Mobile Forensics and Challenges

Saurabh Kumar
Senior Research Scholar
IIT Kanpur
Date: 08/03/2022

https://github.com/skmtr1/Workshop-Mobile-Forensics-And-Security

DIGITAL FORENSICS & INVESTIGATION

Terms and Definitions

- **Mobile Forensics:** The science of recovering digital evidence from mobile phone under forensically sound conditions using accepted methods. (NIST)

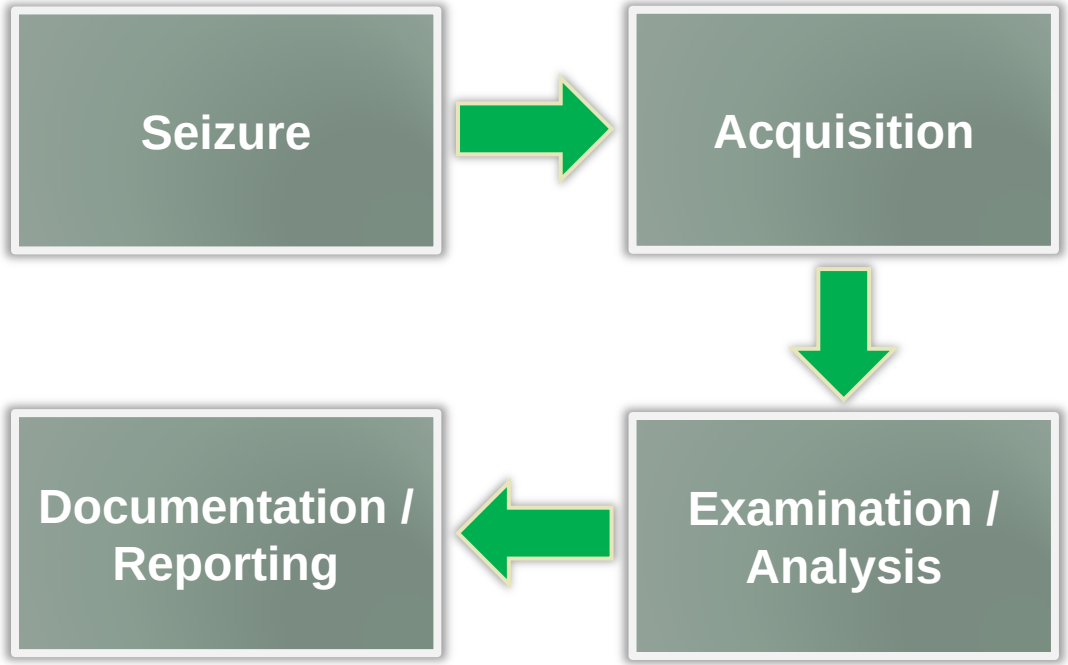
- **Penetration Test:** A method of evaluating the security of a computer system or network by simulating an attack from malicious **outsider/insider**. (Wikipedia)

- **Vulnerability Assessment:** A process of identifying, quantifying and prioritizing the vulnerabilities in a system.

Forensics Overview

- Potential scenarios, not specific to Mobile
- Evidence gathering for legal proceedings
- Corporate investigations
  - Intellectual property or data theft
  - Employment-related investigations including discrimination, sexual harassment
  - Security audit
- Family matters
  - Property disputes
  - Divorce
- Government security and operations
  - Cyber Threats
  - Stopping cyber attacks
  - Intelligence / Counter-intelligence gathering

Investigation Process



Forensics Considerations

- Important items to consider during investigations
  - Chain of custody
  - Detailed notes and complete report

