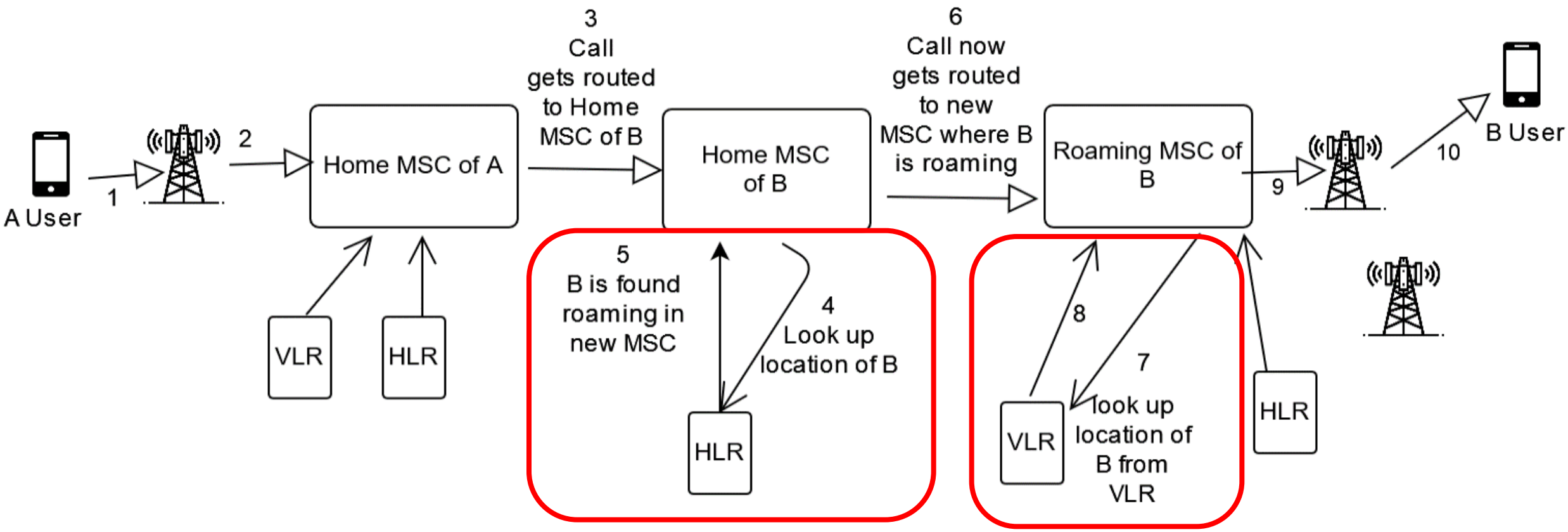
Scenario 2: Users A and B present in different Circles



Call gets routed to the destination MSC based on mobile number code and finally B is located based on the location returned by Home Location Register (HLR)

Mobile Call Routing

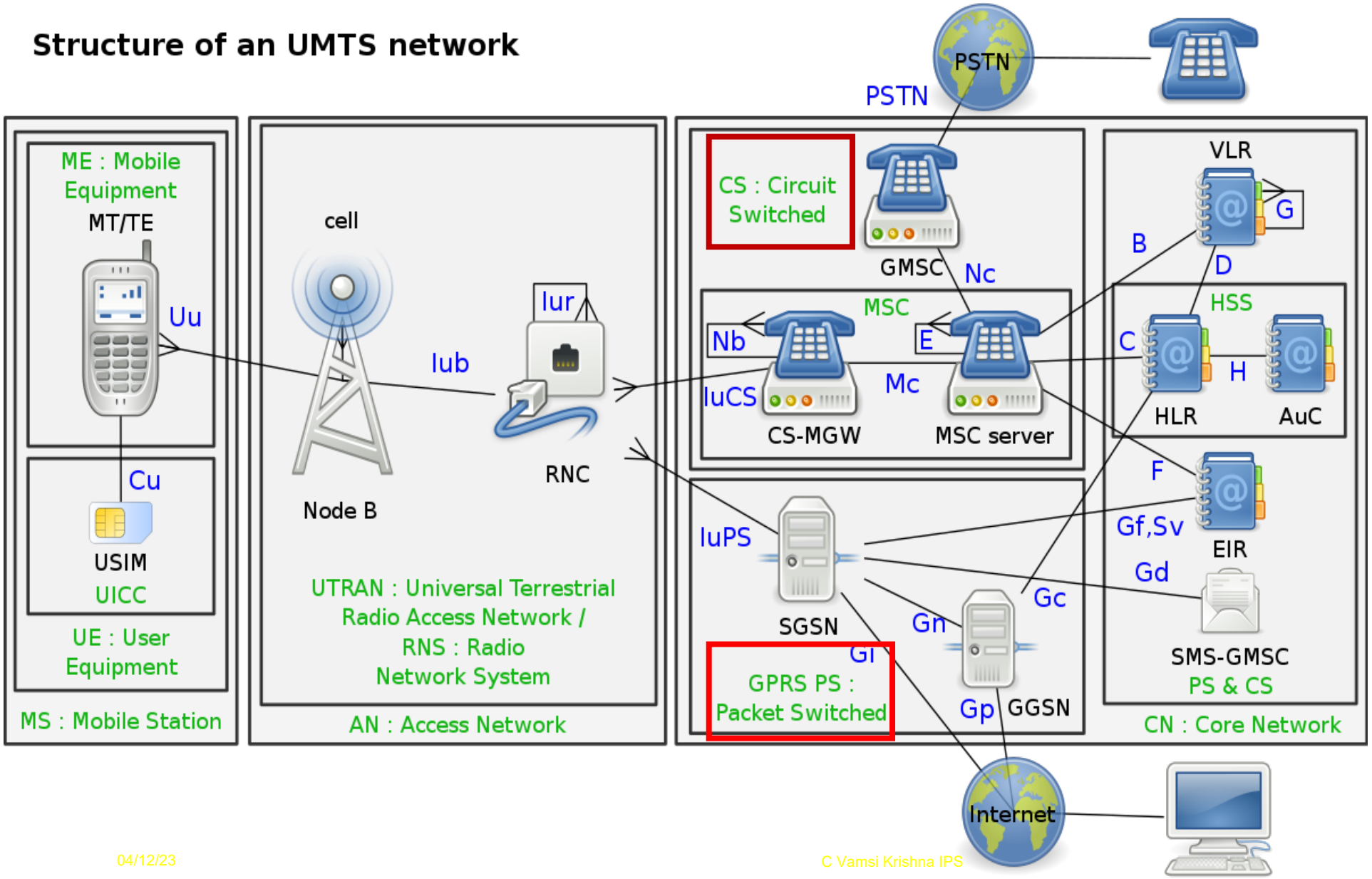
Scenario 3: User A wants to connect to B who is on roaming



Call gets routed to the home MSC of B first. HLR of Home MSC informs that B is roaming in a particular MSC. Call is forwarded to that MSC where B is roaming. Finally, B is located based on the location returned by Visitor Location Register (VLR)

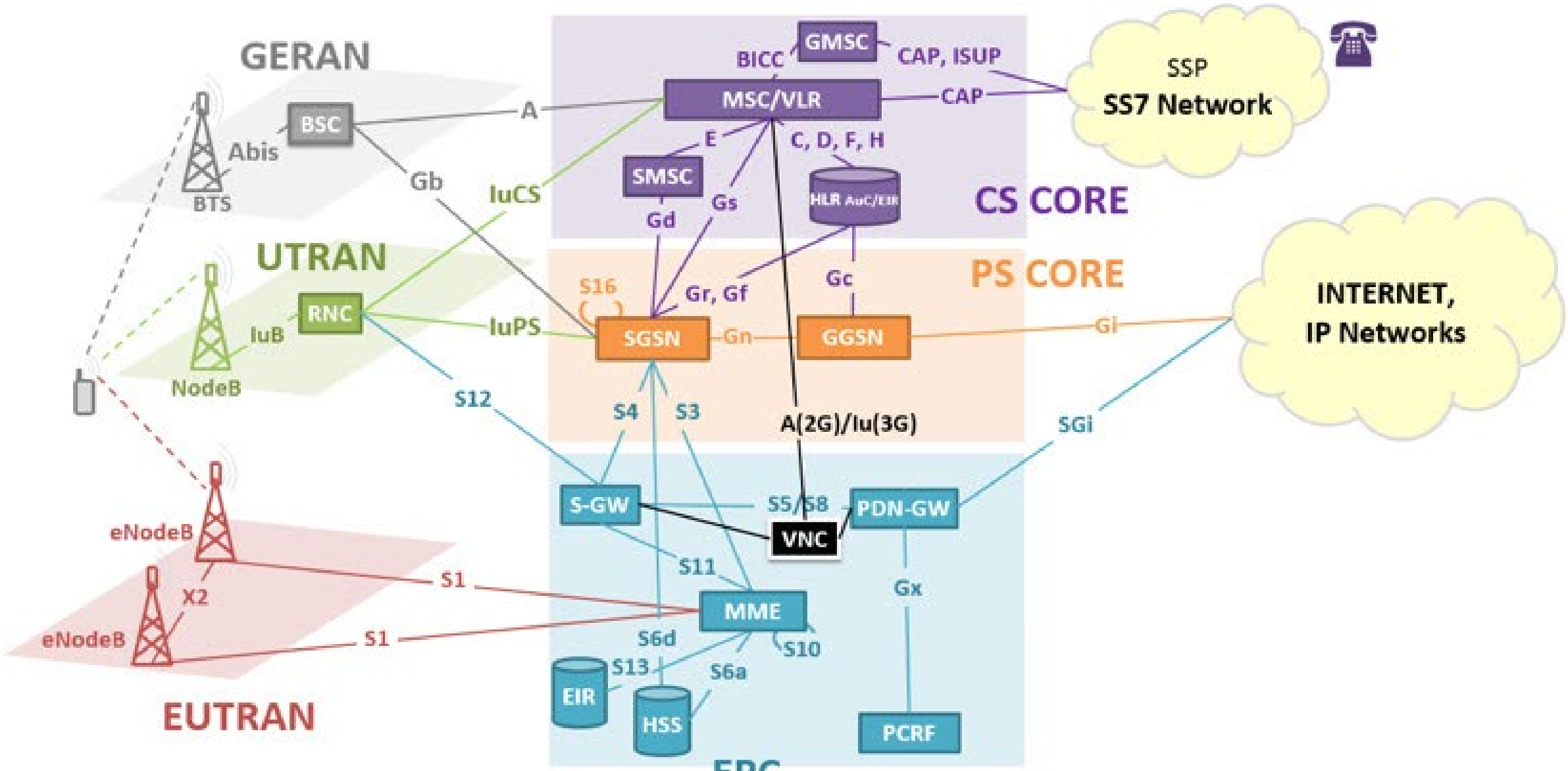
Universal Mobile Telecommunication Systems

[UMTS popularly known as 3G]



ME - Mobile Equipment
UICC - Universal Integrated Circuit Card
Node b - Similar to BTS
RNC - Radio network controller
Circuit Switching
Packet Switching
MSC - S - MSC Server
SGSN - Serving GPRS Support node
GGSN - Gateway GPRS Support node

2G, 3G and 4G networks at a Glance



5th Generation

- 10 times faster than 4G LTE and used in virtual reality, IoT, driverless cars etc

- **5G is convergence of following technologies**
  - **Millimeter waves**
  - **Micro Cells**
  - **Massive MIMO**
  - **Beam Forming**

Millimeter Waves

- 30 GHz to 300 GHz. Shorter waves, higher frequency

Small Cells

- As millimeter waves cannot travel through buildings and bad weather.

Massive MIMO

- Base stations will have several ports to handle increased traffic.

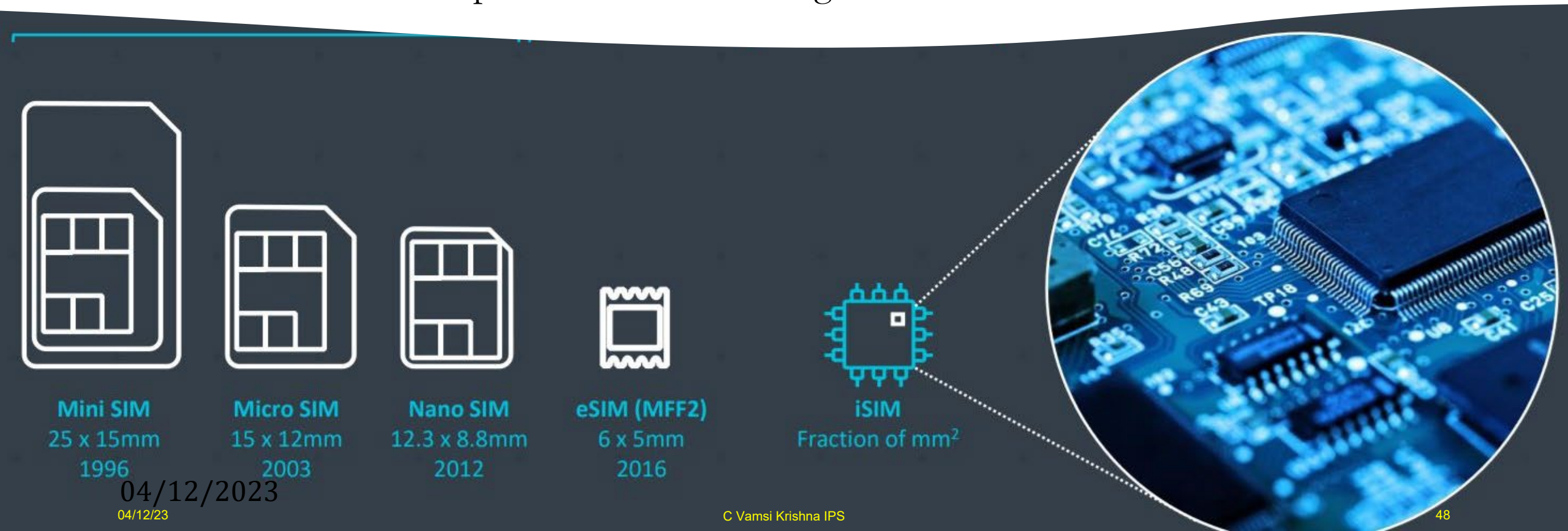
Beam Forming

- Similar to traffic signaling system for cellular signals where the signals are routed to the specific user.