- Validation of investigations results using tools or other investigators

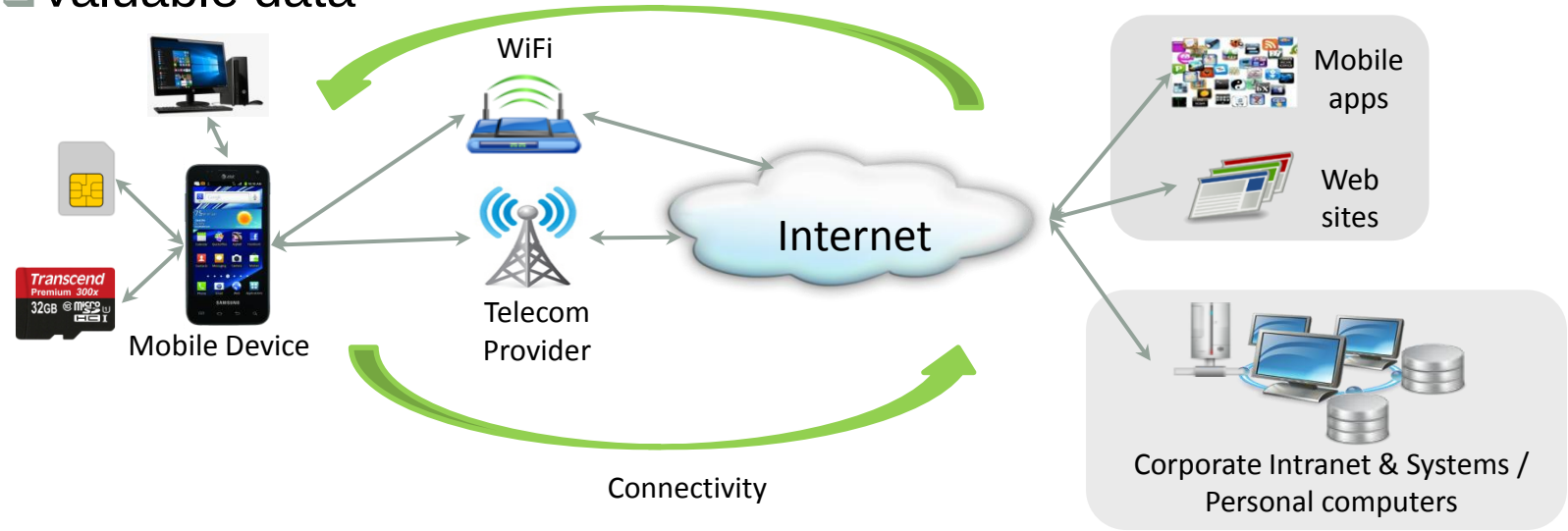
Legalities

- Possibility of a mobile device being involved in crimes
- Easily cross geographical boundaries; multi-jurisdiction issues
- Investigator should be well aware of regional laws
- Data may be altered during collections, causing legal challenges

MOBILE FORENSICS

Why Mobile Forensics?

- Technology improvements
- User activities
- Valuable data
- Always powered on
- Multiple Communication Entity



Types of Evidence from Mobile

- Physical

- Electronic

Physical Evidence from Mobile

- DNA

- Fingerprints

Electronic Evidence

- Can be use to establish **LAB**
- **L**ocation
- **A**ssociation
- **B**ehavior
- Some Information
  - Call history
  - Contacts
  - SMSs
  - Calendar
  - Location
  - Images
  - Audio/Video
  - Many more…

Sources of Information

Call history
Location
Tracking

IMSI
ICCID
Contacts
SMSs

Audio
Video
Backup

IMEI
Contacts
SMSs
Call History
Location

Behavior
Emails
Photos
Location

Network Service Provider

- Can provide
  - Subscriber details
  - Call History – Call Details Record (CDR)
  - List of accessed web services – IP Details Record (IPDR)
  - Geographic location – Tower locations through which a phone is connected for communication
  - Cell Tower Logs (Tower Dump)

Call Details Record (CDR)

- Looks like

Info abut associated Mobile Device

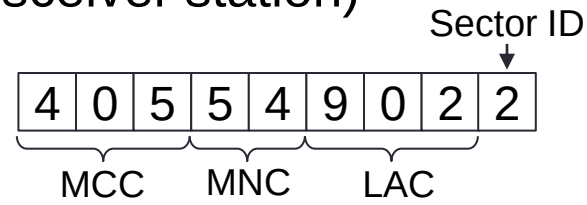
Info about user location

Calling No.	Called No.	REC TYPE	TRANS_DT	Duration	IMEI	CELL ID
94XXXXX093	94XXXXX032	MOC	20130101113117	63	35789004232353	405-54-902-2
94XXXXX534	94XXXXX093	MTC	20130101132532	40	35789004232353	405-54-576-1
94XXXXX997	94XXXXX093	SMT	20130101165754	1	35789004232353	405-54-576-3
94XXXXX093	94XXXXX109	MOC	20130101165937	247	35789004232353	405-54-576-2

Calling No.	Called No.	REC TYPE	Date	Time	Duration	IMEI	FIRST_CELL ID (Origin)
94XXXXX093	94XXXXX032	OUT	01/01/2013	11:31:17	63	35789004232353	405-54-902-2
94XXXXX534	94XXXXX093	IN	01/01/2013	13:25:32	40	35789004232353	405-54-576-1
94XXXXX997	94XXXXX093	S_IN	01/01/2013	16:57:54	1	35789004232353	405-54-576-3
94XXXXX093	94XXXXX109	OUT	01/01/2013	16:59:37	247	35789004232353	405-54-576-2

Cell ID

- Cell ID is used to uniquely identify BTS (base transceiver station)
- Comprises of four components
  - Mobile Country Code (MCC): first 2-3 digit
  - Mobile Network Code (MNC): next 2-3 digit
  - Location Area Code (LAC): variable length
  - Sector ID (SID): last digit
- Device is always associated with a BTS



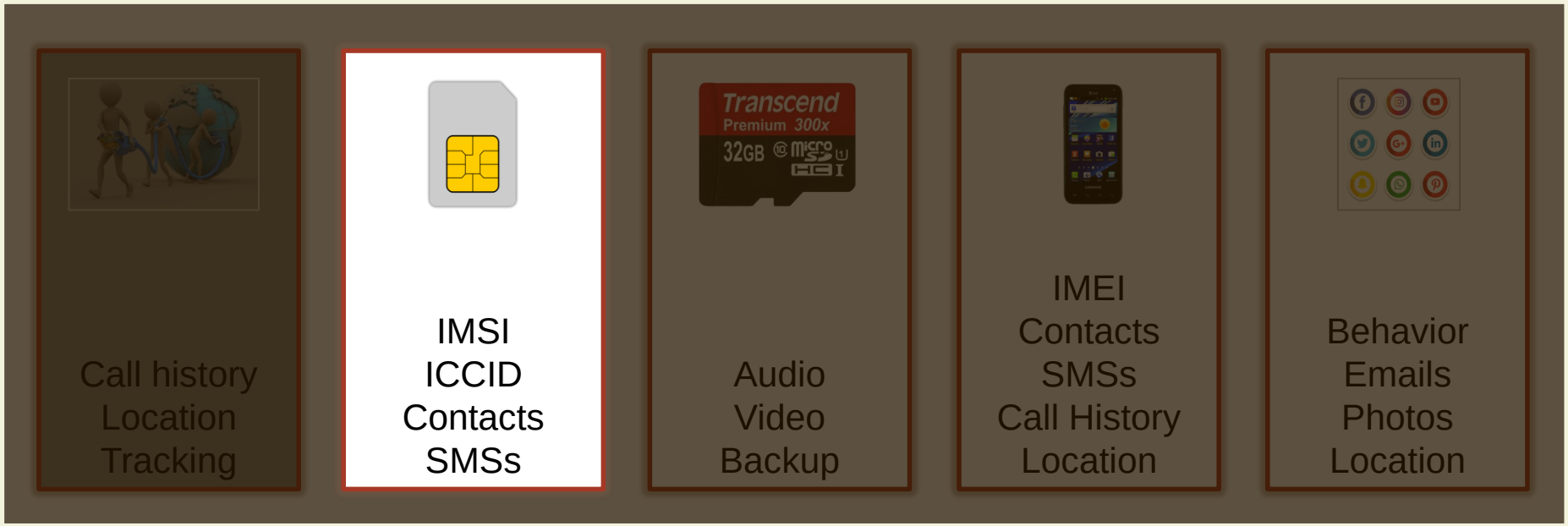
Tower Dump

SUBS NO	OTHER PRTY NO	Date	TIME	Dur	CELLID FIRST	CELLID LAST	REC TYPE	SUBS IMEI	SUBS IMSI	SUBSCRIPTION TYPE	SMS CENTER NO	MSCID
9197XXXXX772	9177XXXXX344	8/20/2013	05:01:51	25	11971-20/8	11971-20/8	MOC	359326022655600	405804191782627	PRE	?	919762099002
9181XXXXX996	9183XXXXX714	8/20/2013	05:10:29	1	13311-20/8	13311-20/8	SMMT	358650031107530	405804191482793	PRE	919823000040	919762099002
9197XXXXX131	9198XXXXX217	8/20/2013	05:38:48	94	13311-20/8	13311-20/8	MTC	359351043644880	405804170433460	POST	?	919762099002
9187XXXXX730	9187XXXXX108	8/20/2013	05:53:03	1	13311-20/8	13311-20/8	SMMO	355672050976690	405804181584703	PRE	919716099155	919762099002

Challenges with Mobile Networks

- No uniformity between CDR format
- Correlation among multiple CDR