Subscriber Identity Module [SIM]

Universal Integrated Circuit Card

- **SIM** card in GSM / UICC in UMTS
- **Different Sizes –** Mini, Micro, Nano
- **Embedded SIM** - **eSIM** is still a physical SIM, but instead of being removable it is embedded and is programmable.
- **Integrated SIM** - **iSIM** is embedded in the main SoC alongside the processor. iSIM is designed for more secure IoT devices.

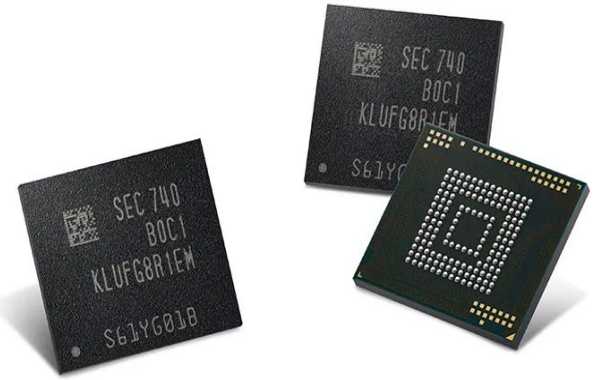


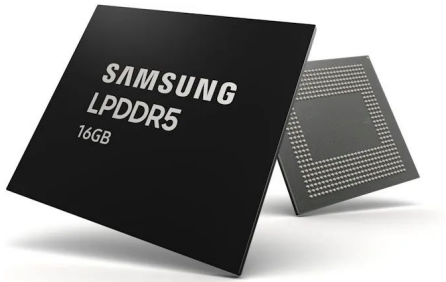
Evidences On SIM

- ICCID number (Integrated Circuit Card Identifier).
- Call logs (only last 10 dialled numbers, no incoming numbers are stored)
- SMS and Phonebook (if stored by user)
- IMSI number (if SIM is activated)
- LOCI (Location information – last tower information before power off)
  - LOCI comprises – TMSI, TMSI time, location update status and LAI (MCC+MNC+LAC)

Understanding Smartphone Storage

- ROM
- RAM
- Flash Memory
  - eMMC - Embedded Multi-Media Card
  - UFS – Universal Flash Storage
- SD Card

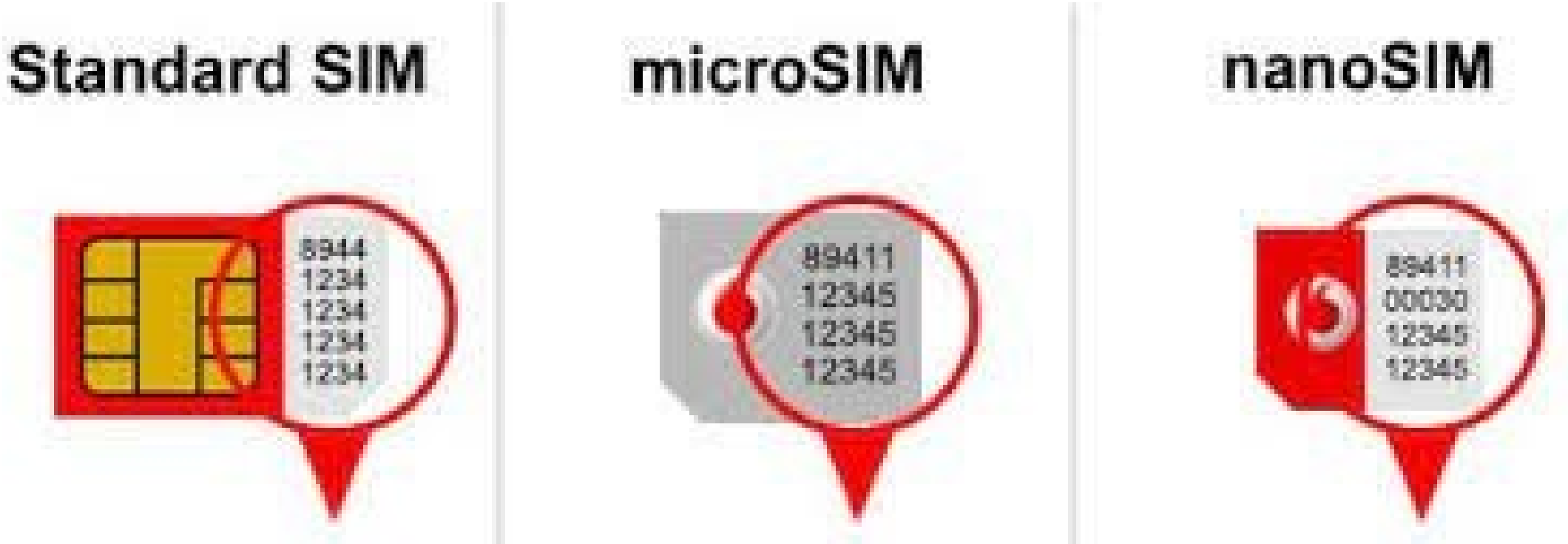




Important GSM Identifiers

ICCID & MSISDN

- **ICCID: Integrated Circuit Card Identifier**
- **MSISDN: Mobile Subscriber Integrated Service Digital Number** is Mobile Phone Number



Mobile Country Code [MCC] and Mobile Network Code [MNC]

- The mobile country code consists of three decimal digits
- Mobile network code consists of two or three decimal digits
- MNC is used to uniquely identify a mobile network operator (carrier)
- https://mcc-mnc.com/ provides for full list of all codes.

IMEI

International Mobile Equipment Identity (IMEI)

The IMEI number identifies a mobile station equipment.

Dial * # 06 # to get a 15-digit string

DUAL SIM PHONES - Each transceiver module is identified by a separate IMEI number

What is an IMEI?

Every device must have a unique IMEI number identifying brand owner & model.

The Brand Owner must apply to the GSMA for the TAC code.

Rule:

TAC: Type Allocation Code

86 — **Reporting Body identifier**

916102 — **Type Identifier** Indicating brand owner and device model allocated by Reporting Body

Serial Number

991292 — **Unique Number** assigned to individual devices by the manufacturer

Check Digit

0 — A function of the other digits [calculated by the manufacturer]

The 15 digit **TAC code** identifies the brand owner and model

Source: GSMA

How are TAC / IMEI serial numbers used?