- Difficulty in analyzing tower dump
  - Huge amount of data
  - Difficulty in extraction of useful information
- Non availability of live tower data

Sources of Information



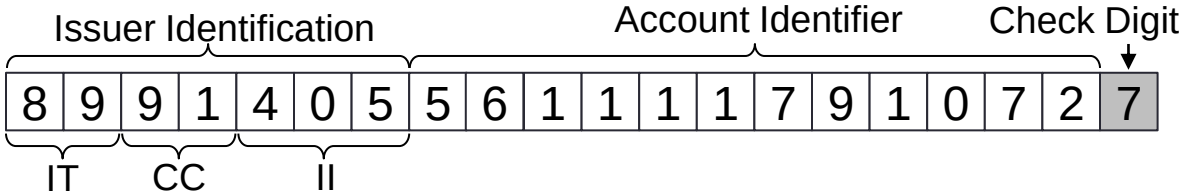
Subscriber Identity Module (SIM)

- Identifies/authenticates a subscriber to the network
- Two Unique Identities
  - ICCID
  - IMSI – (Programmable)
- Storage for contacts, SMSs, etc…

Integrated Circuit Card ID (ICCID)

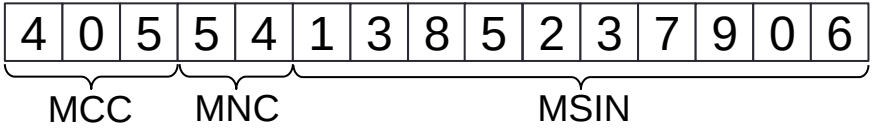
- It is a SIM serial number
- 19 or 20 digit length
- Service provider can identify phone number from ICCID
- Reveals country of origin, Industry Type, and network
  - Issuer Identification Number: composed of industry type (first 2 digit), country code (next 2-3 digit), and issuer identifier (next 1-4 digit)
  - Individual account identification: Variable length
  - Check digit – Last digit of ICCID

IT: Industry Type
CC: Country Code
II: Issuer Identifier



International Mobile Subscriber Identity (IMSI)

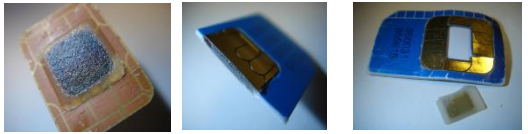
- Used by the network to identify subscriber
- 15 digit number
- Stored on the SIM card (programmed by the network provider)
- Reveals name and country of issuing service provider
  - Mobile Country Code (MCC): first 2-3 digit
  - Mobile Network Code (MNC): next 2-3 digit
  - Mobile Subscriber Identification Number (MSIN): remaining digits



Challenges with SIM

- Issue with ICCID
  - Partial ID is printed on SIM card
  - No printed information about ICCID

- Damaged SIM card



- eSIM

Sources of Information

Call history
Location
Tracking

IMSI
ICCID
Contacts
SMSs

Audio
Video
Backup

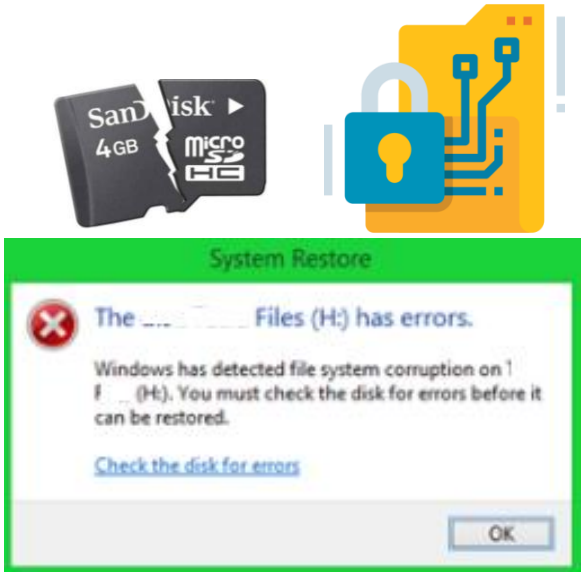
IMEI
Contacts
SMSs
Call History
Location

Behavior
Emails
Photos
Location

Memory Card

- Serves as secondary storage for mobile
- Use file system to store information mostly FAT
- Stores Audio, video, photos, backup, etc…

- Challenge:
  - Damaged memory card
  - Corrupted file system
  - Encryption



Sources of Information

Call history
Location
Tracking

IMSI
ICCID
Contacts
SMSs

Audio
Video
Backup

IMEI
Contacts
SMSs
Call History
Location

Behavior
Emails
Photos
Location

Mobile Handset

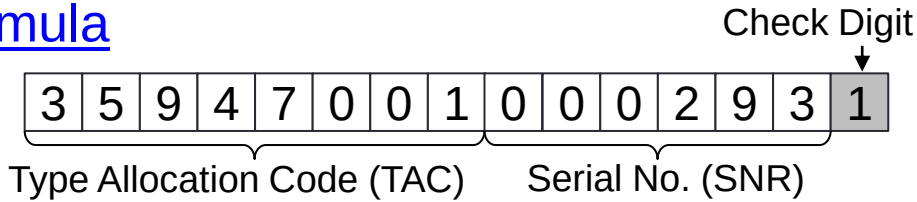
- Just Looking
  - Make / Model
  - Condition
  - Age
  - Capabilities
  - Network type 2G, 3G, 4G, Others
- Rich source of information
  - Contacts, images, videos, call logs, SMSs, etc..
- Uniquely identified by using IMEI






International Mobile Equipment Identifier (IMEI)

- Kind of serial number of the handset, (15 digit long)
- Intended to be unique
  - Can be reprogrammed with specialized equipment (illegal)
- Can reveal (First eight digits, TAC)
  - Make, mode, date and country of origin
- Serial Number (next six digits)
- Check digit (last digit)
- Can be validated by using Luhn formula



Information of Interest

Basic Information	• IMEI • H/W and S/W information • Network Information
Event Logs	• Incoming, outgoing missed call history • SMS history • Session logs – Wi-if, GPRS/3G/4G
Calendar Events	• Meetings, reminders • Last modification
Tasks	• Description • Deadline, priority • Completion date & time
Messaging System	• Text and multimedia messages • BIO messages: vCard, configurations, and others • Beamed messages: file sent via Bluetooth, IT or USB