Unique and accurate IMEI are **essential** for the mobile ecosystem

Source: GSMA

Tampering the IMEI

- Prohibited under **"Mobile Device Equipment Identification Number, Rules, 2017"**
- Rules made under **Section 7** read with **section 25** of the **Indian Telegraph Act, 1885**
- Mobile Device Equipment Identification Number' means a unique
  - (i) international mobile equipment identity number (IMEI);
  - (ii) electronic serial number (ESN)
  - (iii) any other number or signal – that identifies a unique mobile wireless communication device; or for the purposes has the same function and purposes as specified above.
- Punishment **may extend to three years, or with fine or with both.**

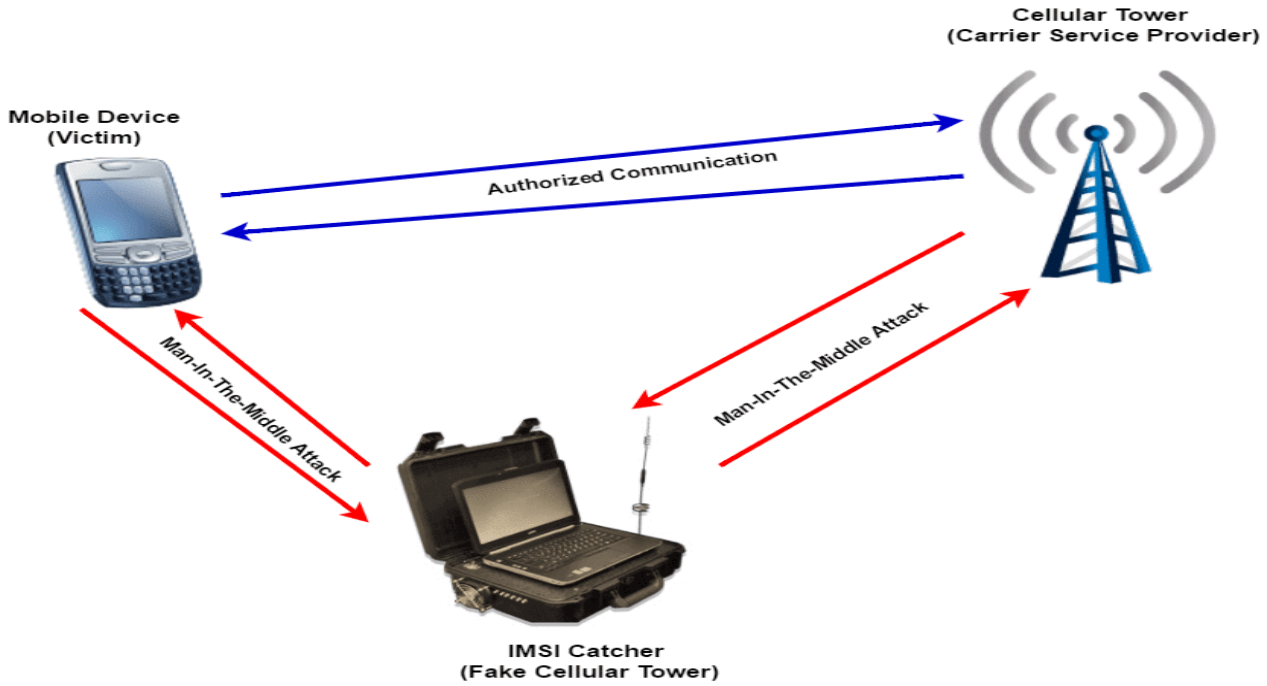
International Mobile Subscriber Identity

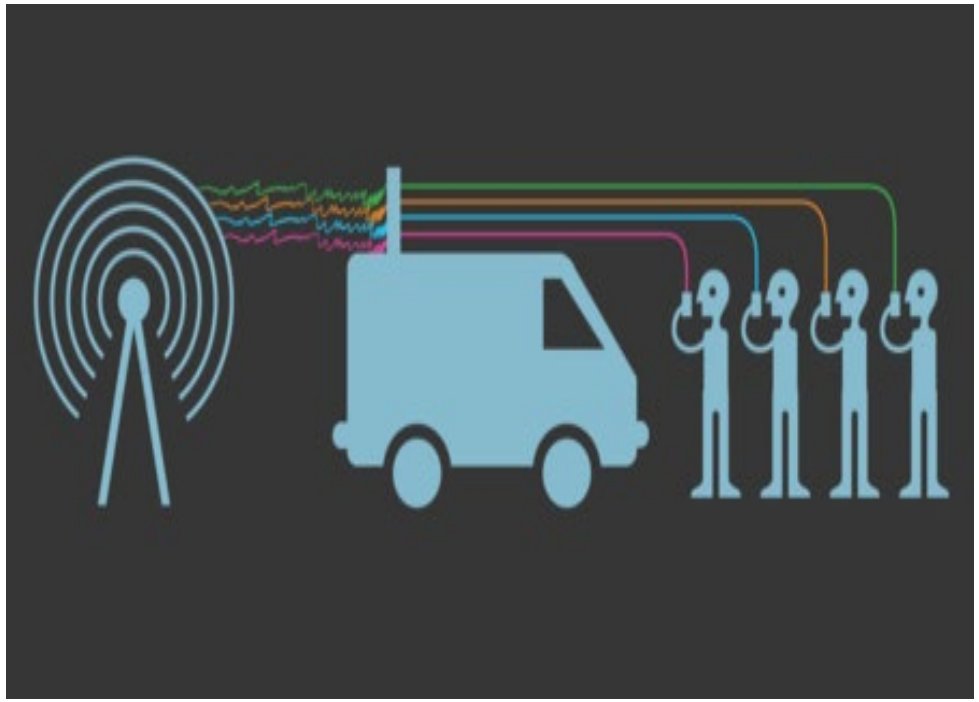
IMSI

- The International mobile subscriber identity is a number that **uniquely identifies every subscriber** of a cellular network.
- **It is stored as a 64-bit field and is sent by the mobile device to the network.**
- 15-digit number

- **TMSI** – Temporary mobile subscriber identity number
  - Is used to keep the IMSI secret
  - Helpful in roaming and identification of SIM card in roaming MSC

IMSI Catcher and Eavesdropping





- SS7 is protocol used to enable interoperability between 2G and 3G networks.
- The cyphering encryption is reduced to either no-encryption or to easily breakable one. (A5/0, A5/1, A5/2)
- Stingray, Skylock, Phantom etc.

Mobile Forensics

Standard Operating Procedure

Evidences inside a mobile phone

The potential evidence on mobile phones:

- Subscriber and equipment identifiers
- Date/time, language, and other settings
- Location information
- Phonebook/Contact information
- Calendar information
- Text messages
- Outgoing, incoming, and missed call logs
- Photos, Audio and video recordings
- Instant messaging & Multi-media messages
- Web browsing activities
- Stored documents and Emails
- Social media and App related data

Fundamental Principle of Digital Evidence Acquisition

Preservation of Original

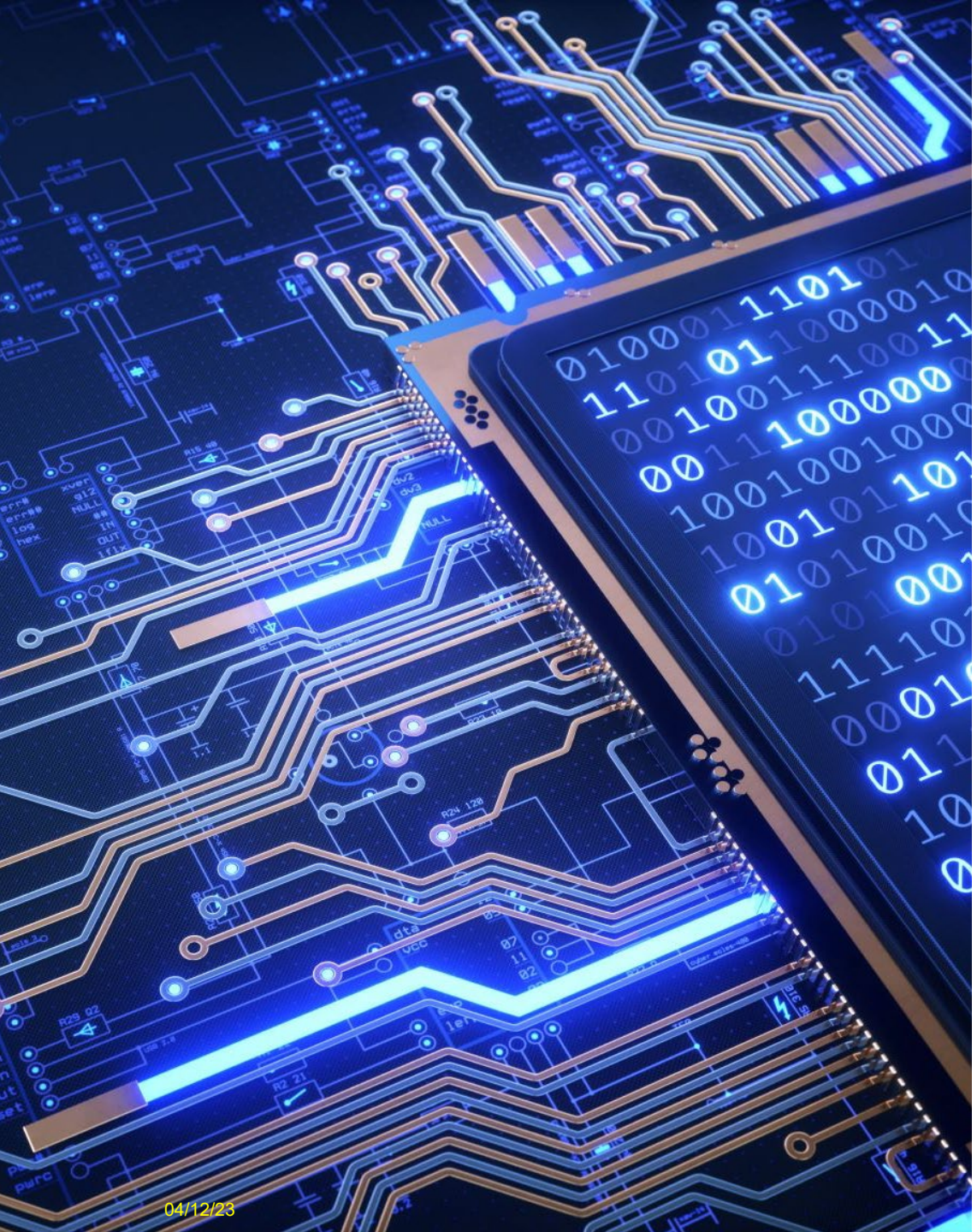
No action taken by law enforcement agencies, or their agents **should change data held on a computer or storage media**, which may subsequently be relied upon in court.

[Association of Chief Police Officers (ACPO) principles of digital evidence collection]

Fundamental Issue with Mobile "Forensics?"…

- The manufacturer of the device prevents the direct access and reading of physical memory.
- To uncover the deleted files and data, will need the help of some tools to overwrite the bootloader and get access to the physical memory.
- Hence, mobile acquisition tools cannot be connected using a write blocker. Drivers need to be installed to ensure communication between the forensic tool and the device.
- No recognized international standard protocol for data transfer and forensic extraction. Different products extract different amounts of information from different devices.
- As the device is constantly switched "**on**", the clock and the processes are always running. **Due to which data gets constantly updated.**

Integrity of Evidence collected??????



Challenges in Mobile Forensics

1. Hardware and OS differences
2. Mobile OS and their versions
3. Encryption and security features
4. On chip Storage
5. Lack of standardization of specifications like cables, storage tech and forensic tools etc
6. Live acquisition and prevention of data modification while conducting forensics – need to be turned on to conduct forensics
7. Anti-Forensic techniques like remote wiping, remote locking etc

How is mobile forensics different from computer forensics?

Mobile Forensics

- Always tries to connect to Network
- Penetrative process
- Write blocker cannot be used
- Storage cannot be separated
- Live acquisition
- Physical and application-based acquisition
- Hash of only file can be taken for integrity check