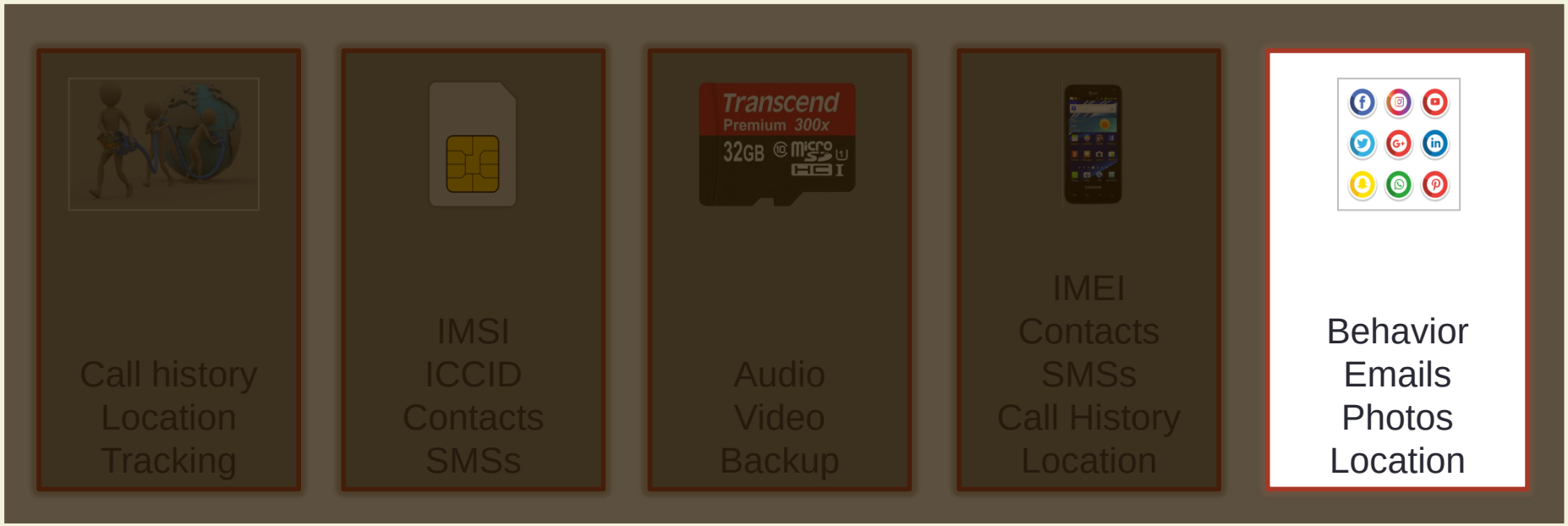
Information of Interest cont..

GPS Navigation	• Last fixed GPS coordinates • Search and Routes history • Saved maps, favorite places
Location Tagger	• GPS coordinates in camera snapshots • Cell tower coordinates in camera snapshots • Cell tower coordinates for SMS, calls
IM Clients	• IP, Login (UID, email) and password* • Contact list • Chat and call history
Contact Info	• Caller groups • Speed dials
Apps	• Multiple Apps with their storage capacity • Like social media activities, emails, web history, etc..

Challenges with Mobile Device

- Multiple smartphone vendors and OS(es)
- Mobile platform security features
- Generic state of the device
- Anti-forensic techniques
- Dynamic nature of evidence
- Accidental reset
- Device alteration
- Phone lock
- Malicious Programs
- Multiple communication point
- Legal issues

Sources of Information



Applications (Apps)

- Can be used to analyze behavior/state of person
  - Social gathering, health condition, etc..
- App stores local data in SQLite database
- Application analysis can give type of information and metadata about an App

- Challenge:
  - Different architecture for different Apps
  - Dynamic nature – behave differently in different environment
  - Use of encryption to store data
  - Correlations between Apps