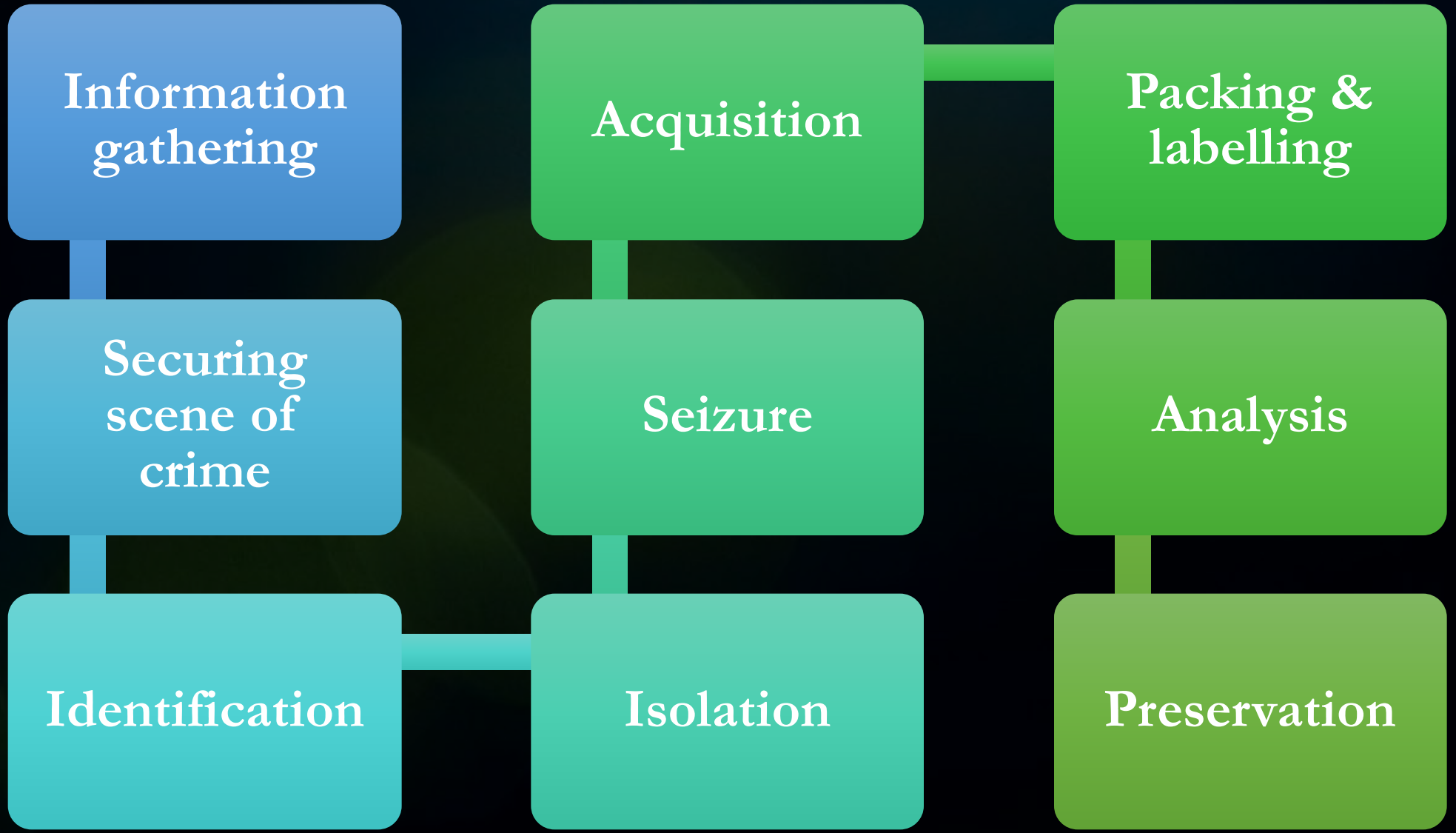
Computer Forensics

- Can work without network connectivity
- Non-penetrative process
- Write blocker can be used
- Storage can be removed
- Image can be made when system is off
- Image of file or partition or disk
- Hash of disk can also be calculated

Challenges for Data Acquisition from Mobile Devices

- Background activities – always running
- Optional or enforced data encryption
- Secure lock screens
- Locked bootloaders and secure kernels
- Remote kill switches
- Non-removable storage
- Activities can be triggered by events
- Push events from online services
- Remote events initiated by the user.
- Soldered RAM chips

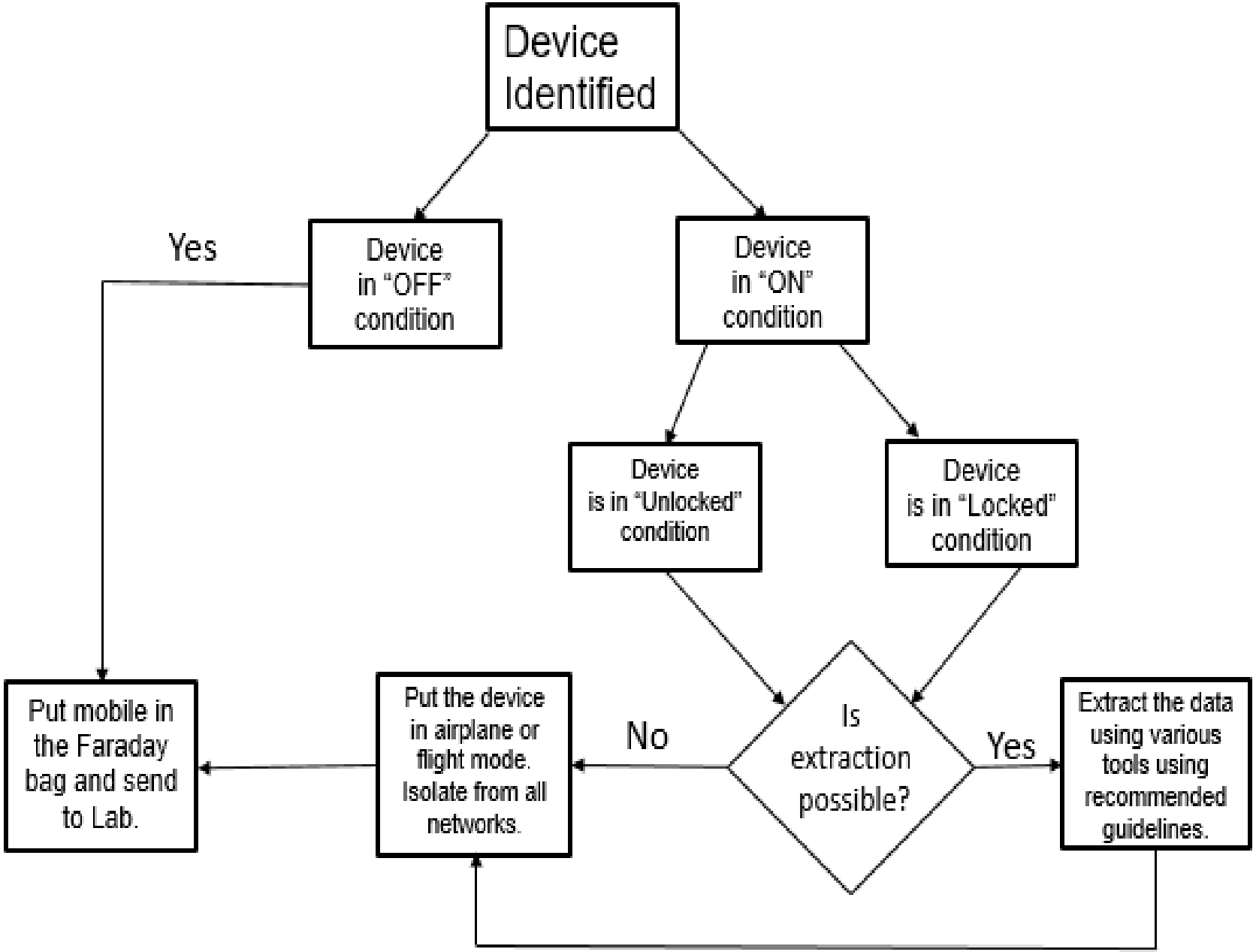
Steps in Mobile Forensic Process



Network Isolation

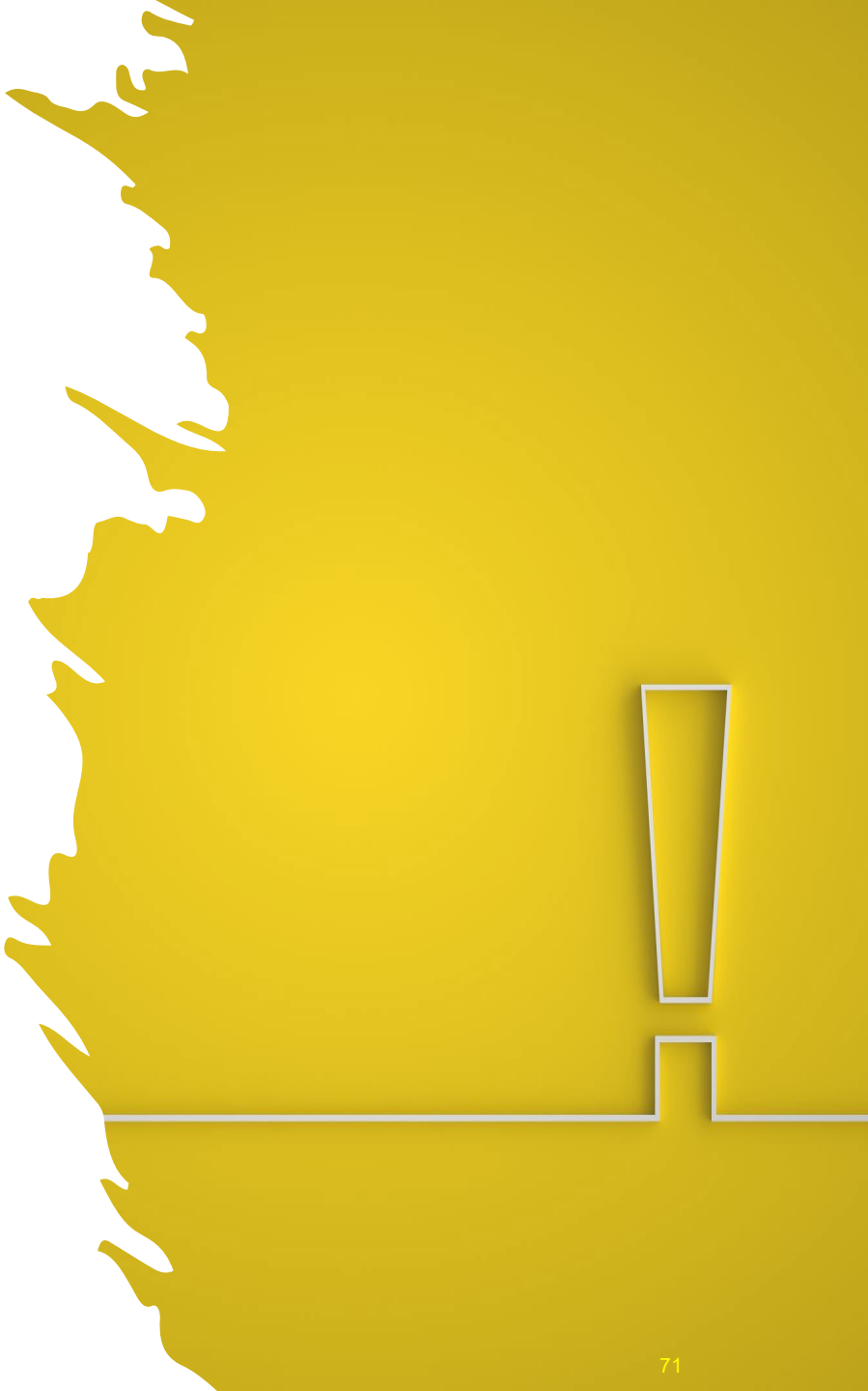
- Once identification is done, now find out current state of the device:
  - Switched ON
  - Switched OFF
- An IO needs to detach the device from any kind of network (Wi-Fi, Bluetooth or Mobile network).
- Airplane/Flight mode can be useful for this.
- **Wi-Fi can work even when the phone is on flight mode**
- **“Faraday Bag”**

Seizure


Device Identified
Device in "OFF" condition
Yes
Device in "ON" condition
Device is in "Unlocked" condition
Device is in "Locked" condition
Is extraction possible?
No
Yes
Put the device in airplane or flight mode. Isolate from all networks.
Put mobile in the Faraday bag and send to Lab.
Extract the data using various tools using recommended guidelines.