CASE STUDY

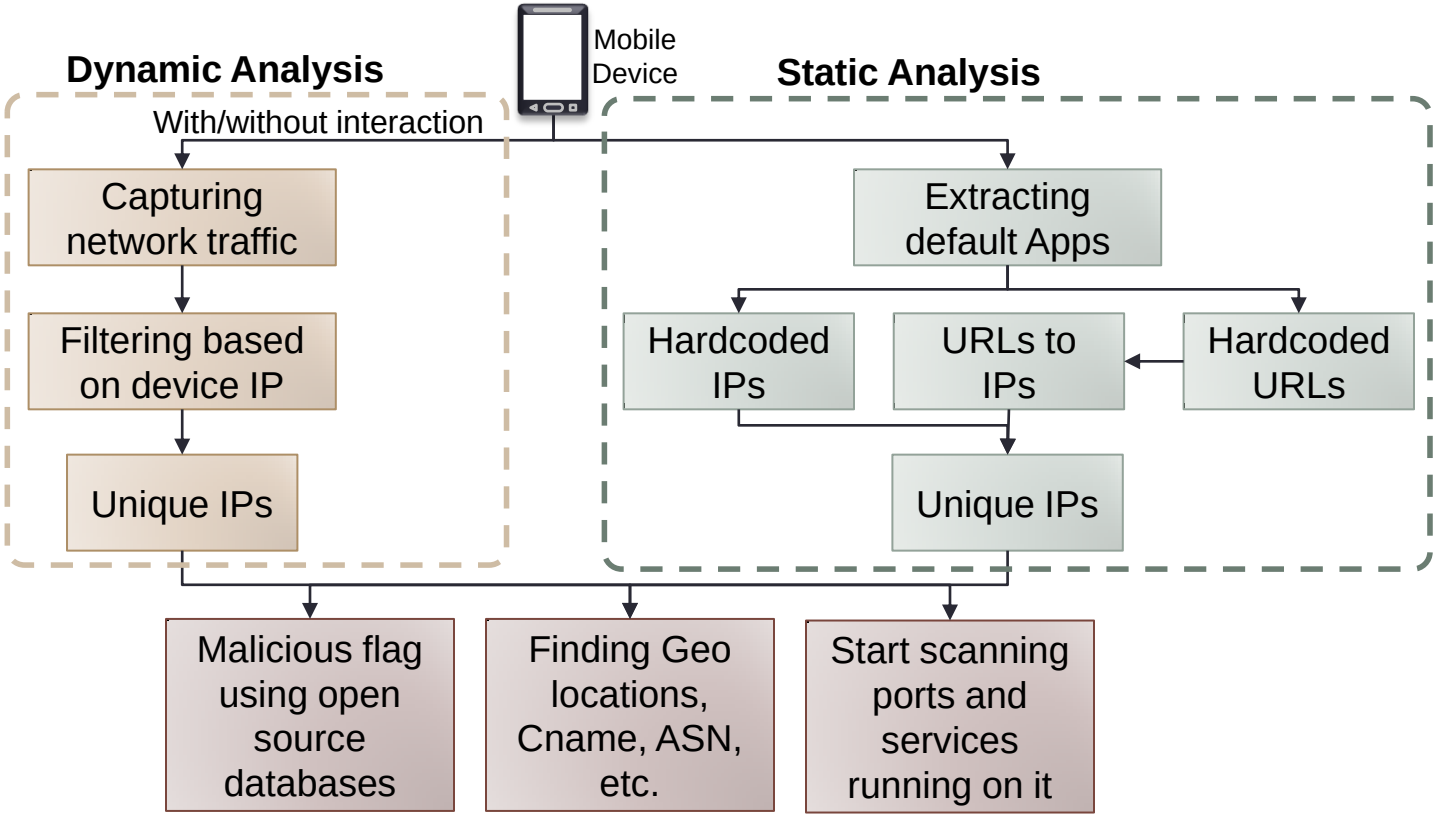
VAPT of Mobile Devices

Why VAPT of Mobile Devices?

- In September 2021 (Lithuania Government)
  - Malicious activities by Xiaomi Mi 10T mobile
  - Communication to outside server
  - Censoring certain terms and phrases

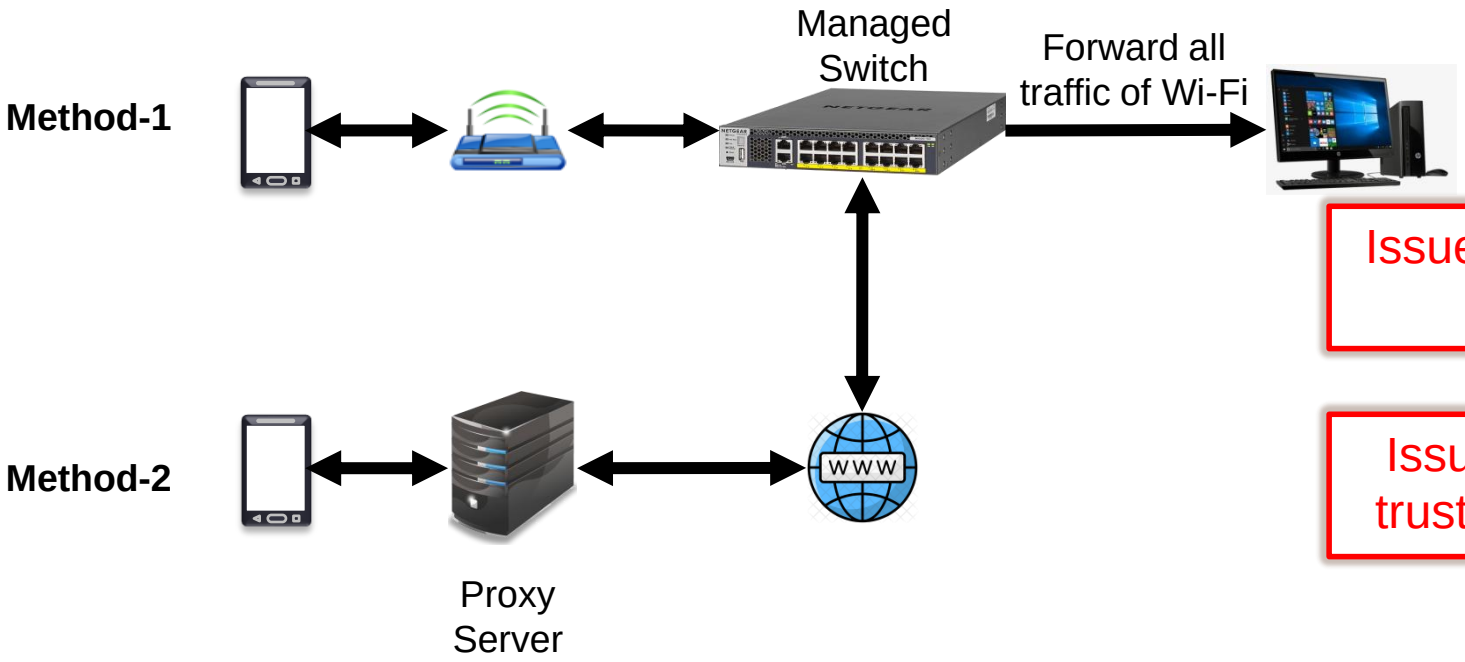
- C3i Hub at IIT Kanpur decided to test new Xiaomi Mi 10T device available in the Indian market

Analysis Workflow



How to Monitor Network traffic

- Two ways.



VAPT OF XIAOMI MI 10T

Analysis of Device

- Three scenarios
- First, Network traffic analysis without interaction
- Second, Traffic analysis with interaction
- Third, Static analysis of default applications (Apps)

Traffic Analysis Without Interaction

Configuration

- Did not configured Google account
- No third-party app installed
- No alteration to device such as rooting
- Connected with Wi-Fi router
- Wi-Fi router is connected with managed switch
- Port mirroring to get network traffic on a system

Results and Observation

- 188 unique IPs
- Active SSH connection to the device from IP 165.XXX.189.245. IP is not present in IP Abuse database.
- Communication with custom port (5222 seems web based SSH) with two IPs (13.XXX.155.113, 13.XXX.235.56). IP 13.XXX.235.56 was flagged malicious by VirusTotal.com

Traffic Analysis With Interaction

Configuration and conditions

- Connected with Wi-Fi router
- Wi-Fi router is connected with a managed switch
- Port mirroring to get network traffic on a system and started capturing
- Creating an Mi account and start interacting with the phone
- Storing sensitive data such as photos, videos. Text files etc., with fine name such as password, username ..

Static Analysis: Default Apps

Procedure

- 89 default Apps
- Extracted using ADB
- From each application extracted hardcoded:
  - IPs
  - URLs
- Obtained unique IPs/URLs
- Search of IPs/URLs in publicly known databases to flag malicious IP/URLs

Results: Traffic Analysis with Interaction and Static Analysis of Default Apps

Results and Observation

- 1533 Unique IPs associated with Apps
- Two IP (129.226.107.102, 129.226.106.5) belongs to Tenecent Cloud Computing (Beijing) Co.
- 15 malicious IP flagged by different services of Virustotal
  - Services: Webroot, Comodo Valkyrie Verdict, EST security-Threat inside
  - Malicious IPs: 163.XXX.208.212, 185.XXX.111.153, 185.XXX.108.153, 185.XXX.110.153, 185.XXX.109.153, 157.XXX.158.198, 157.XXX.163.158, 221.XXX.79.225, 104.XXX.20.226, 104.XXX.21.226, 151.XXX.128.14, 157.XXX.163.158, 157.XXX.158.198

https://github.com/skmtr1/Workshop-Mobile-Forensics-And-Security

Thank You