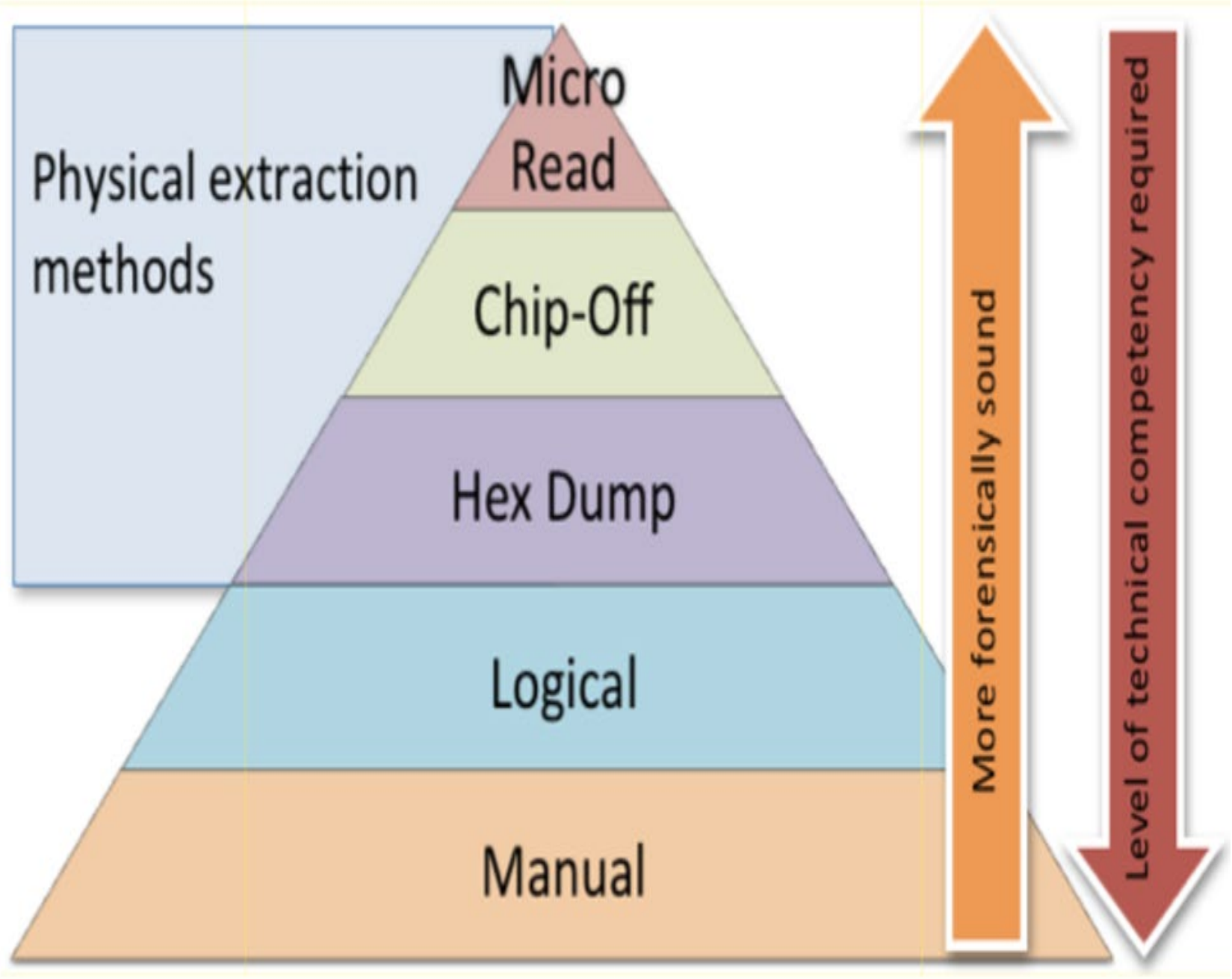
Unlocked Device

- **DO NOT DO ANYTHING THAT LOCKS THE PHONE!!!**
- Take pictures of the device.
- If you have tools for physical or logical extraction of the data with you
  - then try to extract as much information as you can in the field itself.
- Once the extraction is done (or if it is not possible) then isolate it from network and pack it in Faraday Bag and send it by fastest mode to forensic examiner.
- If isolation is not supported, then pack it directly in Faraday Bag and send it by fastest mode to forensic examiner.



Cellular Phone Tool Leveling Pyramid

(Sam Brothers, 2009)



Acquisition

Types of Data Acquisition from mobile phones

1. Physical Extraction:

- Extracting data bit by bit from the physical memory of the device, and removable memory –raw data. This way deleted information can also be extracted. This acquisition allows the examiner to uncover the **deleted files and data**, obviously with the help of some tools.

2. Logical Extraction:

- Extracting the data or application data on the device that you see and can access on the device. Call logs, phone books, SMS messages, pictures, email, browsing, etc. Tools that perform logical acquisition begin by sending a series of commands over the established interface from the computer to the mobile device. The mobile device then responds based upon the command request. The response (mobile device data) is sent back to the workstation and presented to the forensic examiner for reporting purposes. In most instances, an API is used for interacting with the mobile device.

3. Hardware level Data Extraction:

- Using techniques like JTAG, ISP, Chip-off, wherein the Electronic Chip is taken out and by using soldering pins, a hardware level electronic data recovery is done using different gadgets.

Tools Available for Data Extraction

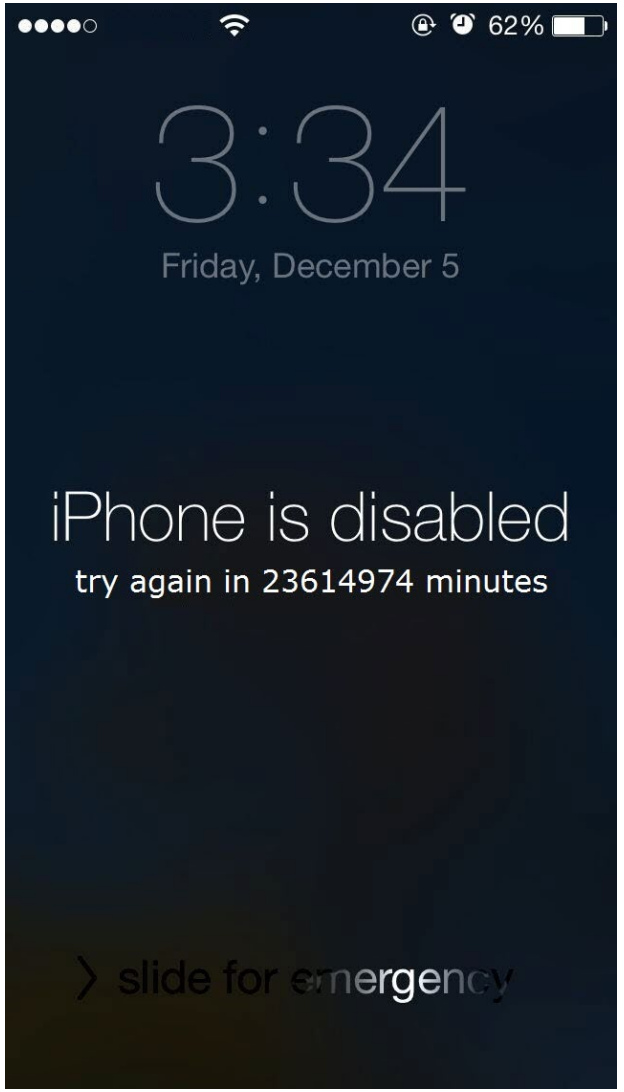
Locked Device

- **Do not try to guess the PIN / Password.**
- Take pictures of the device.
- Use Airplane mode or faraday bag to isolate the phone.
- Send it by fastest mode to forensic examiner.

iOS 7.0 and above

Six failed attempts gets you a 1-minute lockout. Seven gives you 5 minutes, eight gives 15, and nine 1 hour.

After ten failed attempts, the system will either lock you out completely or erase your data, depending on your settings



If Device is switched off

- **DO NOT SWITCH ON THE MOBILE PHONE.**
- Collect Make, Model and serial numbers, IMEI numbers.
- Capture photos of the device showing all details.
- Send it by fastest mode to forensic examiner with necessary documentation and cables or connectors.

Collecting Cables /Connectors Drivers

- One should seize the cables (or connectors) if any while seizing the device.
- **Same cables may not be available in the market on a future date.**
- **Some smartphones only extract data or charge when an original data cable is used.**
- Different devices use different types of cables for example: type – C, micro USB.

Documentation

- Panchnama/ Mahazar is technical in nature
- Process of documenting **every piece of electronic evidence** with its serial number, make and model properly in seizure memo along with the photographs of SOC.
  - **Seizure Memo**
  - Chain Of Custody
  - Forwarding note to FSL

Packing and Labelling

- If acquisition is done;
  - Label the Material Object properly with all the signatures required.
  - Pack the mobile using anti-static bag and then in bubble wrap.
- If faraday bag is being used
  - Put the mobile in faraday bag in switched on mode.
  - Give power supply if required.
  - Use the bag which is rated for particular frequency
- Storage facilities that hold evidence should provide a cool, dry environment appropriate for valuable electronic equipment.